

kaspersky

Kaspersky Security Center 14

© 2023 AO Kaspersky Lab

جدول المحتويات

[تعليمات Kaspersky Security Center 14](#)

[ما الجديد](#)

[Kaspersky Security Center 14](#)

[حول Kaspersky Security Center](#)

[مجموعة التوزيع](#)

[متطلبات الأجهزة والبرامج](#)

[قائمة من تطبيقات Kaspersky المدعومة والحلول](#)

[تفاصيل وميزات برنامج Kaspersky Security Center 14](#)

[عن توافق خادم الإدارة و Kaspersky Security Center 14 Web Console](#)

[حول Kaspersky Security Center Cloud Console](#)

[المفاهيم الأساسية](#)

[خادم الإدارة](#)

[التسلسل الهرمي لخوادم الإدارة](#)

[خادم الإدارة الافتراضي](#)

[خادم الجهاز المحمول](#)

[خادم الويب](#)

[عمل 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](#)

[البنية الهندسية](#)

[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 klservcert](#)

[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 \(LAN\) وخادم إدارة تابعان](#)

[خادم الإدارة في شبكة الاتصال المحلية \(LAN\)، الأجهزة المدارة متصلة بالإنترنت، TMG قيد الاستخدام](#)

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

[خادم الإدارة في منطقة الأجهزة الموصولة مباشرة بالإنترنت \(DMZ\)، الأجهزة المتصلة 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 DMZ](#)

[خادم الإدارة ويوابة اتصال في قطاع شبكة وجهاز عميل](#)

[خادم الإدارة وجهاز إن في DMZ: يوابة الاتصال وجهاز عميل](#)

[خادم الإدارة و Kaspersky Security Center 14 Web Console](#)

[تفعيل وإدارة تطبيق الأمان على جهاز محمول](#)

[أفضل ممارسات النشر](#)

[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](#)

[التكوين 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](#)

[كيفية اختبار نظام إدارة قواعد البيانات \(DBMS\) لخادم إدارة](#)

[تحديد نظام إدارة قواعد البيانات](#)

[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 DMZ](#)

[الوصول إلى الإنترنت: عميل الشبكة كيوابة اتصال في DMZ](#)

[حول نقاط التوزيع](#)

[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 Exchange](#)

[كيفية نشر خادم الأجهزة المحمولة Exchange](#)

[الحقوق المطلوبة لنشر خادم الأجهزة المحمولة Exchange](#)

[حساب لخدمة Exchange ActiveSync](#)

[خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM](#)

[التكوين القاسي: Kaspersky Device Management for iOS في DMZ](#)

[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](#)

[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 النقاظ صورة القرص الثابت لجهاز ما ونسخها](#)

[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 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](#)

[معلومات تثبيت خادم الإدارة](#)

[معلومات 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 المثبت عليها عميل الشبكة إلى حالته السابقة](#)

[التثبيت المحلي للتطبيقات](#)

[التثبيت المحلي لعميل الشبكة](#)

[تثبيت عميل الشبكة في الوضع غير التفاعلي \(الصامت\)](#)

[تثبيت عميل الشبكة لنظام Linux في الوضع الصامت \(مع ملف إجابات\)](#)

[التثبيت المحلي لمكون الإدارة الإضافي للتطبيق](#)

[تثبيت التطبيقات في الوضع غير التفاعلي](#)

[تثبيت التطبيقات باستخدام الحزم المستقلة](#)

[إعدادات حزمة تثبيت عميل الشبكة](#)

[عرض سياسة الخصوصية](#)

[نشر نظم إدارة الأجهزة المحمولة](#)

[نشر نظام للإدارة عبر يروتوكول Exchange ActiveSync](#)

[تثبيت خادم الجهاز المحمول لـ Exchange ActiveSync](#)

[اتصال الأجهزة المحمولة بخادم الأجهزة المحمولة Exchange](#)

[تكوين خادم ويب خدمات معلومات الإنترنت](#)

[التثبيت المحلي لخادم الأجهزة المحمولة Exchange](#)

[التثبيت عن بُعد لخادم الأجهزة المحمولة Exchange](#)

[نشر نظام للإدارة باستخدام يرو توكول iOS MDM](#)

[تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM](#)

[تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الوضع غير التفاعلي](#)

[سيناريو هات نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM](#)

[نظام النشر المبسط](#)

[نظام النشر الذي يتضمن تفويض Kerberos مقيد \(KCD\)](#)

[استخدام خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بواسطة العديد من الخوادم الافتراضية](#)

[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 المقيد \(KCD\)](#)

[استخدام مر اسلة Google Firebase Cloud](#)

[التكامل مع البنية الأساسية للمفاتيح العامة](#)

[Kaspersky Security Center Web Server](#)

[تثبيت Kaspersky Security Center](#)

[الإعداد للثبيت](#)

[حسابات للعمل باستخدام نظام إدارة قواعد البيانات \(DBMS\)](#)

[السيناريو: مصادقة خادم Microsoft SQL](#)

[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 14 Web Console](#)

[الخطوة 4. تحديد 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 14 Web Console](#)
- [الخطوة 5. تحديد 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 الخاص بالاتصال بالأجهزة المحمولة](#)
- [الخطوة 15. تحديد مكونات الإدارة الإضافية للتطبيق](#)
- [الخطوة 16. فك وتثبيت الملفات على القرص الثابت](#)
- [نشر مجموعة تجاوز الفشل من Kaspersky](#)
- [سيناريو: نشر مجموعة تجاوز الفشل من Kaspersky](#)
- [حول مجموعة تجاوز الفشل من Kaspersky](#)
- [تحضير خادم ملف لمجموعة تجاوز الفشل من Kaspersky](#)
- [تحضير العقد لنظام مجموعة تجاوز الفشل من Kaspersky](#)
- [تثبيت Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky](#)
- [بدء تشغيل مهمة وإيقافها يدويًا](#)
- [تثبيت خادم الإدارة على نظام مجموعة تجاوز الفشل](#)
- [الخطوة 1. مراجعة اتفاقية الترخيص وسياسة الخصوصية](#)
- [الخطوة 2. تحديد نوع التثبيت على نظام مجموعة](#)
- [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. تحديد 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 الخاص بالاتصال بالأجهزة المحمولة](#)
- [الخطوة 19. فك وتثبيت الملفات على القرص الثابت](#)
- [تثبيت خادم الإدارة في الوضع غير التفاعلي](#)
- [تثبيت وحدة تحكم الإدارة على محطة عمل المسؤول](#)
- [التغييرات في النظام بعد تثبيت Kaspersky Security Center](#)
- [إزالة التطبيق](#)
- [حول ترقيبة Kaspersky Security Center](#)
- [ترقيبة Kaspersky Security Center من إصدار سابق](#)
- [ترقيبة Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky](#)

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 والمنصات

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 إدارة 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

توصيل الأجهزة خارج المكتب

السيناريو: توصيل الأجهزة الموجودة خارج المكتب عن طريق بوابة الاتصال

حول توصيل الأجهزة خارج المكتب

توصيل أجهزة الكمبيوتر المكتبية الخارجية بخادم الإدارة

حول ملفات التعريف الخاصة باتصال المستخدمين المتواجدين خارج المكتب

إنشاء ملف تعريف خاص باتصال المستخدمين المتواجدين خارج المكتب

حول تغيير عميل الشبكة إلى خوادم إدارة أخرى

إنشاء قاعدة تغيير عميل شبكة حسب موقع الشبكة

تشفير الاتصال مع SSL/TLS

إخطارات الأحداث

تكوين إخطارات الحدث

إخطارات الاختيار

إخطارات الحدث التي يتم عرضها بواسطة الملف التنفيذي

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

حول قيود الوظائف الرئيسية

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 العملية في مجموعة الإدارة

تثبيت تطبيق من خلال سياسات مجموعة Active Directory

تثبيت التطبيقات على خوادم الإدارة الثانوية

تثبيت التطبيقات باستخدام معالج التثبيت عن بُعد

عرض تقرير نشر الحماية

إزالة التطبيقات عن بُعد

الإزالة عن بُعد لتطبيق من الأجهزة العملية الخاصة بمجموعة الإدارة

الإزالة عن بُعد للتطبيق من الأجهزة المحددة

العمل باستخدام حزم التثبيت

إنشاء حزمة توزيع

إنشاء حزم تثبيت مستقلة

إنشاء 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 المُحدّثة

تحضير جهاز التثبيت عن بُعد. الأداة المساعدة riprep.exe

تحضير الجهاز للتثبيت عن بُعد في الوضع التفاعلي

تحضير الجهاز للتثبيت عن بُعد في الوضع غير التفاعلي

إعداد جهاز يعمل بنظام Linux لتثبيت عميل الشبكة 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 الترخيص قيد الاستخدام
إضافة مفتاح ترخيص إلى مستودع خادم الإدارة
حذف 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
تكوين حماية الشبكة
السيناريو: تكوين حماية الشبكة
نشر وإعداد السياسة: نهج مركّز على الجهاز
حول نهج إدارة الأمان المركّز على الجهاز والمركّز 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 موروثّة 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
مرافقة 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
معالج تغيير كلمة مرور المهام

الخطوة 1. تحديد بيانات الاعتماد

الخطوة 2. اختيار إجراء لاتخاذ

الخطوة 3. عرض النتائج

إنشاء تسلسل هرمي لمجموعات الإدارة التابعة لخدم 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 موروث في مجموعة فرعية

تنشيط سياسة

تنشيط سياسة تلقائيًا بعد حدث انتشار الفيروسات

تطبيق سياسة الوجود خارج المكتب

تعديل سياسة التراجع عن التغييرات

مقارنة السياسات

حذف سياسة

نسخ سياسة

تصدير سياسة

استيراد سياسة

تحويل السياسات

إدارة ملفات تعريف السياسة

حول ملف 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 لتنصيب 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: سيناريو

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 المُنزَّلة

تكوين سياسات الاختبار والمهام الإضافية

عرض التحديثات المُنزَّلة

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 التلقائي لمكونات Kaspersky Security Center

تمكين وتعطيل التحديث و التصحيح التلقائيين لمكونات [Kaspersky Security Center](#).

[التوزيع التلقائي للتحديثات](#)

[توزيع التحديثات تلقائياً على الأجهزة العميلة](#)

[توزيع التحديثات تلقائياً على خوادم الإدارة الثانوية](#)

[تعيين نقاط التوزيع تلقائياً](#)

[تعيين نقطة توزيع لجهاز يدوياً](#)

[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](#)

[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. تحديث 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 يدوياً](#)

[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 بالبرامج](#)

[عرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة](#)

[فحص التطبيقات بحثاً 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](#)

[السيناريو: إدارة التطبيق](#)

[إنشاء فئات التطبيق من أجل سياسات Kaspersky Endpoint Security for Windows](#)

[إنشاء فئة تطبيق مضافاً إليها المحتوى يدوياً](#)

[إنشاء فئة تطبيق مضافاً إليها المحتوى تلقائياً](#)

إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق

تكوين إدارة بدء تشغيل التطبيق على الأجهزة العملية

عرض نتائج التحليل الإحصائي لقواعد بدء التشغيل المطبقة على الملفات التنفيذية

عرض سجل التطبيقات

تغيير وقت بدء تخزين البرامج

حول إدارة مفاتيح 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

إشارات حركة المرور 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 قالب 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 ل خادم 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 وفقاً لإعدادات مستوردة

إزالة أجهزة من مجموعات الإدارة في تحديد

مراقبة تثبيت التطبيقات وإلغاء تثبيتها

أنواع الأحداث

بنية البيانات لوصف نوع الحدث

أحداث خادم الإدارة

الأحداث الحرجة لخادم الإدارة

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

أحداث التحذير لخادم الإدارة

الأحداث المعلومة لخدمة الإدارة

أحداث عميل الشبكة

أحداث الخلل الوظيفي لعميل الشبكة

أحداث تحذير عميل الشبكة

الأحداث المعلومة 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 المعلومة لخدمة الأجهزة المحمولة التي تعمل بنظام iOS MDM

أحداث خادم الأجهزة المحمولة Exchange

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة Exchange

الأحداث المعلومة لخدمة الأجهزة المحمولة Exchange

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 وبيانات الاتصال

التكوين القياسي لنقاط التوزيع: مكتب واحد

التكوين القياسي لنقاط التوزيع: مكاتب صغيرة متعددة بعيدة

تعيين جهاز مُدار يعمل كنقطة توزيع

توصيل شريحة شبكة جديدة باستخدام أجهزة Linux

توصيل جهاز Linux للعمل كإدارة في منطقة الأجهزة الموصولة مباشرة بالإنترنت

اتصال جهاز Linux بخادم الإدارة عبر أحد بوابات الاتصال

إضافة بوابة اتصال في منطقة الأجهزة الموصولة مباشرة بالإنترنت للعمل كنقطة توزيع

تعيين نقاط التوزيع تلقائيًا

حول التثبيت المحلي لعميل الشبكة على جهاز مُحدد للعمل كنقطة توزيع

حول استخدام نقطة توزيع كإدارة اتصال

إضافة نطاقات IP لقائمة النطاقات التي تم فحصها الخاصة بنقطة 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 بعنوانين IP للاتصال بخادم الإدارة
استخدام الأداة المساعدة klsconfig 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
إيجاد الحلول لمشكلات عقد خادم الإدارة
عرض وتعديل إعدادات خادم إدارة
ضبط الإعدادات العامة لخادم الإدارة
إعدادات وإجهة 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
إنشاء مهمة نسخ احتياطي للبيانات
الأداة المساعدة لنسخ البيانات احتياطيًا واستعادتها (klbackup)
النسخ الاحتياطي للبيانات واستعادتها في الوضع التفاعلي
النسخ الاحتياطي للبيانات واستعادتها في الوضع غير التفاعلي
نقل خادم إدارة إلى جهاز آخر
تجنب التعارض بين العديد من خوادم الإدارة
المصادقة الثنائية
السيناريو: تكوين المصادقة الثنائية لجميع المستخدمين
عن المصادقة الثنائية
تمكين المصادقة الثنائية لحسابك الخاص
تمكين المصادقة الثنائية لجميع المستخدمين
تعطيل المصادقة الثنائية لحساب مستخدم
تعطيل المصادقة الثنائية لجميع المستخدمين
استثناء الحسابات من عملية المصادقة الثنائية
تحرير اسم مُصدر رمز الأمان
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 العملية
توصيل الأجهزة العملية بخادم الإدارة
اتصال جهاز عميل بخادم الإدارة يدويًا. الأداة المساعدة Klmover

نقل اتصال أحد الأجهزة العميلة بخادم الإدارة

الاتصال البعيد بسطح مكتب جهاز عميل

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

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

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 مستخدمين

[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 وكيل 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 وEAS](#)
[تمكين إدارة الجهاز المحمول](#)
[تعديل إعدادات إدارة الجهاز المحمول](#)
[تعطيل إدارة الجهاز المحمول](#)
[العمل مع الأوامر للأجهزة المحمولة](#)
[الأوامر لإدارة الجهاز المحمول](#)
[استخدام مرسلات Google Firebase Cloud](#)
[إرسال أوامر](#)
[عرض حالات الأوامر في سجل الأمر](#)
[جار العمل بشهادات الأجهزة المحمولة](#)
[بدء معالج تثبيت الشهادة](#)
[الخطوة 1. تحديد نوع الشهادة](#)
[الخطوة 2. تحديد نوع الجهاز](#)

[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. جاري 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 الأجهزة المحمولة في Exchange ActiveSync](#)

[إضافة ملف تعريف الإدارة](#)

[إزالة ملف تعريف الإدارة](#)

[التعامل مع سياسات Exchange ActiveSync](#)

[تكوين نطاق الفحص](#)

[العمل باستخدام أجهزة EAS](#)

[عرض معلومات حول جهاز EAS](#)

[قطع اتصال جهاز EAS من الإدارة](#)

[حقوق المستخدم لإدارة الأجهزة المحمولة Exchange ActiveSync](#)

[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 الثنائية 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](#)

[جزم 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 المفعله"](#)

[\(Kaspersky Security Network \(KSN](#)

[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 كوكيل KSN](#)

[التبديل بين التعليمات عبر الإنترنت والتعليمات دون الاتصال به](#)

[تصدير الأحداث إلى أنظمة SIEM](#)

[السيناريو: تكوين تصدير الحدث إلى نظام 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](#)

[حول تصدير الأحداث باستخدام تنسيق Syslog](#)

[تصدير الأحداث باستخدام تنسيقات CEF وLEEF](#)

[تكوين Kaspersky Security Center لتصدير الأحداث إلى نظام SIEM](#)

[تصدير الأحداث مباشرة من قاعدة البيانات](#)

[إنشاء استعلام SQL باستخدام أداة klsq2 المساعدة](#)

[مثال لاستعلام SQL في أداة klsq2 المساعدة](#)

[عرض اسم قاعدة بيانات Kaspersky Security Center](#)

[عرض نتائج التصدير](#)

[استخدام SNMP في إرسال الإحصاءات إلى تطبيقات الأطراف الخارجية](#)

[عمل 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 مستخدم IAM لمثلثات Amazon EC2](#)

[التأكد من أن خادم إدارة Kaspersky Security Center لديه الأدونات للعمل مع خدمات AWS](#)

[إنشاء دور IAM لخادم الإدارة](#)

[إنشاء حساب مستخدم IAM للعمل مع Kaspersky Security Center](#)

[إنشاء دور IAM لتنصيب التطبيقات على مثلثات Amazon EC2](#)

[استخدام Amazon RDS](#)

[إنشاء مثلث Amazon RDS](#)

[إنشاء مجموعة خيارات لمثلث Amazon RDS](#)

[تعديل مجموعة الخيارات](#)

[تعديل الأدونات لدور IAM لمثلث 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 اشتر الك 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 لمثلث MySQL](#)

[المتطلبات الأساسية للأجهزة العملية في بيئة السحابة والتي تكون لازمة للعمل مع Kaspersky Security Center](#)

[إنشاء حزم التنصيب المطلوبة لمعالج تكوين بيئة السحابة](#)

[معالج تكوين بيئة السحابة](#)

[حول معالج تكوين بيئة السحابة](#)

[الخطوة 1. تحديد طريقة تفعيل التطبيق](#)

[الخطوة 2. تحديد بيئة السحابة](#)

[الخطوة 3. التحويل 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 \(بيئة السحابة\)](#)
- [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](#)

[استخدام البرامج النصية للنشر لنشر تطبيقات الأمان](#)

[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](#)

[نافذة طريقة إخطار المستخدم](#)

[القسم عام](#)

[نافذة تحديد الجهاز](#)

[نافذة تحديد اسم الكائن الجديد](#)

[قسم فئات التطبيق](#)

[ميزات استخدام وإجهاة 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 بتنصيب 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 في أنظمة التشغيل Windows و macOS و Linux: المقارنة](#)

[Kaspersky Security Center 14 Web Console](#)

[حول Kaspersky Security Center 14 Web Console](#)

[متطلبات الأجهزة والبرامج لـ Kaspersky Security Center 14 Web Console](#)

[نشر مخطط خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console](#)

[المنافذ المستخدمة بواسطة وحدة تحكم الويب لـ Kaspersky Security Center 14 Web Console](#)

[السيناريو: تثبيت وإعداد مبدئي لـ Kaspersky Security Center 14 Web Console](#)

[التثبيت:](#)

[تثبيت نظام إدارة قواعد البيانات](#)

[تكوين خادم MariaDB x64 للعمل مع Kaspersky Security Center 14](#)

[تكوين خادم MySQL x64 للعمل مع Kaspersky Security Center 14](#)

[تثبيت Kaspersky Security Center \(تثبيت قياسي\)](#)

[تثبيت Kaspersky Security Center 14 Web Console](#)

[تثبيت Kaspersky Security Center 14 Web Console على منصات Linux](#)

[تثبيت Kaspersky Security Center 14 Web Console على منصات Linux](#)

[معلومات تثبيت Kaspersky Security Center 14 Web Console](#)

[ترقية Kaspersky Security Center Web Console](#)

[شهادات للعمل مع Kaspersky Security Center 14 Web Console](#)

[إعادة إصدار شهادة Kaspersky Security Center Web Console](#)

[استبدال شهادة Kaspersky Security Center 14 Web Console](#)

[تحديد الشهادات لخادم الإدارة الموثوقة](#)

[تحويل شهادة PFX إلى تنسيق PEM](#)

[التحويل إلى Kaspersky Security Center Cloud Console](#)

[تسجيل الدخول إلى Kaspersky Security Center 14 Web Console وتسجيل الخروج](#)

[إدارة الهوية والوصول في Kaspersky Security Center 14 Web Console](#)

[حول إدارة الهوية والوصول](#)

[تمكين إدارة الهوية والوصول: سيناريو](#)

[تكوين إدارة الهوية والوصول في Kaspersky Security Center 14 Web Console](#)

[تسجيل وإجهة ويب Kaspersky Industrial CyberSecurity for Networks في Kaspersky Security Center 14 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](#)

[الإعداد الأولي لـ Kaspersky Security Center 14 Web Console](#)

[معالج البدء السريع \(Kaspersky Security Center 14 Web Console\)](#)

[الخطوة 1. تحديد إعدادات اتصال الإنترنت](#)

[الخطوة 2. جار تنزيل التحديثات المطلوبة](#)

[الخطوة 3. تحديد مناطق الحماية والمنصات](#)

[الخطوة 4. اختبار 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

حول توصيل الأجهزة خارج المكتب

توصيل أجهزة الكمبيوتر 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

بدء معالج نشر الحماية

الخطوة 1. تحديد حزمة التثبيت

الخطوة 2. تحديد طريقة لتوزيع ملف المفاتيح أو رمز التنشيط

الخطوة 3. تحديد إصدار عميل الشبكة

الخطوة 4. تحديد الأجهزة

الخطوة 5. تحديد إعدادات مهمة التثبيت عن بُعد

الخطوة 6. إدارة إعادة التشغيل

الخطوة 7. إزالة التطبيقات غير المتوافقة قبل التثبيت

الخطوة 8. نقل الأجهزة إلى الأجهزة المُدارة

الخطوة 9. تحديد الحسابات للوصول إلى الأجهزة

الخطوة 10. بدء التثبيت

تكوين خادم الإدارة

تكوين اتصال Kaspersky Security Center 14 Web Console بخادم الإدارة

عرض سجل الاتصالات بخادم 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

حذف خادم إدارة افتراضي

تغيير خادم الإدارة للأجهزة العملية

تمكين حماية الحساب من تعديل غير مصرح به

المصادقة الثنائية

السيناريو: تكوين المصادقة الثنائية لجميع المستخدمين

عن المصادقة الثنائية

[تمكين المصادقة الثنائية لحسابك الخاص](#)
[تمكين المصادقة الثنائية لجميع المستخدمين](#)
[تعطيل المصادقة الثنائية لحساب مستخدم](#)
[تعطيل المصادقة الثنائية لجميع المستخدمين](#)
[استثناء الحسابات من عملية المصادقة الثنائية](#)
[إنشاء مفتاح سري جديد](#)

[تحرير اسم مُصدر رمز الأمان](#)
[النسخ الاحتياطي والاستعادة لبيانات خادم الإدارة](#)
[إنشاء مهمة نسخ احتياطي للبيانات](#)

[نشر تطبيقات Kaspersky من خلال Kaspersky Security Center 14 Web Console](#)

[السيناريو: نشر تطبيقات Kaspersky من خلال Kaspersky Security Center 14 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 نجاح Kaspersky Endpoint Security for Windows](#)

[إنشاء حزم تثبيت مستقلة](#)

[عرض قائمة حزم التثبيت المستقلة](#)

[إنشاء حزمة توزيع مخصصة](#)

[تحديد إعدادات التثبيت عن بُعد على أجهزة Unix](#)

[إدارة الأجهزة المحمولة](#)

[استبدال تطبيقات الأمان من جهة خارجية](#)

[اكتشاف الأجهزة المتصلة بالشبكة](#)

[سيناريو: اكتشاف الأجهزة المتصلة بالشبكة](#)

[اكتشاف الأجهزة](#)

[استقصاء شبكة Windows](#)

[استقصاء Active Directory](#)

[استقصاء نطاق IP](#)

[إضافة نطاق IP وتعديله](#)

[استطلاع شبكة لا تتطلب تكويناً](#)

[تكوين قواعد الاستيقاظ للأجهزة غير المخصصة](#)

[تطبيقات Kaspersky: الترخيص والتنشيط](#)

[ترخيص التطبيقات المُدارة](#)

[إضافة مفتاح ترخيص إلى مستودع خادم الإدارة](#)

[نشر مفتاح ترخيص على الأجهزة العميلة](#)

[التوزيع التلقائي لمفتاح الترخيص](#)

[عرض معلومات حول مفاتيح الترخيص قيد الاستخدام](#)

[حذف مفتاح ترخيص من المستودع](#)

[إلغاء الموافقة على اتفاقية ترخيص المستخدم النهائي](#)

[تجديد ترخيص تطبيقات Kaspersky](#)

[استخدام Kaspersky Marketplace لاختبار حلول أعمال Kaspersky](#)

[تكوين حماية الشبكة](#)

[السيناريو: تكوين حماية الشبكة](#)

[حول نهج 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](#)

[الإعدادات اليدوية 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

منح الوصول دون اتصال إلى الجهاز الخارجي المحظور بواسطة التحكم في الجهاز

إزالة تحديثات تطبيقات أو برامج عن بُعد

التراجع عن كائن إلى مراجعة سابقة

تغيير أولوية قواعد نقل الجهاز

المهام

حول المهام

حول نطاق المهمة

إنشاء مهمة

بدء مهمة يدويًا

عرض قائمة المهام

إعدادات المهمة العامة

بدء معالج تغيير كلمة مرور المهام

الخطوة 1. تحديد بيانات الاعتماد

الخطوة 2. اختيار إجراء لاتخاذ

الخطوة 3. عرض النتائج

إدارة الأجهزة العملية

إعدادات جهاز مدار

إنشاء مجموعات إدارة

إضافة أجهزة إلى مجموعة إدارة يدويًا

نقل أجهزة إلى مجموعة إدارة يدويًا

إنشاء قواعد نقل الجهاز

نسخ قواعد نقل الجهاز

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

تحديثات الأجهزة

إنشاء تحديد جهاز

تكوين تحديد جهاز

علامات الجهاز

حول 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

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

عرض مخطط حالة توزيع السياسة

تنشيط سياسة تلقائيًا بعد حدث انتشار الفيروسات

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 التشفير 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

تكوين حقوق الوصول إلى ميزات التطبيق. التحكم في الوصول على أساس الدور.

حقوق الوصول إلى ميزات التطبيق

أدوار المستخدم المحددة مسبقًا

إضافة حساب خاص للمستخدم داخلي

إنشاء مجموعة مستخدمين

تحرير حساب خاص للمستخدم داخلي

تحرير مجموعة مستخدمين

إضافة حسابات المستخدمين إلى مجموعة داخلية

تعيين مستخدم كمالك للجهاز

حذف مستخدم أو مجموعة أمان

إنشاء دور للمستخدم

تحرير دور المستخدم

تحرير نطاق دور المستخدم

حذف دور مستخدم

[رابط ملفات تعريف السياسة بأدوار](#)

[إدارة الكائنات في Kaspersky Security Center 14 Web Console](#)

[إضافة وصف للمراجعة](#)

[حذف كائن](#)

[\(Kaspersky Security Network \(KSN](#)

[حول KSN](#)

[إعداد الوصول إلى Kaspersky Security Network](#)

[تمكين وتعطيل KSN](#)

[عرض بيان KSN المقبول](#)

[قبول بيان KSN محدث](#)

[التحقق مما إذا كانت نقطة التوزيع تعمل كوكيل 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 لتنزيل التحديثات إلى مستودع خادم الإدارة](#)

[عرض التحديثات المُنزلة](#)

[التحقق من التحديثات المُنزلة](#)

[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 وويبات 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](#)

[حول تطبيقات الجهات الخارجية](#)

[تثبيت تحديثات برامج الجهات الخارجية](#)

[السيناريو: تحديث برامج الجهات الخارجية](#)

[حول تحديثات 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 تثبيت التحديثات](#)

[إنشاء مهمة تثبيت تحديثات Windows Update](#)

[عرض معلومات حول تحديثات برامج الجهات الخارجية المتوفرة](#)

[تصدير قائمة تحديثات البرنامج 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 المدارة](#)
[تصدير قائمة بأحداث التشفير إلى ملف نص](#)
[تجاهل الثغرات الأمنية في البرامج](#)
[إدارة التطبيقات المشغلة على أجهزة العميل](#)
[السيناريو: إدارة التطبيق](#)
[حول التحكم في التطبيقات](#)
[الحصول على قائمة بالتطبيقات المثبتة على أجهزة العميل وعرضها](#)
[الحصول على قائمة بالملفات التنفيذية المخزنة على أجهزة العميل وعرضها](#)
[إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا](#)
[إنشاء فئة تطبيق تتضمن ملفات تنفيذية من أجهزة محددة](#)
[إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد](#)
[عرض قائمة فئات التطبيق](#)
[تكوين التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows](#)
[إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق](#)
[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](#)
[حول 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](#)

جار تكوين وضع لوحة المعلومات فقط

تقارير

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 واختبارات الفعالية

استخدام تحديبات الحدث

إنشاء تحديد حدث

إنشاء تحديد حدث

عرض قائمة تحديد الحدث

عرض تفاصيل حدث

تصدير الأحداث إلى ملف

عرض تاريخ كائن من حدث

حذف الأحداث

حذف تحديبات الحدث

تعيين مدة التخزين لحدث

أنواع الأحداث

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

أحداث خادم الأجهزة المحمولة Exchange

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة Exchange

الأحداث المعلوماتية الخاصة بخادم الأجهزة المحمولة Exchange

حظر الأحداث المتكررة

حول حظر الأحداث المتكررة

إدارة حظر الأحداث المتكررة

إزالة حظر الأحداث المتكررة

تلقي الأحداث من Microsoft Exchange Servers لـ Kaspersky Security

الإخطارات وحالات الجهاز

استخدام الإخطارات

عرض الإخطارات التي تظهر على الشاشة

حول حالات الجهاز

تكوين تغيير 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](#)

[تسجيل نشاط Kaspersky Security Center 14 Web Console](#)

[التكامل بين Kaspersky Security Center والحلول الأخرى](#)

[تكوين الوصول إلى KATA/KEDR Web Console](#)

[جارٍ إنشاء اتصال في الخلفية](#)

[تصدير الأحداث إلى أنظمة SIEM](#)

[السيناريو: تكوين تصدير الحدث إلى نظام 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 للتصدير 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](#)

[حول تصدير الأحداث باستخدام تنسيق Syslog](#)

[تكوين Kaspersky Security Center لتصدير الأحداث إلى نظام SIEM](#)

[تصدير الأحداث مباشرة من قاعدة البيانات](#)

[إنشاء استعلام SQL باستخدام أداة klsq2 المساعدة](#)

[مثال لاستعلام SQL في أداة klsq2 المساعدة](#)

[عرض اسم قاعدة بيانات Kaspersky Security Center](#)

[عرض نتائج التصدير](#)

[العمل باستخدام Kaspersky Security Center 14 Web Console في بيئة السحابة](#)

[معالج تكوين بيئة سحابة Kaspersky Security Center 14 Web Console](#)

[الخطوة 1. قراءة المعلومات حول المعالج](#)

[الخطوة 2. ترخيص التطبيق](#)

[الخطوة 3. تحديد بيئة السحابة والمصادقة](#)

[الخطوة 4. استنقاء القطاع، تكوين المزامنة مع السحابة واختبار إجراءات إضافية](#)

[الخطوة 5. تكوين Kaspersky Security Network لصالح Kaspersky Security Center](#)

[الخطوة 6. إنشاء تكوين أولي للحماية](#)

[استنقاء مقطع الشبكة عبر Kaspersky Security Center 14 Web Console](#)

[إضافة اتصالات لاستنقاء قطاع السحابة](#)

[حذف اتصال خاص باستنقاء قطاع السحابة](#)

[تكوين جدول الاستنقاء عبر Kaspersky Security Center 14 Web Console](#)

[عرض نتائج استنقاء قطاع السحابة عبر Kaspersky Security Center 14 Web Console](#)

[عرض خصائص الأجهزة السحابية عبر Kaspersky Security Center 14 Web Console](#)

[التزامن مع السحابة: تكوين القاعدة المتحركة](#)

[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 لأحد التطبيقات وتنزيل النتائج](#)
[تشغيل تطبيق على جهاز عميل](#)
[تنزيل وحذف الملفات من العزل والنسخ الاحتياطي](#)
[تنزيل الملفات من العزل والنسخ الاحتياطي](#)
[حول إزالة الكائنات من العزل أو النسخ الاحتياطي أو مستودعات التهديدات النشطة](#)

[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 العملية](#)

[الإعداد البدوي 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 الحدوث](#)

[الإعداد البدوي المهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security](#)

[الإعداد البدوي للمهمة الجماعية لفحص جهاز باستخدام Kaspersky Endpoint Security](#)

[جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة](#)

[الإعداد البدوي 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](#)

[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](#)

[معلومات تثبيت خادم الإدارة](#)

[معلومات تثبيت عميل الشبكة](#)

[البنية التحتية الافتراضية](#)

[نصائح لتقليل الحمل على الأجهزة الظاهرة](#)

[دعم الأجهزة الظاهرة الديناميكية](#)

[دعم نسخ الأجهزة الظاهرة](#)

[دعم عودة نظام الملفات الخاص بالأجهزة المثبت 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 المقيد \(KCD\)](#)

[استخدام مراسلة Google Firebase Cloud](#)

[التكامل مع البنية الأساسية للمفاتيح العامة](#)

[Kaspersky Security Center Web Server](#)

[عمل روتيني آخر](#)

[إشارات حركة المرور 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 \(مع أويديون استخدام ميزة إدارة الثغرات الأمنية والتصحيحات\)](#)

[حساب رقم وتكوين خوادم الإدارة](#)

[حسابات نقاط التوزيع ويوإيات الاتصال](#)

[المتطلبات لنقطة توزيع](#)

[حساب عدد نقاط التوزيع وتكوينهم](#)

[حساب عدد يوإيات 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 قاعدة البيانات](#)

[مهام جماعية لتحديث Kaspersky Endpoint Security](#)

[مهمة مخزون البرنامج](#)

[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](#)

[مصادر المعلومات المتعلقة بالتطبيق](#)

[مسرود المصطلحات](#)

[\(AWS Application Program Interface \(AWS API](#)

[AWS Management Console](#)

[HTTPS](#)

[JavaScript](#)

[Kaspersky Private Security Network \(شبكة KSN الخاصة\)](#)

[Kaspersky Security Center Administrator](#)

[Kaspersky Security Center Operator](#)

[Kaspersky Security Center Web Server](#)

[\(Kaspersky Security Network \(KSN](#)

[SSL](#)

[Update](#)

[أداة التحقق من سلامة نظام \(SHV\) \(Kaspersky Security Center\)](#)

[إعدادات البرنامج](#)

[إعدادات المهمة](#)

[استعادة بيانات خادم الإدارة](#)

[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 \(IAM\)](#)
[انتشار الفيروس](#)
[يواية الاتصال](#)
[بيئة السحابة](#)
[جهاز EAS](#)
[جهاز iOS MDM](#)
[جهاز KES](#)
[جهاز حماية UEFI](#)
[حالة الحماية](#)
[حالة حماية الشبكة](#)
[حزمة التثبيت](#)
[حقوق المسؤول](#)
[خادم الأجهزة المحمولة Exchange](#)
[خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM](#)
[خادم الإدارة](#)
[خادم الإدارة الافتراضي](#)
[خادم الإدارة الرئيسي](#)
[خادم الجهاز المحمول](#)
[خدمات تحديث خادم WSUS \(Windows\)](#)
[خطورة الحدث](#)
[خوادم تحديث Kaspersky](#)
[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](#)
[مجموعة الدور](#)
[محطة عمل المسؤول](#)
[مسؤول العميل](#)
[مسؤول موفر الخدمة](#)
[مستخدم IAM](#)
[مستخدمين داخليين](#)
[مستودع الأحداث](#)
[مستوى أهمية التصحيح](#)

مفتاح اشتراك إضافي
مفتاح مفعّل
مفتاح وصول AWS IAM
مكون الإدارة الإضافي
ملف التعريف
ملف المفتاح
ملف تعريف iOS MDM
ملف تعريف التزويد
ملف تعريف التكوين
منطقة الأجهزة الموصولة مباشرة بالإنترنت (DMZ)
مهمة جماعية
مهمة لأجهزة محددة
مهمة محلية
موفر خدمة الحماية ضد الفيروسات
نسخ احتياطي لبيانات خادم الإدارة
نقطة توزيع
وحدة تحكم الإدارة
وكيل المصادقة
معلومات حول التعليمات البرمجية الخاصة بطرف ثالث
إشعارات العلامة التجارية
المشكلات المعروفة

<p><u>تكوين حماية الشبكة</u> إدارة أمن المؤسسة</p>		<p><u>ما الجديد</u> اكتشف كل ما هو جديد في أحدث إصدار للتطبيق.</p>	
<p><u>تطبيقات Kaspersky. تحديث قواعد البيانات والوحدات النمطية للبرامج</u> الحفاظ على موثوقية نظام الحماية.</p>		<p><u>متطلبات الأجهزة والبرامج</u> تحقق أياً من أنظمة التشغيل وإصدارات التطبيق مدعومة.</p>	
<p><u>المراقبة وإعداد التقارير</u> عرض البنية الأساسية الخاصة بك، وحالات الحماية والإحصائيات.</p>		<p><u>النشر والإعداد الأولي</u> تخطيط استخدام الموارد، وتثبيت خادم الإدارة، وتثبيت عميل الشبكة، وتطبيقات الأمان على الأجهزة العميلة وجمع الأجهزة في مجموعات الإدارة.</p>	
<p><u>استبدال تطبيقات الأمان من جهة خارجية</u> تعرف على طرق لإلغاء تثبيت التطبيقات غير المتوافقة.</p>		<p><u>اكتشاف الأجهزة المتصلة بالشبكة</u> اكتشف الأجهزة الجديدة والموجودة على شبكة مؤسستك.</p>	
<p><u>تعديل نقاط التوزيع وبوابات الاتصال</u> تكوين نقاط التوزيع.</p>		<p><u>تطبيقات Kaspersky. النشر المركزي</u> نشر تطبيقات Kaspersky.</p>	
<p><u>أفضل ممارسات موفري الخدمة (التعليمات عبر الإنترنت فقط)</u> تعرف على التوصيات حول كيفية نشر التطبيق وتكوينه واستخدامه، بالإضافة إلى شرح طرق حل المشكلات النمطية عند عمل التطبيق.</p>		<p><u>ترقية Kaspersky Security Center من إصدار سابق</u> ترقية Kaspersky Security Center 14 من إصدار سابق.</p>	
<p><u>دليل القياس (التعليمات عبر الإنترنت فقط)</u> 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.</p>		<p><u>تطبيقات Kaspersky. الترخيص والتفعيل</u> تفعيل تطبيقات Kaspersky في بضع خطوات.</p>	
<p><u>إدارة الثغرات الأمنية والتصحيحات</u> ابحث عن الثغرات الأمنية وأصلحها في برامج الجهات الخارجية.</p>		<p><u>تصدير الأحداث إلى أنظمة SIEM</u> قم بتكوين تصدير الأحداث إلى أنظمة SIEM لتحليلها.</p>	
<p><u>العمل في بيئة السحابة</u> يمكن نشر Kaspersky Security Center في بيئات السحابة: منصة Amazon Web Services™، ومنصة Microsoft Azure™، ومنصة Google™ Cloud.</p>			

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 وكيل الشبكة على الأجهزة التي تعمل بنظام التشغيل Microsoft Windows 10 IoT Enterprise
- في تقرير التهديدات، يمكنك الآن تصفية قائمة التهديدات لعرض التهديدات التي تم اكتشافها بواسطة Cloud Sandbox.

لدى Kaspersky Security Center 14 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 المستخدم بتمكين هذا الوضع، تُعرض لوحة معلومات تتضمن مجموعة محددة مسبقاً 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 مؤخراً، أو قائمة التهديدات الأكثر شيوعاً في الشبكة.
- يدعم Kaspersky Security Center 14 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.

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، و عميل 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 تتجاوز الفشل من Kaspersky 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 Kaspersky](#) التالية:
- برنامج 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 لـ [Kaspersky Security Center 14 Web Console](#) ووحدة تحكم الإدارة القائمة على MMC.
- يمكنك الآن تلقي تصحيحات خادم الإدارة كحزمة توزيع، والتي يمكنك استخدامها في التحديثات المستقبلية للإصدارات الأحدث.
- تمت إضافة قسم جديد، وتثبيتات، لبرنامج Kaspersky Endpoint Detection and Response Optimum حتى برنامج Kaspersky Security Center 13.1 Web Console. تمت إضافة العديد من التطبيقات المصغرة الجديدة أيضاً 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 يتعين 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 لاحقاً 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 المراقبة والإبلاغ. يبيّن 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:

- المصادقة الثنائية المطبقة. يمكنك تمكين المصادقة الثنائية لتقليل مخاطر الوصول غير المصرح به إلى خادم 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 تكوين iOS MDM لضمان تحول سلس لأجهزة iOS المُدارة بعد انتهاء شهادة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.
- مجلد التطبيقات متعددة المستأجرين لم يعد معروضاً في وحدة تحكم الإدارة.

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.

حول Kaspersky Security Center

يحتوي هذا القسم على معلومات حول الغرض من Kaspersky Security Center وميزاته ومكوناته الرئيسية.

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. يُمكن التطبيق المسؤول من الوصول إلى المعلومات المفصلة حول مستوى أمن 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 لحوادim الإدارة لإدارة شبكة المؤسسة، بالإضافة إلى الشبكات الموجودة في المكاتب البعيدة أو مؤسسات العميل.
- المؤسسة العملية عبارة عن مؤسسة يقوم مزود الخدمة بضمان حمايتها ضد الفيروسات.
- قم بإنشاء ترتيب هرمي لمجموعات الإدارة لإدارة مجموعة محددة من الأجهزة العملية ككل.
- إدارة نظام الحماية ضد الفيروسات الذي تم إنشاؤه استنادًا إلى تطبيقات Kaspersky.
- إنشاء صور نظام التشغيل ونشرها على الأجهزة العملية عبر الشبكة، وإجراء تثبيت عن بُعد للتطبيقات بواسطة Kaspersky وبإباعي البرامج الأخرين.
- إدارة التطبيقات المثبتة على الأجهزة العملية عن بُعد بواسطة Kaspersky والموردين الأخرين. تثبيت التحديثات والعتور على الثغرات الأمنية وإصلاحها.
- تنفيذ نشر مركزي لمفاتيح الترخيص لتطبيقات Kaspersky على الأجهزة العملية 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.

مجموعة التوزيع

يمكنك شراء التطبيق عبر متاجر Kaspersky عبر الإنترنت (على سبيل المثال، من <https://www.kaspersky.com>) أو عبر الشركات الشريكة.

إذا قمت بشراء Kaspersky Security Center من متجر عبر الإنترنت، فيمكنك نسخ التطبيق من موقع ويب المتجر. يتم إرسال المعلومات المطلوبة لتنشيط التطبيق عبر البريد الإلكتروني بعد الدفع.

متطلبات الأجهزة والبرامج

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 جيجابايت. عند استخدام إدارة الثغرات الأمنية والتصحيحات، يجب توفير مساحة على القرص بمقدار 100 جيجابايت 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:

- Microsoft Windows 10 Enterprise 2015 LTSC 32 بت/64 بت
- Microsoft Windows 10 Enterprise 2016 LTSC 32 بت/64-بت
- Microsoft Windows 10 Enterprise 2019 LTSC 32 بت/64 بت
- Microsoft Windows 10 Pro RS5 (تحديث أكتوبر 2018، رقم 1809) 32 بت / 64 بت
- Microsoft Windows 10 Pro for Workstations RS5 (تحديث أكتوبر 2018، رقم 1809) 32 بت / 64 بت
- Microsoft Windows 10 Enterprise RS5 (تحديث أكتوبر 2018، رقم 1809) 32 بت / 64 بت
- Microsoft Windows 10 Education RS5 (تحديث أكتوبر 2018، رقم 1809) 32 بت / 64 بت
- Microsoft Windows 10 Pro 19H1 32 بت/64 بت

- 32 Microsoft Windows 10 Pro for Workstations 19H1 بت/64 بت
- 32 Microsoft Windows 10 Enterprise 19H1 بت/64 بت
- 32 Microsoft Windows 10 Education 19H1 بت/64 بت
- 32 Microsoft Windows 10 Home 19H2 بت/64 بت
- 32 Microsoft Windows 10 Pro for Workstations 19H2 بت/64 بت
- 32 Microsoft Windows 10 Enterprise 19H2 بت/64 بت
- 32 Microsoft Windows 10 Education 19H2 بت/64 بت
- Microsoft Windows 10 Home 20H1 (تحديث مايو 2020) 32 بت/64 بت
- Microsoft Windows 10 Pro 20H1 (تحديث مايو 2020) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 20H1 (تحديث مايو 2020) 32 بت/64 بت
- Microsoft Windows 10 Education 20H1 (تحديث مايو 2020) 32 بت/64 بت
- Microsoft Windows 10 Home 20H2 (تحديث أكتوبر 2020) 32 بت/64 بت
- Microsoft Windows 10 Pro 20H2 (تحديث أكتوبر 2020) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 20H2 (تحديث أكتوبر 2020) 32 بت/64 بت
- Microsoft Windows 10 Education 20H2 (تحديث أكتوبر 2020) 32 بت/64 بت
- Microsoft Windows 10 Home 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Pro 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Education 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Home 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Pro 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Education 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 11 Home بت 64
- Microsoft Windows 11 Pro بت 64
- Microsoft Windows 11 Enterprise 64 بت
- Microsoft Windows 11 Education 64 بت
- Microsoft Windows 8.1 Pro 32 بت / 64 بت

- Microsoft Windows 8.1 Enterprise 32 بت / 64 بت
- Microsoft Windows 8 Pro 32 بت / 64 بت
- Microsoft Windows 8 Enterprise 32 بت / 64 بت
- Microsoft Windows 7 Professional with Service Pack 1 والإصدارات الأعلى 32 بت / 64 بت
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 والإصدارات الأعلى 32 بت / 64 بت
- Windows Server 2008 R2 Standard with Service Pack 1 والإصدار الأعلى 64 بت
- Windows Server 2008 R2 with Service Pack 1 (جميع الإصدارات) 64 بت
- Windows Server 2012 Server Core 64 بت
- Windows Server 2012 Datacenter 64 بت
- Windows Server 2012 Essentials 64 بت
- Windows Server 2012 Foundation 64 بت
- Windows Server 2012 Standard 64 بت
- Windows Server 2012 R2 Server Core 64 بت
- Windows Server 2012 R2 Datacenter 64 بت
- Windows Server 2012 R2 Essentials 64 بت
- Windows Server 2012 R2 Foundation 64 بت
- Windows Server 2012 R2 Standard 64 بت
- Windows Server 2016 Datacenter (LTSB) 64 بت
- Windows Server 2016 Standard (LTSB) 64 بت
- Windows Server 2016 Server Core (Installation Option) (LTSB) 64 بت
- Windows Server 2019 Standard 64 بت
- Windows Server 2019 Datacenter 64 بت
- Windows Server 2019 Core 64 بت
- Windows Server 2022 Standard 64 بت
- Windows Server 2022 Datacenter 64 بت
- Windows Server 2022 Core 64 بت
- Windows Storage Server 2012 64 بت
- Windows Storage Server 2012 R2 64 بت

• Windows Storage Server 2016 64 بت

• Windows Storage Server 2019 64 بت

يتم دعم الأنظمة الأساسية الظاهرية التالية:

• VMware vSphere 6.7

• VMware vSphere 7.0

• VMware Workstation 16 Pro

• Microsoft Hyper-V Server 2012 64 بت

• Microsoft Hyper-V Server 2012 R2 64 بت

• Microsoft Hyper-V Server 2016 64 بت

• Microsoft Hyper-V Server 2019 64 بت

• Microsoft Hyper-V Server 2022 64 بت

• Citrix XenServer 7.1 LTSR

• Citrix XenServer 8.x

• Parallels Desktop 17

• Oracle VM VirtualBox 6.x (تسجيل الدخول لحساب Windows guest فقط)

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

• Microsoft SQL Server 2012 Express 64 بت

• Microsoft SQL Server 2014 Express 64 بت

• Microsoft SQL Server 2014 Express 64 بت

• Microsoft SQL Server 2017 Express 64 بت

• Microsoft SQL Server 2019 Express 64 بت

• Microsoft SQL Server 2014 (جميع الإصدارات) 64 بت

• Microsoft SQL Server 2016 (جميع الإصدارات) 64 بت

• Microsoft SQL Server 2017 (جميع الإصدارات) على Windows 64 بت

• Microsoft SQL Server 2017 (جميع الإصدارات) على Linux 64 بت

• Microsoft SQL Server 2019 (جميع الإصدارات) على Windows 64 بت (يتطلب إجراءات إضافية)

• Microsoft SQL Server 2019 (جميع الإصدارات) على Linux 64 بت (يتطلب إجراءات إضافية)

• قاعدة بيانات Microsoft Azure SQL

- جميع إصدارات خادم SQL Server المدعومة في المنصات السحابية Amazon RDS و Microsoft Azure
- مجتمع MySQL 5.7 32 بت/64 بت
- MySQL Standard Edition 8.0 (إصدار 8.0.20 فأحدث) 32 بت/64 بت
- MySQL Enterprise Edition 8.0 (إصدار 8.0.20 فأحدث) 32 بت/64 بت
- MariaDB 10.5.x 32 بت / 64 بت
- MariaDB 10.4.x 32 بت / 64 بت
- MariaDB 10.3.22 وأحدث 32 بت / 64 بت
- MariaDB Server 10.3 32 بت / 64 بت مع مشغل التخزين InnoDB
- MariaDB Galera Cluster 10.3 32 بت مع محرك تخزين InnoDB
- MariaDB 10.1.30 وأحدث 32 بت / 64 بت

يوصى باستخدام MariaDB 10.3.22 إذا كنت تستخدم إصدارًا سابقًا، فقد تستغرق مهمة تحديث أداء Windows أكثر من يوم واحد للعمل.

SIEM وأنظمة إدارة المعلومات الأخرى:

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

Kaspersky Security Center 14 Web Console

خادم Kaspersky Security Center 14 Web Console

الحد الأدنى لمتطلبات الجهاز:

- وحدة المعالجة المركزية: 4 مراكز معالجة وتردد تشغيلي بسعة 2.5 جيجاهرتز
- ذاكرة الوصول العشوائي: 8 جيجابايت
- مساحة القرص المتوفرة: 40 جيجابايت

أنظمة التشغيل التالية مدعومة:

- Microsoft Windows (لإصدارات 64-بت فقط):
- Microsoft Windows 10 Enterprise 2015 LTSC
- Microsoft Windows 10 Enterprise 2016 LTSC
- Microsoft Windows 10 Enterprise 2019 LTSC

- Microsoft Windows 10 Pro RS5 (تحديث أكتوبر 2018، رقم 1809)
- Microsoft Windows 10 Pro for Workstations RS5 (تحديث أكتوبر 2018، رقم 1809)
- Microsoft Windows 10 Enterprise RS5 (تحديث أكتوبر 2018، رقم 1809)
- Microsoft Windows 10 Education RS5 (تحديث أكتوبر 2018، رقم 1809)
- Microsoft Windows 10 Pro 19H1
- Microsoft Windows 10 Pro for Workstations 19H1
- Microsoft Windows 10 Enterprise 19H1
- Microsoft Windows 10 Education 19H1
- Microsoft Windows 10 Pro 19H2
- Microsoft Windows 10 Pro for Workstations 19H2
- Microsoft Windows 10 Enterprise 19H2
- Microsoft Windows 10 Education 19H2
- Microsoft Windows 10 Home 20H1 (تحديث مايو 2020)
- Microsoft Windows 10 Pro 20H1 (تحديث مايو 2020)
- Microsoft Windows 10 Enterprise 20H1 (تحديث مايو 2020)
- Microsoft Windows 10 Education 20H1 (تحديث مايو 2020)
- Microsoft Windows 10 Home 20H2 (تحديث أكتوبر 2020)
- Microsoft Windows 10 Pro 20H2 (تحديث أكتوبر 2020)
- Microsoft Windows 10 Enterprise 20H2 (تحديث أكتوبر 2020)
- Microsoft Windows 10 Education 20H2 (تحديث أكتوبر 2020)
- Microsoft Windows 10 Home 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Pro 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Education 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Home 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Pro 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Education 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت

- Microsoft Windows 11 Home •
- Microsoft Windows 11 Pro •
- Microsoft Windows 11 Enterprise •
- Microsoft Windows 11 Education •
- Windows Server 2012 Server Core •
- Windows Server 2012 Datacenter •
- Windows Server 2012 Essentials •
- Windows Server 2012 Foundation •
- Windows Server 2012 Standard •
- Windows Server 2012 R2 Server Core •
- Windows Server 2012 R2 Datacenter •
- Windows Server 2012 R2 Essentials •
- Windows Server 2012 R2 Foundation •
- Windows Server 2012 R2 Standard •
- (Windows Server 2016 Datacenter (LTSC) •
- (Windows Server 2016 Standard (LTSC) •
- (Windows Server 2016 Server Core (Installation Option) (LTSC) •
- Windows Server 2019 Standard 64 بت •
- Windows Server 2019 Datacenter 64 بت •
- Windows Server 2019 Core 64 بت •
- Windows Server 2022 Standard 64 بت •
- Windows Server 2022 Datacenter 64 بت •
- Windows Server 2022 Core 64 بت •
- Windows Storage Server 2012 64 بت •
- Windows Storage Server 2012 R2 64 بت •
- Windows Storage Server 2016 64 بت •
- Windows Storage Server 2019 64 بت •
- Linux (إصدارات 64 بت فقط): •

- (Debian GNU/Linux 11.x (Bullseye
- (Debian GNU/Linux 10.x (Buster
- (Debian GNU/Linux 9.x (Stretch
- (Ubuntu Server 20.04 LTS (Focal Fossa
- (Ubuntu Server 18.04 LTS (Bionic Beaver
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12 (جميع حزم الخدمات)
- SUSE Linux Enterprise Server 15 (جميع حزم الخدمات)
- SUSE Linux Enterprise Desktop 15 (حزمة الخدمة 3) ARM
- Astra Linux Special Edition 1.7 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي)
- Astra Linux Special Edition 1.6 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي)
- Astra Linux Common إصدار 2.12
- Alt Server 10
- Alt Server 9.2
- (Alt 8 SP Server (LKNV.11100-01
- (Alt 8 SP Server (LKNV.11100-02
- (Alt 8 SP Server (LKNV.11100-03
- Oracle Linux 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 إصدار معتمد

من بين منصات المحاكاة الافتراضية، يتم دعم Virtual Machine المستندة إلى Kernel لأنظمة التشغيل التالية:

- 64 Alt 8 SP Server (LKNV.11100-01) بت
- 64 Alt Server 10 بت
- Astra Linux Special إصدار 1.7 (بما في ذلك وضع بيئة البرامج المغلقة والوضع الإلزامي) 64 بت
- 64 بت/32 (Debian GNU/Linux 11.x (Bullseye

• Ubuntu Server 20.04 LTS (Focal Fossa) 32 بت/64 بت

• RED OS 7.3 Server 64 بت

• RED OS 7.3 إصدار معتمد 64 بت

لا يتوافق خادم Kaspersky Security Center 14 Web Console Server مع أنظمة التشغيل:

• Microsoft Windows Essential Business Server 2008 Standard/Premium

• Microsoft Windows Small Business Server 2003 Standard/Premium مع SP1

• Microsoft Windows Small Business Server 2003 R2 Standard/Premium

• Microsoft Windows Small Business Server 2008 Standard/Premium

• Microsoft Windows Small Business Server 2011 Essentials

• Microsoft Windows Small Business Server 2011 Premium Add-on

• Microsoft Windows Small Business Server 2011 Standard

• Microsoft Windows Home Server 2011

• Microsoft Windows MultiPoint Server 2010 Standard/Premium

• Microsoft Windows MultiPoint Server 2011 Standard/Premium

• Microsoft Windows MultiPoint Server 2012 Standard/Premium

• Microsoft Windows Server 2000

• Microsoft Windows Server 2003 Enterprise مع SP2

• Microsoft Windows Server 2003 Standard مع SP2

• Microsoft Windows Server 2003 R2 Enterprise مع SP2

• Microsoft Windows Server 2003 R2 Standard مع SP2

الأجهزة العميلة

بالنسبة لجهاز عميل، لا يتطلب استخدام Kaspersky Security Center 14 Web Console وجود مستعرض.

تتطابق متطلبات الأجهزة والبرامج في الجهاز مع تلك الخاصة بالمستعرض المستخدم للعمل مع Kaspersky Security Center 14 Web Console.

المستعرضات:

• إصدار Mozilla Firefox Extended Support 91.8.0 أو إصدار أحدث (91.8.0 تم إصداره في 5 أبريل 2022)

• إصدار Mozilla Firefox 99.0 أو إصدار أحدث (تم إصدار 99.0 في 5 أبريل 2022)

• Google Chrome 100.0.4896.88 أو إصدار أحدث (إصدار رسمي)

• Microsoft Edge 100 أو إصدار أحدث

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

متطلبات الأجهزة:

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

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

خادم الأجهزة المحمولة Exchange

يتم تضمين جميع متطلبات الأجهزة والبرامج لخادم الأجهزة المحمولة Exchange في متطلبات خادم Microsoft Exchange.

يكون التوافق مع Microsoft Exchange Server 2007 و Microsoft Exchange Server 2010 و Microsoft Exchange Server 2013 مدعماً.

وحدة تحكم الإدارة

متطلبات الأجهزة:

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

متطلبات البرامج:

• نظام التشغيل Microsoft Windows (يتم تحديد الإصدار المدعوم لنظام التشغيل حسب متطلبات خادم الإدارة) باستثناء أنظمة التشغيل التالية:

- Windows Server 2012 Server Core 64 بت
- Windows Server 2012 R2 Server Core 64 بت
- Windows Server 2016 Server Core (Installation Option) (LTSB) 64 بت
- Windows Server 2019 Core 64 بت
- Windows Server 2022 Core 64 بت
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 10.0 يعمل على:
- Microsoft Windows Server 2008 R2 Service Pack 1

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 Service Pack 1
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Internet Explorer 11.0 يعمل على:
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 R2 Service Pack 1
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows 7 Service Pack 1
- Microsoft Windows 8.1
- Microsoft Windows 10
- Microsoft Edge يعمل على Microsoft Windows 10

عميل الشبكة

الحد الأدنى لمتطلبات الجهاز:

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

- Microsoft Windows Embedded POSReady 2009 بأحدث إصدار من Service Pack 32 بت
- Microsoft Windows Embedded POSReady 7 32 بت / 64 بت
- Microsoft Windows Embedded Standard 7 Service Pack 1 32 بت / 64 بت
- Microsoft Windows Embedded 8 Standard 32 بت / 64 بت
- Microsoft Windows Embedded 8.1 Industry Pro 32 بت / 64 بت
- Microsoft Windows Embedded 8.1 Industry Enterprise 32 بت / 64 بت
- Microsoft Windows Embedded 8.1 Industry Update 32 بت / 64 بت

- Microsoft Windows 10 Enterprise 2015 LTSC 32 بت / 64 بت
- Microsoft Windows 10 Enterprise 2016 LTSC 32 بت / 64-بت
- Microsoft Windows 10 IoT Enterprise 2015 LTSC 32 بت / ARM
- Microsoft Windows 10 IoT Enterprise 2016 LTSC 32 بت / ARM
- Microsoft Windows 10 Enterprise 2019 LTSC 32 بت / 64 بت
- Microsoft Windows 10 IoT Enterprise إصدار 1703 32 بت / 64 بت
- Microsoft Windows 10 IoT Enterprise إصدار 1709 32 بت / 64 بت
- Microsoft Windows 10 IoT Enterprise إصدار 1803 32 بت / 64 بت
- Microsoft Windows 10 IoT Enterprise إصدار 1809 32 بت / 64 بت
- Microsoft Windows 10 20H2 32 بت / 64 بت
- Microsoft Windows 10 Enterprise 21H2 32 بت / 64 بت
- Microsoft Windows 10 IoT Enterprise 32 بت / 64 بت
- Microsoft Windows 10 IoT Enterprise 32 بت / 64 بت
- Microsoft Windows 10 IoT Enterprise 2021 LTSC 32 بت / 64 بت
- Microsoft Windows 10 IoT Enterprise إصدار 1607 32 بت / 64 بت
- Microsoft Windows 10 Home RS3 (Fall Creators Update، v1709) 32 بت / 64 بت
- Microsoft Windows 10 Pro RS3 (Fall Creators Update، v1709) 32 بت / 64 بت
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update، v1709) 32 بت / 64 بت
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update، v1709) 32 بت / 64 بت
- Microsoft Windows 10 Education RS3 (Fall Creators Update، v1709) 32 بت / 64 بت
- Microsoft Windows 10 Home RS4 (تحديث أبريل 2018، رقم 17134) 32 بت / 64 بت
- Microsoft Windows 10 Pro RS4 (تحديث أبريل 2018، رقم 17134) 32 بت / 64 بت
- Microsoft Windows 10 Pro for Workstations RS4 (تحديث أبريل 2018، رقم 17134) 32 بت / 64 بت
- Microsoft Windows 10 Enterprise RS4 (تحديث أبريل 2018، رقم 17134) 32 بت / 64 بت
- Microsoft Windows 10 Education RS4 (تحديث أبريل 2018، رقم 17134) 32 بت / 64 بت
- Microsoft Windows 10 Home RS5 (أكتوبر 2018) 32 بت / 64 بت
- Microsoft Windows 10 Pro RS5 (أكتوبر 2018) 32 بت / 64 بت
- Microsoft Windows 10 Pro for Workstations RS5 (أكتوبر 2018) 32 بت / 64 بت

- Microsoft Windows 10 Enterprise RS5 (أكتوبر 2018) 32 بت / 64 بت
- Microsoft Windows 10 Education RS5 (أكتوبر 2018) 32 بت / 64 بت
- Microsoft Windows 10 Pro 19H1 32 بت/64 بت
- Microsoft Windows 10 Pro 19H1 32 بت/64 بت
- Microsoft Windows 10 Pro for Workstations 19H1 32 بت/64 بت
- Microsoft Windows 10 Enterprise 19H1 32 بت/64 بت
- Microsoft Windows 10 Education 19H1 32 بت/64 بت
- Microsoft Windows 10 Home 19H2 32 بت/64 بت
- Microsoft Windows 10 Home 19H2 32 بت/64 بت
- Microsoft Windows 10 Pro for Workstations 19H2 32 بت/64 بت
- Microsoft Windows 10 Enterprise 19H2 32 بت/64 بت
- Microsoft Windows 10 Education 19H2 32 بت/64 بت
- Microsoft Windows 10 Home 20H1 (تحديث مايو 2020) 32 بت/64 بت
- Microsoft Windows 10 Pro 20H1 (تحديث مايو 2020) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 20H1 (تحديث مايو 2020) 32 بت/64 بت
- Microsoft Windows 10 Education 20H1 (تحديث مايو 2020) 32 بت/64 بت
- Microsoft Windows 10 Home 20H2 (تحديث أكتوبر 2020) 32 بت/64 بت
- Microsoft Windows 10 Pro 20H2 (تحديث أكتوبر 2020) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 20H2 (تحديث أكتوبر 2020) 32 بت/64 بت
- Microsoft Windows 10 Education 20H2 (تحديث أكتوبر 2020) 32 بت/64 بت
- Microsoft Windows 10 Home 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Pro 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Education 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Home 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Pro 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Education 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت

- Microsoft Windows 11 Home بت 64
- Microsoft Windows 11 Pro بت 64
- Microsoft Windows 11 Enterprise 64 بت
- Microsoft Windows 11 Education 64 بت
- Microsoft Windows 8.1 Pro بت / 64 بت
- Microsoft Windows 8.1 Enterprise بت / 64 بت
- Microsoft Windows 8 Pro بت / 64 بت
- Microsoft Windows 8 Enterprise بت / 64 بت
- Microsoft Windows 7 Professional with Service Pack 1 والإصدارات الأعلى 32 بت / 64 بت
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 والإصدارات الأعلى 32 بت / 64 بت
- Microsoft Windows 7 Home Basic/Premium with Service Pack 1 والإصدارات الأعلى 32 بت / 64 بت
- Microsoft Windows XP Professional Service Pack 3 والإصدارات الأعلى 32 بت
- Microsoft Windows XP Professional for Embedded Systems Service Pack 3 32 بت
- Windows Small Business Server 2011 Essentials 64 بت
- Windows Small Business Server 2011 Premium Add-on 64 بت
- Windows Small Business Server 2011 Standard 64 بت
- Windows MultiPoint Server 2011 Standard/Premium 64 بت
- Windows MultiPoint Server 2012 Standard/Premium 64 بت
- Windows Server 2008 Foundation with Service Pack 2 بت / 64 بت
- Windows Server 2008 Service Pack 2 (كل الإصدارات) 32 بت / 64 بت
- Windows Server 2008 R2 Datacenter Service Pack 1 والإصدار الأعلى 64 بت
- Windows Server 2008 R2 Enterprise Service Pack 1 والإصدار الأعلى 64 بت
- Windows Server 2008 R2 Foundation with Service Pack 1 والإصدار الأعلى 64 بت
- Windows Server 2008 R2 Core Mode Service Pack 1 والإصدارات الأحدث 64 بت
- Windows Server 2008 R2 Standard Service Pack 1 والإصدار الأحدث 64 بت
- Windows Server 2008 R2 Service Pack 1 (جميع الإصدارات) 64 بت
- Windows Server 2012 Server Core 64 بت
- Windows Server 2012 Datacenter 64 بت

- 64 بت Windows Server 2012 Essentials
- 64 بت Windows Server 2012 Foundation
- 64 بت Windows Server 2012 Standard
- 64 بت Windows Server 2012 R2 Server Core
- 64 بت Windows Server 2012 R2 Datacenter
- 64 بت Windows Server 2012 R2 Essentials
- 64 بت- Windows Server 2012 R2 Foundation
- 64 بت Windows Server 2012 R2 Standard
- 64 بت Windows Server 2016 Datacenter (LTSC)
- 64 بت Windows Server 2016 Standard (LTSC)
- 64 بت Windows Server 2016 Server Core (Installation Option) (LTSC)
- 64 بت Windows Server 2019 Standard
- 64 بت Windows Server 2019 Datacenter
- 64 Windows Server 2019 Core بت
- 64 بت Windows Server 2022 Standard
- 64 بت Windows Server 2022 Datacenter
- 64 Windows Server 2022 Core بت
- 64 بت Windows Storage Server 2012
- 64 بت Windows Storage Server 2012 R2
- 64 بت Windows Storage Server 2016
- 64 بت Windows Storage Server 2019
- 32 بت/64 بت (Debian GNU/Linux 11.x (Bullseye)
- 32 بت / 64 بت. (Debian GNU/Linux 10.x (Buster)
- 32 بت/64 بت (Debian GNU/Linux 9.x (Stretch)
- 32 بت/64 بت Ubuntu Server 20.04 LTS (Focal Fossa)
- 64 بت Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM
- 32 بت/64 بت Ubuntu Server 18.04 LTS (Bionic Beaver)
- 32 بت/64 بت Ubuntu Desktop 20.04 LTS (Focal Fossa)

- 32 Ubuntu Desktop 18.04 LTS (Bionic Beaver) بت/64 بت
- 64 CentOS 8.x بت
- 64 CentOS 7.x بت
- 64 CentOS 7.x ARM بت
- 64 Red Hat Enterprise Linux Server 8.x بت
- 64 Red Hat Enterprise Linux Server 7.x بت
- 32 Red Hat Enterprise Linux Server 6.x بت/64
- 12 SUSE Linux Enterprise Server (جميع حزم الخدمة) 64 بت
- 15 SUSE Linux Enterprise Server (جميع حزم الخدمة) 64 بت
- 15 SUSE Linux Enterprise Desktop (جميع حزم الخدمة) 64 بت
- 15 SUSE Linux Enterprise Desktop (حزمة الخدمة 3) 64 ARM بت
- 64 openSUSE 15 بت
- EulerOS 2.0 SP8 ARM نظام
- 64 Pardus OS 19.1 نظام التشغيل بت
- 64 Astra Linux Special إصدار 1.7 (بما في ذلك وضع بيئة البرامج المغلقة والوضع الإلزامي) بت
- 64 Astra Linux Special إصدار 1.6 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي) بت
- 64 Astra Linux Common إصدار 2.12 بت
- 64 Astra Linux Special الإصدار 4.7 ARM
- 64 Alt Server 10 بت
- 64 Alt Server 9.2 بت
- 32 Alt Workstation 10 بت / 64 بت
- محطة العمل البديلة 9.2 32 بت / 64 بت
- 64 Alt 8 SP Server (LKNV.11100-01) بت
- 64 Alt 8 SP Server (LKNV.11100-02) بت
- 64 Alt 8 SP Server (LKNV.11100-03) إصدار بت
- 32 Alt 8 SP Workstation (LKNV.11100-01) بت / 64 بت
- 32 Alt 8 SP Workstation (LKNV.11100-02) بت / 64 بت
- 32 Alt 8 SP Workstation (LKNV.11100-03) بت / 64 بت

- Mageia 4 32 بت
- Oracle Linux 7 64 بت
- Oracle Linux 8 64 بت
- Linux Mint 19.x 32 بت
- Linux Mint 20.x 64 بت
- AlterOS 7.5 والإصدارات الأحدث 64 بت
- GosLinux IC6 64 بت
- RED OS 7.3 64 بت
- RED OS 7.3 Server 64 بت
- RED OS 7.3 إصدار معتمد 64 بت
- ROSA Enterprise Linux Server 7.3 64 بت
- ROSA Enterprise Linux Desktop 7.3 64 بت
- ROSA COBALT Workstation 7.3 64 بت
- ROSA COBALT Server 7.3 64 بت
- Lotos (Linux core) الإصدار 4.19.50، 64 (DE: MATE) بت
- (macOS Sierra (10.12
- (macOS High Sierra (10.13
- (macOS Mojave (10.14
- (macOS Catalina (10.15
- (macOS Big Sur (11.x
- (macOS Monterey (12.x

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

يتم دعم الأنظمة الأساسية الظاهرية التالية:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 بت
- Microsoft Hyper-V Server 2012 R2 64 بت

- Microsoft Hyper-V Server 2016 64 بت
- Microsoft Hyper-V Server 2019 64 بت
- Microsoft Hyper-V Server 2022 64 بت
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- آلة افتراضية على أساس Kernel. تدعم أنظمة التشغيل التالية:
- Alt 8 SP Server (LKNV.11100-01) 64 بت
- Alt Server 10 64 بت
- Astra Linux Special إصدار 1.7 (بما في ذلك وضع بيئة البرامج المغلقة والوضع الإلزامي) 64 بت
- Debian GNU/Linux 11.x (Bullseye) 32 بت/64 بت
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 بت/64 بت
- RED OS 7.3 64 بت
- RED OS 7.3 Server 64 بت
- RED OS 7.3 إصدار معتمد 64 بت

على الأجهزة التي تعمل بنظام 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.

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

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

قائمة من تطبيقات Kaspersky المدعومة والحلول

يدعم Kaspersky Security Center النشر والإدارة المركزيين لجميع تطبيقات وحلول Kaspersky المدعومة حاليًا. يوضح الجدول أدناه تطبيقات وحلول Kaspersky التي تدعمها وحدة التحكم الإدارية المعتمدة على MMC و Kaspersky Security Center 14 Web Console. لمعرفة إصدارات التطبيقات والحلول، ارجع إلى صفحة ويبدو دورة حياة دعم المنتج.

قائمة تطبيقات وحلول Kaspersky المدعومة بواسطة Kaspersky Security Center 14 Web Console

اسم تطبيق أو حل Kaspersky	مدعومة بوحدة التحكم الإدارية المعتمدة على MMC	مدعوم بواسطة Kaspersky Security Center 14 Web Console
لمحطات العمل		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓

✓	✓	Kaspersky Endpoint Security for Linux ARM :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
—	✓	الأمن الإلكتروني الصناعي من Kaspersky لعقد Linux
✓	✓	Kaspersky Industrial CyberSecurity for (النشر المركزي غير مدعوم) Networks
للأجهزة المحمولة		
✓	✓	:Kaspersky Endpoint Security for Android
✓	—	iOS لأجهزة Kaspersky Security
لخوادم الملفات		
✓	✓	Kaspersky Security for Windows Server
✓	✓	Kaspersky Endpoint Security for Windows
✓	✓	Kaspersky Endpoint Security for Linux
بالنسبة للأجهزة الظاهرية		
✓	✓	Kaspersky Security for Virtualization Light Agent
—	✓	Kaspersky Security for Virtualization Agentless
بالنسبة لأنظمة البريد وخوادم /sharepoint التعاون (النشر المركزي غير مدعوم)		
—	✓	Kaspersky Security for Linux Mail Server
—	✓	بوابة البريد الأمانة من Kaspersky
—	✓	Microsoft Exchange لـ Kaspersky Security Servers
بالنسبة لاكتشاف هجمات مستهدفة		
✓	✓	Kaspersky Sandbox
✓	—	برنامج Kaspersky Endpoint Detection and Response Optimum 2.0
✓	—	Kaspersky Managed Detection and Response
لأجهزة KasperskyOS		
✓	—	بوابة Kaspersky IoT الأمانة
✓	—	Kaspersky Security Management Suite (مكون إضافي لـ Kaspersky Thin Client)

تراخيص وميزات برنامج Kaspersky Security Center 14

يتطلب برنامج Kaspersky Security Center ترخيصًا لبعض من ميزاته.

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

تراخيص وميزات Kaspersky Security Center

<u>Kaspersky EDR</u> ☑ <u>Optimum</u>	<u>برنامج</u> <u>Kaspersky Hybrid Cloud</u> ☑ <u>Security</u>	<u>Kaspersky Hybrid Cloud Security</u> ☑ <u>Standard</u>	<u>Kaspersky Total Security for</u> <u>Business</u> ☑ <u>Business</u>	<u>Kaspersky Endpoint Security for Business</u> ☑ <u>Advanced</u>	<u>Kaspersky Endpoint Security</u> ☑ <u>لتحديد الأعمال</u>	<u>إدارة الثغرات الأمنية</u> ☑ <u>والتصحيات</u>	ميزات Kaspersky Security Center
✓	✓	✓	✓	✓	✓	✓	<u>تقييم الثغرات الأمنية</u>
✓	✓	—	✓	✓	—	✓	<u>إدارة التصحيح</u>
✓	✓	✓	✓	✓	✓	✓	<u>التحكم في الوصول على أساس الدور</u>
✓	✓	—	✓	✓	—	✓	<u>التثبيت لنظم التشغيل والتطبيقات</u>
✓	—	—	✓	✓	✓	✓	<u>إدارة الأجهزة المحمولة (أي إدارة أجهزة المستخدمين التي تعمل بنظام iOS أو Android)</u>
—	✓	✓	—	—	—	—	<u>معالج تكوين بيئة السحابة للعمل في بيئات السحابة مثل AWS أو Microsoft Azure أو Google Cloud</u>
✓	✓	✓	✓	✓	✓	✓	<u>تصدير الأحداث إلى أنظمة: SIEM: Syslog</u>
✓	✓	—	✓	✓	—	✓	<u>تصدير الأحداث إلى أنظمة: SIEM: QRadar بواسطة IBM و Micro Focus بواسطة ArcSight</u>

عن توافق خادم الإدارة و Kaspersky Security Center 14 Web Console

نوصي بشدة باستخدام أحدث إصدار من خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console؛ خلاف ذلك، قد تكون وظائف Kaspersky Security Center محدودة.

يمكنك تثبيت وترقية خادم إدارة Kaspersky Security Center وكذلك Kaspersky Security Center 14 Web Console بشكل مستقل. في هذه الحالة، يجب عليك التأكد أن إصدار Kaspersky Security Center 14 Web Console المثبت متوافق مع إصدار خادم الإدارة الذي تتصل به.

- يدعم Kaspersky Security Center 14 Web Console خادم إدارة Kaspersky Security Center للإصدارات التالية: 14 و 13.2 و 13.1.
- يدعم خادم الإدارة Kaspersky Security Center 14 Administration Server Kaspersky Security Center 14 Web Console للإصدارات التالية: 14 و 13.2 و 13.1.

حول Kaspersky Security Center Cloud Console

يعني استخدام Kaspersky Security Center كتطبيق محلي، عليك 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 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، ويمكنك 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
- البرتغالية (البرازيل)
- الروسية
- الإسبانية
- الإسبانية (LATAM)

يتوفر المزيد من المعلومات حول [Kaspersky Security Center Cloud Console](#) و [Kaspersky Security Center](#) في وثائق [Kaspersky Security Center Cloud Console](#) وفي وثائق [Kaspersky Endpoint Security for Business](#).

المفاهيم الأساسية

يوضح هذا القسم المفاهيم الأساسية ذات صلة Kaspersky Security Center.

خادم الإدارة

تتيح مكونات Kaspersky Security Center إدارة تطبيقات Kaspersky المثبتة 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 المحدد أثناء تثبيت خادم الإدارة.

ويقوم خادم الإدارة بالوظائف التالية:

- تخزين بنية مجموعات الإدارة
- تخزين معلومات حول تكوين الأجهزة العملية.
- ترتيب المستودعات لحزم توزيع التطبيقات.
- تثبيت التطبيقات عن بُعد على الأجهزة العملية وإزالة التطبيقات.
- تحديث قواعد بيانات التطبيقات والوحدات النمطية لبرامج تطبيقات Kaspersky
- إدارة السياسات والمهام على الأجهزة العملية.
- تخزين معلومات حول الأحداث التي وقعت على الأجهزة العملية.
- 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 و Kaspersky Security Center 14 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 14 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 14 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 مُقيّد. 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 الإنترنت 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 أمن مكافحة الفيروسات. جميع إمكانيات الإدارة المركزية ومراقبة حالة أمن مكافحة الفيروسات في شبكات الشركة تظل متوفرة.
- كيف يستخدم موفر الخدمة Kaspersky Security Center. لا يحتاج موفر الخدمة إلا إلى تثبيت Kaspersky Security Center و Kaspersky Security Center 14 Web Console فقط. لإدارة عدد كبير من الأجهزة العميلة لمؤسسات مختلفة، يمكن لمزود الخدمة إضافة خوادم إدارة افتراضية 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.

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

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.

هناك نوعان لخادم الجهاز المحمول:

- خادم الأجهزة المحمولة Exchange. تم تثبيت هذا على جهاز حيث تم تثبيت خادم Microsoft Exchange، مما يسمح باسترداد المعلومات من خادم Microsoft Exchange ونقلها إلى خادم الإدارة. يتم استخدام خادم الجهاز المحمول لإدارة الأجهزة المحمولة التي تدعم بروتوكول Exchange ActiveSync.
- خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. 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

Kaspersky Security Center Web Server (المشار إليه فيما بعد بخادم الويب) هو مكون Kaspersky Security Center يتم تثبيته معاً 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 تلقائياً 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 تلقائياً على خادم الويب. يتم حذف ملف التعريف الذي تم نشره تلقائياً 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 مباشراً 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:

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

حيث:

- < اسم خادم الويب> 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 للمستخدم وصولاً إليه.

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

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

عمل الشبكة

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

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

- تتميز بالاسم "عمل شبكة Kaspersky Security Center 14"

- تعيين للبدء تلقائيًا عند بدء تشغيل نظام التشغيل

- باستخدام حساب النظام المحلي

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

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

- حزمة التثبيت في قسم تخزين خادم الإدارة (يجب أن يكون لديك خادم إدارة مثبتًا)

- حزمة التثبيت الموجودة [على خوادم ويب Kaspersky](#)

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

اسم العملية التي يبدأها عمل الشبكة هو knagent.exe.

يقوم عمل 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).

- استخدام وضع تشغيل عام لجميع التطبيقات من خلال إنشاء مهام جماعية بإعدادات محددة. تشمل 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 كمبيوتر الموظف من مجموعة إدارة المحاسبين إلى مجموعة إدارة المُطوّرين. وبعد ذلك، سوف يتلقى الكمبيوتر تلقائيًا إعدادات التطبيق اللازمة للمُطوّرين.

الجهاز المُدار

الجهاز المُدار هو جهاز كمبيوتر 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 وكتابة 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 إدارة الأجهزة غير المخصصة. 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 التحكم الإدارية عليه أو تستخدمه لفتح Kaspersky Security Center 14 Web Console. يمكن للمسؤولين استخدام هذه الأجهزة في الإدارة المركزية عن بُعد لتطبيقات Kaspersky المثبتة 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 Kaspersky عن بُعد من خلال Kaspersky Security Center 14 Web Console. مكون الإدارة الإضافي للويب يُشار إليه هنا فيما بعد باسم مكون الإدارة الإضافي. مكون الإدارة الإضافي هو واجهة بين Kaspersky Security Center 14 Web Console وتطبيق Kaspersky محدد. باستخدام مكون الإدارة الإضافي، يمكنك تكوين المهام والسياسات المخصصة للتطبيق.

يمكنك تنزيل المكونات الإضافية للإدارة من [صفحة الدعم الفني لـ Kaspersky](#).

يوفر مكون الإدارة الإضافي ما يلي:

- واجهة لإنشاء وتحرير [مهام](#) 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 14 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 حالياً 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 الحماية ضد 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، تصبح السياسة المفعلة الحالية غير نشطة تلقائياً.

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 حالياً للجهاز.

تعمل ملفات التعريفية للسياسة وفقاً 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 نحو مركزي. يمكن لهذه المثيلات الاختلاف وفقاً 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 أي 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 و**سجل 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 بتغيير 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 تحديدها 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 تحديدها باستخدام وسائل أخرى يتم تنفيذها في الوقت المحلي لجهاز ما.

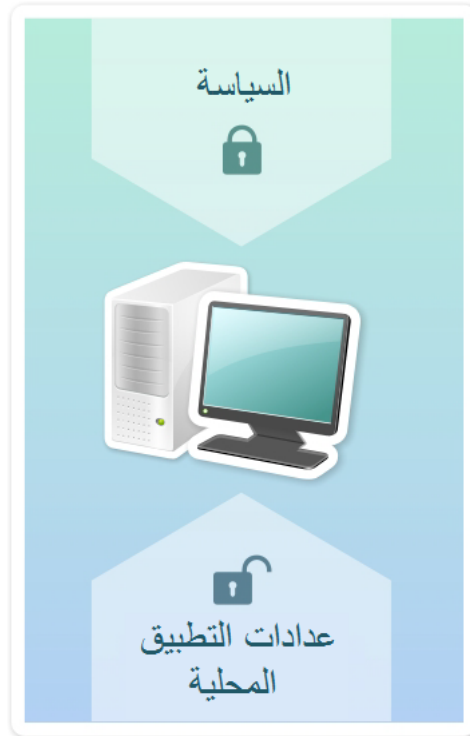
كيفية ارتباط إعدادات التطبيق المحلية بالسياسات

يمكنك استخدام السياسات لتعيين القيم المماثلة لإعدادات التطبيق لجميع 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 للسياسة بتعديلها، أي الإعدادات غير المقفلة.

يتم تحديد قيمة الإعدادات التي يستخدمها التطبيق على جهاز عميل (انظر الشكل التالي) 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 الإعداد، فإن التطبيق يستخدم قيمة الإعداد المحلية على كل جهاز عميل بدلاً من القيمة المحددة في السياسة. ويمكن بعدها تغيير الإعداد في إعدادات التطبيق المحلية.



السياسة وإعدادات 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 مؤمن ضد التغييرات في السياسة.
- بواسطة سياسة المجموعة إذا كان الإعداد مؤمناً ضد التغييرات

نقطة توزيع

نقطة توزيع (كانت تُعرّف فيما سبق بوكيل التحديث) هي جهاز مثبت عليه عميل الشبكة يتم استخدامه لتوزيع التحديثات، وتثبيت التطبيقات عن بُعد، واسترداد معلومات حول الأجهزة المتصلة بالشبكة. يمكن لنقطة التوزيع إجراء الوظائف التالية:

- توزيع التحديثات وحزم التثبيت الواردة من خادم الإدارة على الأجهزة العاملة في المجموعة (بما في ذلك طريقة الإرسال المتعدد المتبعة باستخدام UDP). 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.

- تعمل نقاط التوزيع على تسريع توزيع التحديثات وتحرير مساحة موارد خادم الإدارة.
- 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 تتوفر 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.
- إجراء التثبيت عن بُعد للبرامج التابعة لجهات خارجية وتطبيقات Kaspersky عبر أدوات Microsoft Windows، بما في ذلك التثبيت على الأجهزة العاملة بدون عميل الشبكة.
- تتيح هذه الميزة نقل حزم تثبيت عميل الشبكة عن بُعد إلى الأجهزة العاملة التي توجد في الشبكات التي يتعذر على خادم الإدارة الوصول إليها.
- يعمل كخادم وكيل يشارك في Kaspersky Security Network.
- يمكنك تمكين وكيل KSN على جانب نقطة التوزيع لجعل الجهاز يعمل كوكيل KSN. في هذه الحالة، يتم تشغيل خدمة وكيل (ksnproxy) (KSN) على الجهاز.

يتم نقل الملفات من خادم الإدارة إلى نقطة توزيع عبر HTTP أو HTTPS، إذا ما كان اتصال SSL ممكناً. 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 يدوياً (بواسطة المسؤول)، أو تلقائياً (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، فسيتم توصيل عميل الشبكة في الجهاز المدار بنقطة التوزيع الأقرب في التسلسل الهرمي.

يمكن أيضاً 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. يحدث 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 آخر. يتيح لك ذلك تجنب الحمل الزائد على الشبكة الذي يمكن أن يحدث نظرًا إلى تراكم IP. ميزة وظائف تعيين العنوان الفريد في Kaspersky Security Center 10 Service Pack 3 والإصدارات الأحدث. لن يتم تغيير عناوين IP للإرسال المتعدد التي تم تعيينها في الإصدارات السابقة للتطبيق.

إذا تم تعيين اثنين أو أكثر من نقاط التوزيع إلى منطقة شبكة واحدة أو إلى مجموعة إدارة واحدة، فستصبح أحدهما 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 نشطة. 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 حدث بمستوى الأهمية تحذير. سيتم نشر الحادث في خصائص الجهاز، في قسم **الحوادث**.

يتطلب تشغيل مهام التثبيت عن بُعد على جهاز المعين 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 المعين 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 10000 جهاز.

لديك خياران عند استخدام بوابات الاتصال:

- نوصي بتثبيت بوابة اتصال في منطقة الأجهزة الموصولة 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).

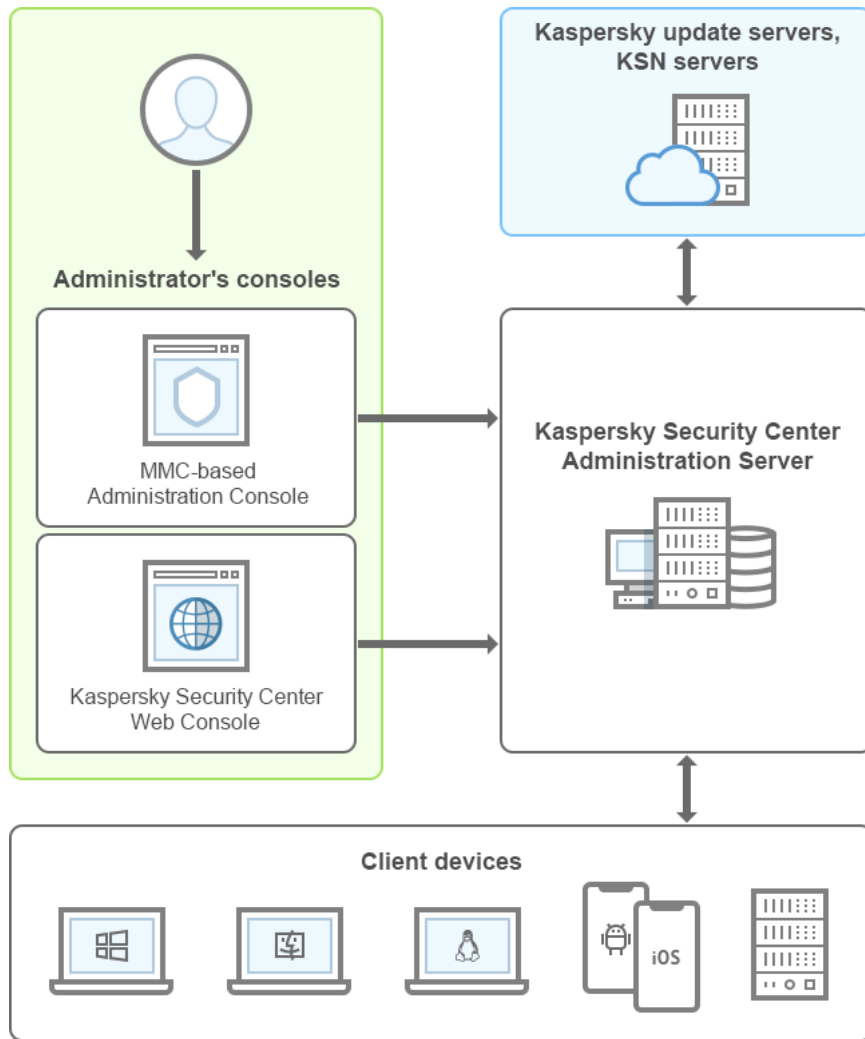
لا يمكن لبوابة الاتصال أن تتصل بخادم الإدارة من خلال بوابة اتصال أخرى. وهذا يعني أن عميل الشبكة لا يمكن أن يعمل كبوابة اتصال بشكل متزامن ويستخدم بوابة اتصال ليتصل بخادم الإدارة.

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.

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 بوحدة التحكم). توفير واجهة مستخدم لخدمات الإدارة الخاصة بخادم الإدارة و عميل الشبكة. يتم تنفيذ وحدة تحكم الإدارة كأداة إضافية لـ Microsoft Management Console (MMC). يتيح 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 مركز تخزين معلومات حول التطبيقات المثبتة على شبكة المؤسسة وحول كيفية إدارتها.

- خوادم تحديث Kaspersky (خوادم HTTP(S) 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 قبل 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.

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.

للحصول على معلومات حول نشر Kaspersky Security Center Cloud Console، ارجع إلى [توثيق Kaspersky Security Center Cloud Console](#).

يتألف تثبيت Kaspersky Security Center من الخطوات التالية:

1. عمل تحضير ي

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 جهاز الكمبيوتر 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) و عميل الشبكة على الأجهزة المُدارة.
- سيتم إنشاء مجموعات الإدارة (من المحتمل أن تكون مُجمعة 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 تحضير ي

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 المفاتيح)، [رموز التنشيط](#)، وقائمة تطبيقات Kaspersky التي يمكن تفعيلها بواسطة كل مفتاح ترخيص.

إذا كنت تريد تجربة برنامج Kaspersky Security Center أو لا، فيمكنك الحصول على نسخة تجريبية مجانية لمدة 30 يوماً 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 ستستخدم وكيفية توزيعها على مكاتبك](#) إذا كنت تقوم بتشغيل شبكة موزعة.

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 العملية التي تحتوي على خادم إدارة واحد أو كان من الضروري إنشاء تسلسل هرمي لخوادم الإدارة. قد يتعين عليك أيضاً 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 الأجهزة المحمولة Exchange](#) و [خادم الأجهزة المحمولة التي تعمل بنظام 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/أو المزود بإدارة الثغرات الأمنية والتصحیحات، 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، فُرجى ملاحظة أنه يمكنك تحيل البيانات المخزنة في قاعدة البيانات إلى MySQL أو MariaDB أو [Azure SQL](#) أو DBMS. لإجراء التحويل، [انسخ بياناتك احتياطياً واستعدّها إلى نظام DBMS الجديد](#).

8 تثبيت نظام إدارة قواعد البيانات وإنشاء قاعدة بيانات

تعرف على المزيد حول [حسابات استخدام DBMS](#) وتثبيت DBMS. اكتب إعدادات نظام إدارة قواعد البيانات (DBMS) واحفظها لأنك ستحتاج إليها أثناء تثبيت خادم الإدارة. تشمل هذه الإعدادات اسم خادم SQL Server ورقم المنفذ المستخدم للاتصال بخادم SQL Server واسم الحساب وكلمة المرور للوصول إلى خادم SQL Server.

بشكل افتراضي، يقوم مثبت 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 وفقاً 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 ونشر 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 مثبت Kaspersky Security Center بإنشاء ثلاثة حسابات محلية سيتم تشغيل خادم الإدارة وخدمات Kaspersky Security Center بموجبها:

○ AK-KL-*: حساب خدمة خادم إدارة

○ KIScSvc: حساب للخدمات الأخرى من مجموعة خادم الإدارة

○ KIPxeUser: 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 لديها 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، و Kaspersky Security Center 14 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 أيضاً تثبيت مجموعة المكونات الإضافية الافتراضية فقط الخاصة بإدارة تطبيقات Kaspersky. كما يمكنك أيضاً 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. يمكنك التثبيت المخصص من تحديد مكونات الإدارة الإضافية لـ Kaspersky المراد تثبيتها. إذا لزم الأمر، يمكنك بدء تثبيت مخطط في وضع غير تفاعلي.

يتم تثبيت وحدة تحكم الإدارة وإصدار خادم عميل الشبكة مع خادم الإدارة. يمكنك أيضاً اختبار تثبيت Kaspersky Security Center 14 Web Console أثناء التثبيت.

إذا كنت ترغب في تثبيت وحدة تحكم الإدارة و/أو Kaspersky Security Center 14 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 تلقائياً عند أول اتصال خادم الإدارة. قم بتنفيذ التكوين الأولي لخادم الإدارة وفقاً 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 جاهزاً للاستخدام المستقبلي.

تأكد من أن وحدة تحكم الإدارة تعمل ويمكنك الاتصال بخادم الإدارة عبر وحدة تحكم الإدارة. وتأكد أيضاً 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 هي جزء من معالج البدء السريع. كما يمكنك أيضاً بدء اكتشاف الأجهزة يدوياً. 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 تلقائياً.

2 تثبيت عميل الشبكة وتطبيقات أمان على أجهزة متصلة بالشبكة.

يشمل نشر الحماية (تكوين الحماية في شبكة تنظيم عميل، السيناريوس: 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 تشكل تهديداً. يضمن عميل الشبكة الاتصال بين الجهاز وخادم الإدارة. يتم تكوين إعدادات عميل الشبكة تلقائياً 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 و عميل الشبكة عند بعد أو محلياً.

التثبيت عن بُعد—باستخدام معالج نشر الحماية، يمكنك تثبيت تطبيق الأمان عن بُعد (على سبيل المثال، Kaspersky Endpoint Security for Windows) و عميل 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، نصحك بالاتصال بالجهاز يدوياً 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 محلياً على هذه الأجهزة.

يتم وصف تثبيت عميل الشبكة على الأجهزة التي تستخدم نظامي التشغيل Linux و MacOS 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 و macOS تعد أقل عرضة للتهديدات 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 مثبت 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 المدارة على هذه الأجهزة.

4 تكوين حماية الأجهزة المحمولة

هذه الخطوة هي 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 باتباع 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 يدوياً. 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 تلقائياً، ولكن يمكنك تعيينها يدوياً، 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

الجدول أدناه تظهر المنافذ الافتراضية التي يجب فتحها على خوادم الإدارة والأجهزة العميلة. يمكنك إذا كنت ترغب في ذلك أن تغير أرقام المنافذ الافتراضية.

يظهر الجدول أدناه المنافذ الافتراضية التي يجب فتحها على خادم الإدارة. مع ذلك، 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 و MariaDB Server أو المنفذ 1433 لخادم Microsoft SQL Server). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

المنافذ التي يجب فتحها على 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 قسم <u>خادم الويب</u> في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة أو في Kaspersky Security Center 13.1 Web Console.
8061	klcsweb	TCP (TLS)	نقل حزم التثبيت التي تم نشرها إلى أجهزة عميلة	نشر حزم التثبيت. يمكنك تغيير رقم المنفذ الافتراضي في قسم <u>خادم الويب</u> في نافذة خصائص خادم الإدارة في وحدة تحكم الإدارة أو في Kaspersky Security Center 13.1 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 DMZ)	إدارة أجهزة العملاء وخوادم الإدارة الثانوية. يمكنك تغيير رقم المنفذ الافتراضي لتلقي الاتصالات من عملاء الشبكة عند <u>تكوين منافذ الاتصال</u> . يمكنك تغيير رقم المنفذ الافتراضي لتلقي الاتصالات من خوادم الإدارة الثانوية عند إنشاء تسلسل هرمي لخوادم الإدارة في وحدة تحكم الإدارة أو في <u>Kaspersky Security Center 14 Web Console</u> .
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 <u>Kaspersky Security Center 14 Web Console</u> .
13291	klserver	TCP (TLS)	تلقي اتصالات من وحدة تحكم الإدارة إلى خادم الإدارة	إدارة خادم الإدارة. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص <u>خادم الإدارة</u> في وحدة تحكم الإدارة.
13299	klserver	TCP (TLS)	تلقي اتصالات من Kaspersky Security Center 14 Web Console إلى خادم الإدارة؛ تلقي	Kaspersky Security Center 14 Web Console. OpenAPI.

<p>يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة (في القسم الفرعي <u>منافذ الاتصال</u> من القسم عام) في وحدة تحكم الإدارة، أو عند إنشاء تسلسل هرمي لخوادم الإدارة <u>في وحدة تحكم الإدارة</u> أو في <u>Kaspersky Security Center 14 Web Console</u>.</p>	<p>اتصالات إلى خادم الإدارة عبر OpenAPI</p>			
<p>إدارة الأجهزة العميلة.</p> <p>يمكنك تغيير رقم المنفذ الافتراضي عند <u>تكوين منافذ الاتصال</u> أثناء تثبيت Kaspersky Security Center أو عند <u>توصيل جهاز عميل بخادم الإدارة يدويًا</u>.</p>	<p>تلقي اتصالات من عملاء الشبكة</p>	TCP	klserver	14000
<p>خادم وكيل KSN.</p> <p>يمكنك تغيير رقم المنفذ الافتراضي في <u>نافذة خصائص خادم الإدارة</u>.</p>	<p>تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN</p>	TCP	ksnproxy	13111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)
<p>خادم وكيل KSN.</p> <p>يمكنك تغيير رقم المنفذ الافتراضي في <u>نافذة خصائص خادم الإدارة</u>.</p>	<p>تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN</p>	UDP	ksnproxy	15111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)
<p>خادم عميل التنشيط الذي تستخدمه الأجهزة غير المحمولة لتنشيط تطبيقات Kaspersky برموز التنشيط.</p> <p>يمكنك تغيير رقم المنفذ الافتراضي في <u>نافذة خصائص خادم الإدارة</u>.</p>	<p>تلقي اتصالات لتنشيط التطبيق من الأجهزة المدارة (باستثناء الأجهزة المحمولة)</p>	TCP (TLS)	klactprx	17000
<p>خادم وكيل التنشيط للأجهزة المحمولة.</p> <p>يمكنك تغيير رقم المنفذ الافتراضي في <u>نافذة خصائص خادم الإدارة</u>.</p>	<p>تلقي اتصالات <u>لتفعيل التطبيق من الأجهزة المحمولة</u></p>	TCP (TLS)	klactprx	17100 (فقط إذا كنت تدير أجهزة محمولة)
<p>الاتصال عن بُعد بالأجهزة المدارة باستخدام Kaspersky Security Center 14 Web Console.</p> <p>يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة (في <u>المنافذ الإضافية</u> القسم الفرعي <u>بالقسم العام</u> في وحدة التحكم الإدارة فقط).</p>	<p><u>نفق الاتصالات</u> إلى الأجهزة المدارة باستخدام الأداة المساعدة klstunnel</p>	HTTPS (TLS)	klserver	19170
<p>إدارة الجهاز المحمول.</p> <p>يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة <u>في وحدة تحكم الإدارة</u> أو في <u>Kaspersky Security Center 14 Web Console</u>.</p>	<p>تلقي اتصالات من الأجهزة المحمولة</p>	TCP (TLS)	klserver	13292 (فقط إذا كنت تدير أجهزة محمولة)
<p>إدارة أجهزة العملاء لحماية UEFI.</p> <p>يمكنك تغيير رقم المنفذ الافتراضي <u>عند توصيل أجهزة محمولة</u>، أو لاحقًا في نافذة خصائص خادم الإدارة (في القسم الفرعي <u>المنافذ الإضافية</u> بقسم عام) في وحدة تحكم الإدارة أو في <u>Kaspersky Security Center 14 Web Console</u>.</p>	<p>تلقي اتصالات من أجهزة حماية UEFI</p>	TCP (TLS)	klserver	13294 (فقط إذا كنت تدير أجهزة محمولة)

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

المنفذ الذي يستخدمه خادم Kaspersky Security Center iOS MDM

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

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

المنفذ الذي يستخدمه خادم Kaspersky Security Center Web Console

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
8080	:Node.js جافا سكريبت من جانب الخادم	TCP (TLS)	تلقي اتصالات <u>من مستعرض الويب إلى Kaspersky Security Center 14 Web Console</u>	Kaspersky Security Center 14 Web Console يمكنك تغيير رقم المنفذ الافتراضي عند تثبيت Kaspersky Security Center 14 Web Console <u>على جهاز يعمل بنظام Windows أو على منصة Linux</u> . إذا قمت بتثبيت Kaspersky Security Center 14 Web Console على نظام التشغيل Linux ALT، فيجب عليك تحديد رقم منفذ بخلاف 8080، لأن المنفذ 8080 يستخدمه نظام التشغيل.

الجدول أدناه يوضح المنفذ الذي يجب فتحه على الأجهزة المدارة المثبت عليها عميل الشبكة.

المنافذ التي يستخدمها عميل الشبكة

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
15000	klagent	UDP	إشارات الإدارة من خادم الإدارة إلى وكلاء الشبكة	إدارة الأجهزة العميلة. يمكنك تغيير رقم المنفذ الافتراضي في إعدادات سياسة عميل الشبكة <u>في وحدة تحكم الإدارة أو في Kaspersky Security Center 14 Web Console</u> .
15000	klagent	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 التنبيهات.

يوضح الجدول الموجود أدناه المنافذ التي يجب فتحها على جهاز مدار مثبت عليه عميل شبكة والتي تعمل كنقطة توزيع.

المنافذ التي يستخدمها عميل الشبكة وتعمل كنقطة توزيع

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
13000	klagent	TCP (TLS)	تلقي اتصالات <u>من عملاء الشبكة</u>	إدارة الأجهزة العميلة وتسليم التحديثات وحزم التنبيهات. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع <u>في وحدة تحكم الإدارة أو في Kaspersky Security Center 14 Web Console</u> .
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 <u>في وحدة تحكم الإدارة أو في Kaspersky Security Center 14 Web Console</u> .

تسليم التحديثات وحزم التثبيت. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console 14 .	الإرسال المتعدد لعملاء الشبكة	UDP	klagent	15001
خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console 14 .	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	UDP	ksnproxy	15111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)
قم بإرسال خادم. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع في وحدة تحكم الإدارة أو في Kaspersky Security Center Web Console 14 .	إرسال الإشعارات إلى الأجهزة المدارة	TCP ((TLS	klagent	13295 (إذا كنت تستخدم نقطة التوزيع كخادم إرسال فقط)

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 14 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 klsetsvcert](#) أو من خلال قسم خصائص خادم الإدارة في وحدة تحكم الإدارة بناءً على نوع الشهادة. عند استخدام الأداة المساعدة klsetsvcert، 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 المنشأة تلقائيًا.

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

شهادات خادم الإدارة

مطلوب شهادة خادم الإدارة لمصادقة خادم الإدارة، وكذلك للتفاعل الآمن بين خادم الإدارة و عميل الشبكة على الأجهزة المُدارة. عند توصيل وحدة تحكم الإدارة بخادم الإدارة لأول مرة، تتم مطابقتك 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 بالمشاركة ("C").

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. 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 بشكل 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 ثنائي الاتجاه SSL)، فيمكنك إنشاء هذه الشهادات عن طريق الجهة المعتمدة لشهادات المستخدم التي يتم إنشاؤها تلقائيًا ("MCA"). يمكنك 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.

يمكنك 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. تعد كل شهادة عميل على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM فريدة من نوعها. 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

يتم استخدام نوع خاص من الشهادات بواسطة خادم ويب Kaspersky Security Center (المشار إليه فيما يلي باسم خادم الويب)، وهو أحد مكونات خادم إدارة Kaspersky Security Center. 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 للهاتف. 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 14 Web Console

يحتوي Kaspersky Security Center 14 Web Console Server على شهادته الخاصة (المشار إليها فيما يلي أيضًا باسم خادم وحدة تحكم الويب Kaspersky Security Center وشهادة Kaspersky Security Center Web Console)، وهو أمر مطلوب لمصادقة Kaspersky Security Center 14 Web Console. عند فتح Kaspersky Security Center 14 Web Console، يتصل خادم وحدة تحكم الويب بخادم الإدارة. بدوره، يطلب خادم الإدارة بيانات اعتماد المستخدم وشهادة وحدة تحكم الويب للتحقق من المصادقة.

عند فتح Kaspersky Security Center 14 Web Console، يعلمك المستعرض أن الاتصال بـ Kaspersky Security Center 14 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 هذا التحذير، يمكنك القيام بأحد الإجراءات التالية:

- [استبدال 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 التحكم الإدارية وتبادل البيانات مع الأجهزة. تستخدم الشهادة كذلك للمصادقة عندما تكون خوادم الإدارة الأساسية متصلة بخوادم الإدارة الثانوية.

شهادة صادرة من Kaspersky

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

شهادة خادم الإدارة صالحة لمدة خمس سنوات، إذا تم إصدار الشهادة قبل 1 سبتمبر 2020. بخلاف ذلك، فإن مدة صلاحية الشهادة تقتصر على 397 يومًا. يتم إنشاء شهادة جديدة بواسطة خادم الإدارة كإحتياطية 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 العملية تلقائيًا لمصادقة خادم الإدارة بالشهادة الجديدة.

إذا حددت مدة صلاحية أطول من 397 يومًا لشهادة خادم الإدارة، فسيعرض مستعرض الويب خطأً.

الشهادات المخصصة

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

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")	<p>الحد الأدنى لطول المفتاح: 2048.</p> <p>القيود الأساسية:</p> <ul style="list-style-type: none"> • مرجع معتمد: صحيح • قيد طول المسار: لا شيء <p>استخدام المفتاح:</p> <ul style="list-style-type: none"> • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL <p>استخدام المفتاح الموسع (اختياري): مصادقة الخادم، مصادقة العميل.</p>	<p>معلمة استخدام المفتاح الموسع اختيارية.</p> <p>يمكن لقيمة قيد طول المسار أن تختلف عن "لا شيء"، ولكنها لا تقل عن "1".</p>
شهادة المحمول، الشهادة الاحتياطية للمحمول ("M"، "MR")	<p>الحد الأدنى لطول المفتاح: 2048.</p> <p>القيود الأساسية:</p> <ul style="list-style-type: none"> • مرجع معتمد: صحيح • قيد طول المسار: لا شيء <p>استخدام المفتاح:</p> <ul style="list-style-type: none"> • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL <p>استخدام المفتاح الموسع (اختياري): مصادقة الخادم.</p>	<p>معلمة استخدام المفتاح الموسع اختيارية.</p> <p>يمكن لقيمة قيد طول المسار أن تختلف عن "لا شيء"، إذا كان طول مسار الشهادة المشتركة لا يقل عن "1".</p>
شهادة المرجع المصدق لشهادات المستخدم التي تم إنشاؤها تلقائيًا ("MCA")	<p>الحد الأدنى لطول المفتاح: 2048.</p> <p>القيود الأساسية:</p> <ul style="list-style-type: none"> • مرجع معتمد: صحيح 	<p>معلمة استخدام المفتاح الموسع اختيارية.</p> <p>يمكن لقيمة قيد طول المسار أن تختلف عن "لا شيء"، إذا كان طول مسار الشهادة المشتركة لا يقل عن "1".</p>

	<ul style="list-style-type: none"> • قيد طول المسار: لا شيء • استخدام المفتاح: • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح • توقيع CRL <p>استخدام المفتاح الموسع (اختياري): مصادقة الخادم، مصادقة العميل.</p>	
شهادة خادم الويب	<p>استخدام المفتاح الموسع: مصادقة الخادم.</p> <p>تتضمن حاوية PEM / PKCS # 12 التي تم تحديد الشهادة منها السلسلة الكاملة للمفاتيح العامة.</p> <p>الاسم البديل للموضوع (SAN) للشهادة موجود؛ أي أن قيمة حقل subjectAltName صالحة.</p> <p>تفي الشهادة بالمتطلبات الفعالة للمستعرضات المفروضة على شهادات الخادم، فضلاً عن المتطلبات الأساسية الحالية لمنتدى CA/Browser.</p>	لا يمكن تطبيقه.
شهادة Kaspersky Security Center Web Console	<p>تتضمن حاوية PEM التي تم تحديد الشهادة منها السلسلة الكاملة للمفاتيح العامة.</p> <p>الاسم البديل للموضوع (SAN) للشهادة موجود؛ أي أن قيمة حقل subjectAltName صالحة.</p> <p>تفي الشهادة بالمتطلبات الفعالة للمستعرضات لشهادات الخادم، بالإضافة إلى المتطلبات الأساسية الحالية لمنتدى CA/Browser.</p>	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 للهيئة المخصصة لحقول الشهادة. من المفيد استبدال الشهادة فوراً بعد تثبيت خادم الإدارة وقبل انتهاء معالج البدء السريع.

إذا حددت مدة صلاحية أطول من 397 يوماً لشهادة خادم الإدارة، فسيعرض مستعرض الويب خطأً.

المتطلبات الأساسية

يجب إنشاء الشهادة الجديدة بتنسيق PKCS#12 (على سبيل المثال، عن طريق PKI الخاص بالمؤسسة) ويجب أن تكون صادرة عن مرجع مصدق موثوق به (CA). يجب أن تتضمن الشهادة الجديدة أيضاً سلسلة الثقة الكاملة والمفتاح الخاص، والتي يجب تخزينها في ملف بامتداد pfx أو p12. بالنسبة للشهادة الجديدة، يجب استيفاء المتطلبات المذكورة في الجدول أدناه.

متطلبات شهادات خادم الإدارة

نوع الشهادة	المتطلبات
الشهادة المشتركة، والشهادة الاحتياطية المشتركة ("C"، "CR")	الحد الأدنى لطول المفتاح: 2048.

القيود الأساسية:

- مرجع معتمد: صحيح
- 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.

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 ECU اختياريًا، ولكن إذا كانت شهادتك تحتوي عليه، فيجب تحديد بيانات مصادقة العميل في ECU.

الشهادات الصادرة عن مرجع مصدق عام ليس لديها إذن توقيع الشهادة. لاستخدام هذه الشهادات، تأكد من تثبيت وكيل الشبكة إصدار 13 أو أعلى 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 اتصالاتهم وسيظهر "خطأ في مصادقة خادم الإدارة". لتحديد الشهادة الجديدة واسترجاع الاتصال، استخدم خط الأوامر [الأداة المساعدة klmove](#).

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 <type> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}]  
[<[-f <time>]][-r <calistfile>][-l <logfile
```

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 معالم الأداة المساعدة klsetsrvcert في الجدول أدناه.

قيم معالم الأداة المساعدة klsetsrvcert

المعلمة	القيمة
<t <type-	نوع الشهادة المراد استبدالها. القيم المحتملة لمعلمة <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.	
الجدول الزمني لتغيير الشهادة باستخدام تنسيق "DD-MM-YYYY hh: mm" (للمنافذ 13000 و13291). استخدم هذه المعلمة إذا كنت تريد استبدال الشهادة الاحتياطية العامة أو المشتركة قبل انتهاء صلاحيتها. حدد الوقت الذي يجب أن تتزامن فيه الأجهزة المُدارة مع خادم الإدارة في شهادة جديدة.	<f <time-
حاوية تحتوي على الشهادة والمفتاح الخاص بتنسيق PKCS#12 (ملف بامتداد p12 أو pfx).	i- <<inputfile
كلمة المرور المستخدمة لحماية الحاوية p12. يتم تخزين الشهادة والمفتاح الخاص في الحاوية ، وبالتالي، فإن كلمة المرور مطلوبة لفك تشفير الملف مع الحاوية.	p- <<password
معلومات التحقق من صحة الشهادة (مفصلة بفاصلة منقوطة). لاستخدام شهادة مخصصة بدون إذن التوقيع، حدد -NoCA o في الأداة المساعدة klservcert. هذا مفيد للشهادات الصادرة عن مرجع مصدق عام.	<o <chkopt-
سيتم إنشاء شهادة جديدة لاسم DNS المحدد.	g- <<dnsname
قائمة جهة إصدار الشهادة الجذرية الموثوقة، بتنسيق PEM.	r- <<calistfile
ملف إخراج النتائج. بشكل افتراضي، يتم إعادة توجيه الإخراج إلى دفق إخراج قياسي.	l- <<logfile

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

```
klsetsrvcert -t C -i <inputfile> -p <password> -o NoCA
```

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

توصيل عملاء الشبكة بخادم الإدارة باستخدام الأداة المساعدة klmover

بعد استبدال شهادة خادم الإدارة باستخدام موجّه الأوامر [الأداة المساعدة klservcert](#)، 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 [-عنوان <عنوان الخادم>] [-pn <رقم المنفذ>] [-ps <رقم منفذ <SSL>] [-cert <المسار المؤدي إلى ملف الشهادة>]
```

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

يتم عرض وصف معلمات الأداة المساعدة klmover في الجدول أدناه.

قيم معلمات الأداة المساعدة klservcert

المعلمة	القيمة
- عنوان <server address>	عنوان خادم الإدارة للاتصال. يمكنك تحديد عنوان IP أو اسم NetBIOS أو اسم DNS.
- رقم المنفذ <port number>	رقم المنفذ الذي سيتم إنشاء اتصال غير مشفر بخادم الإدارة عن طريقه.

رقم المنفذ الافتراضي هو 14000.	رقم المنفذ <SSL port>
رقم منفذ SSL الذي يتم من خلاله إنشاء الاتصال المشفر بخادم الإدارة باستخدام SSL. رقم المنفذ الافتراضي هو 13000.	<number>
استخدام اتصال غير مشفر بخادم الإدارة. إذا لم يكن المفتاح قيد الاستخدام، فسيتم توصيل عميل الشبكة بخادم الإدارة باستخدام بروتوكول SSL المشفر.	-nossl
استخدم ملف الشهادة المحدد لمصادقة الوصول إلى خادم الإدارة.	cert <path to certificate-><file>

إعادة إصدار شهادة خادم الويب

شهادة **خادم الويب** المستخدمة في برنامج Kaspersky Security Center مطلوبة لنشر حزم تثبيت عميل الشبكة التي تقوم بتنزيلها لاحقاً 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 المدارة 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 مطلقاً 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 مدارة 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 يتم فتحها، حدد قسم **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 **إعادة الإصدار**.

b. في نافذة **إعادة إصدار الشهادة** التي تفتح، في مجموعة إعدادات **عنوان الاتصال ومدة 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 تفي **بمتطلبات Kaspersky Security Center ومتطلبات الشهادات المصدق عليها من شركة Apple**. 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 #12 PKCS**، 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 (.pem, .prk)**، 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 وجهازها للاستخدام في برنامج **Kaspersky Security Center**. تحقق مما إذا كانت شهادتك المخصصة تفي **بمتطلبات Kaspersky Security Center** ومتطلبات **الشهادات المصدق عليها من شركة Apple**. إذا اقتضى الأمر ذلك، فقم بتعديل الشهادة.

يمكنك استخدام **الأداة المساعدة kliosrvcertgen.exe** في إنشاء 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 قسم **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 #12 PKCS**، 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 (.pem, .prk)**، 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**.

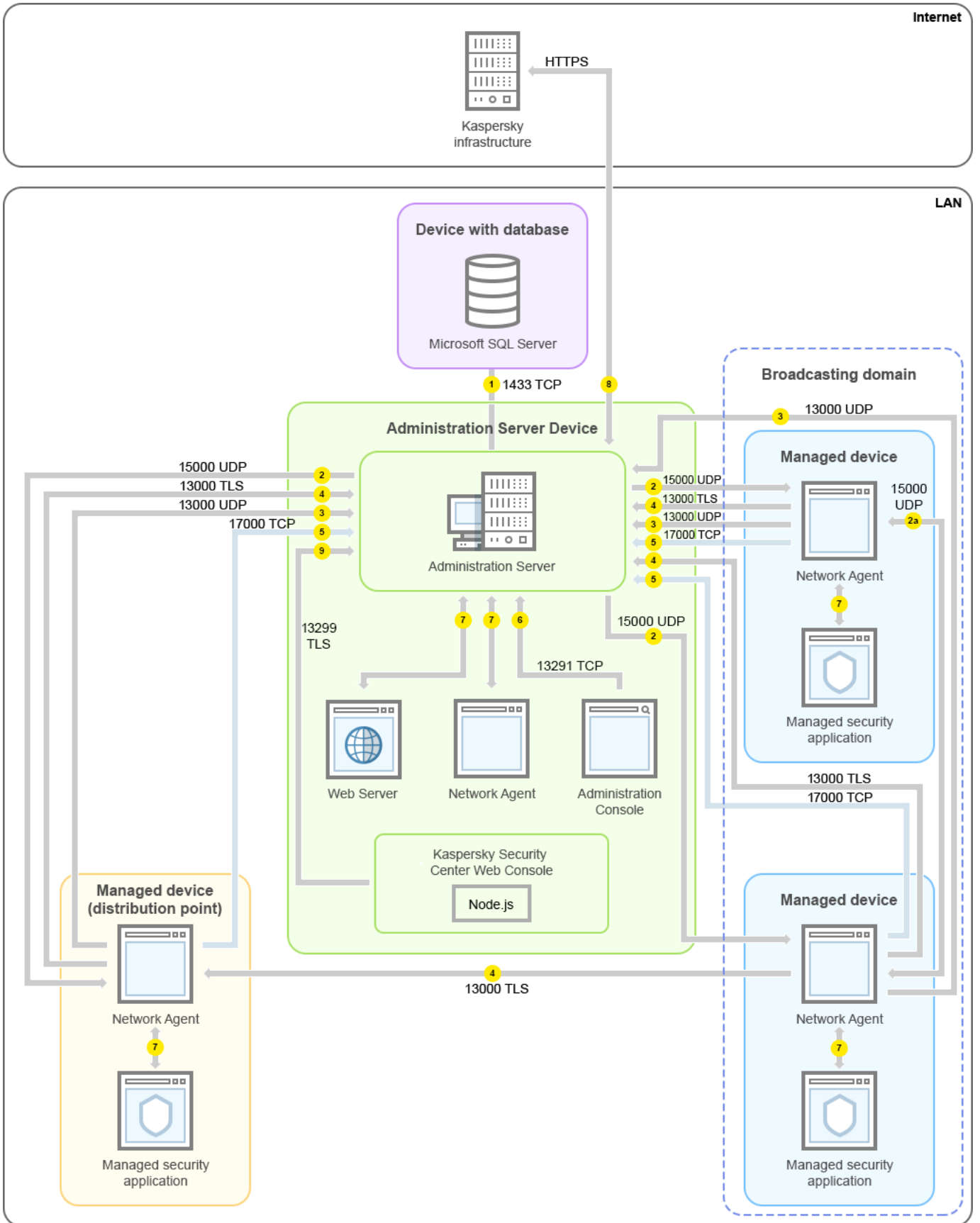
8. إذا اقتضى الأمر ذلك، من نافذة **خصائص خادم الإدارة**، في حقل **منفذ HTTPS لخادم الويب**، غير رقم منفذ HTTPS لخادم الويب. انقر فوق **موافق**. يتم إعادة إصدار شهادة خادم الويب.

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 المُدارة 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 المدارة 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، وتفصيل 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 و MariaDB 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 المحملة 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).

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 SSL رقم 13000.

إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر منفذ رقم 14000 غير مستند إلى SSL. كما يدعم Kaspersky Security Center اتصال عملاء الشبكة عبر منفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ SSL 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.)

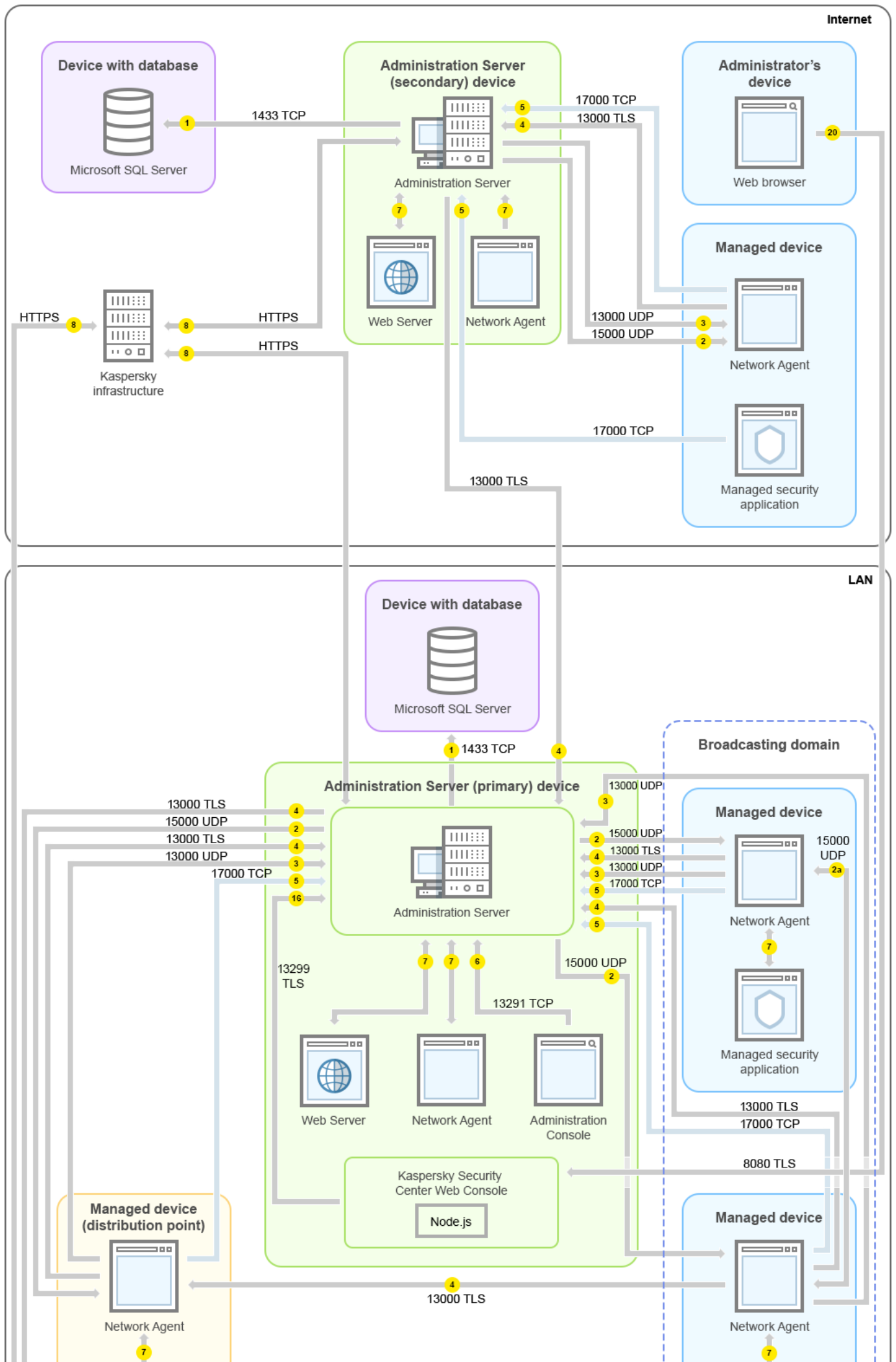
7. تتبادل التطبيقات الموجودة على جهاز واحد حركة البيانات المحلية (إما على خادم الإدارة أو على جهاز مدار). ولا يتعين فتح أي موانئ خارجية.

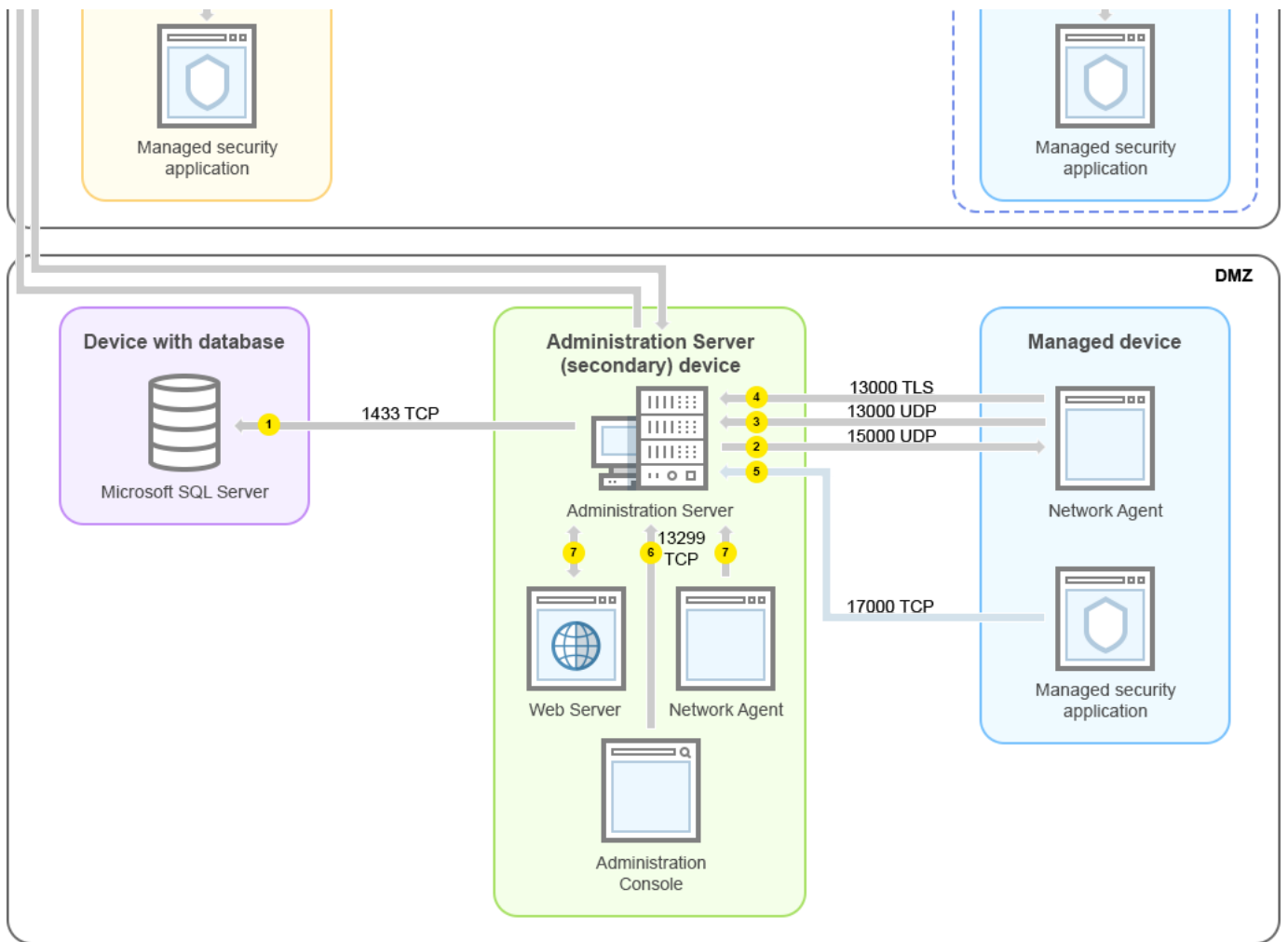
8. يتم نقل البيانات من خادم الإدارة إلى خوادم Kaspersky (مثل: بيانات شبكة KSN أو معلومات عن التراخيص)، والبيانات من خوادم Kaspersky إلى خادم الإدارة (مثل: تحديثات التطبيقات وتحديثات قاعدة بيانات مكافحة الفيروسات) عبر بروتوكول HTTPS. إذا كنت لا تريد أن يكون لخادم الإدارة الخاص بك اتصالاً بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل خادم Kaspersky Security Center Web Console 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 الموصولة مباشرة بالإنترنت (DMZ)؛ خادم إدارة تابع آخر متصل بالإنترنت.





التسليم الهرمي لخدمات 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 و MariaDB 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 المحملة 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).
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 SSL رقم 13000. إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر منفذ رقم 14000 غير مستند إلى SSL. كما يدعم Kaspersky Security Center اتصال عملاء الشبكة عبر منفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ SSL رقم 13000.

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

5. الأجهزة المدارة (باستثناء الأجهزة المحملة) 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 المحليّة (إما على خادم الإدارة أو على جهاز مدار). ولا يتعين فتح أي موانئ خارجية.

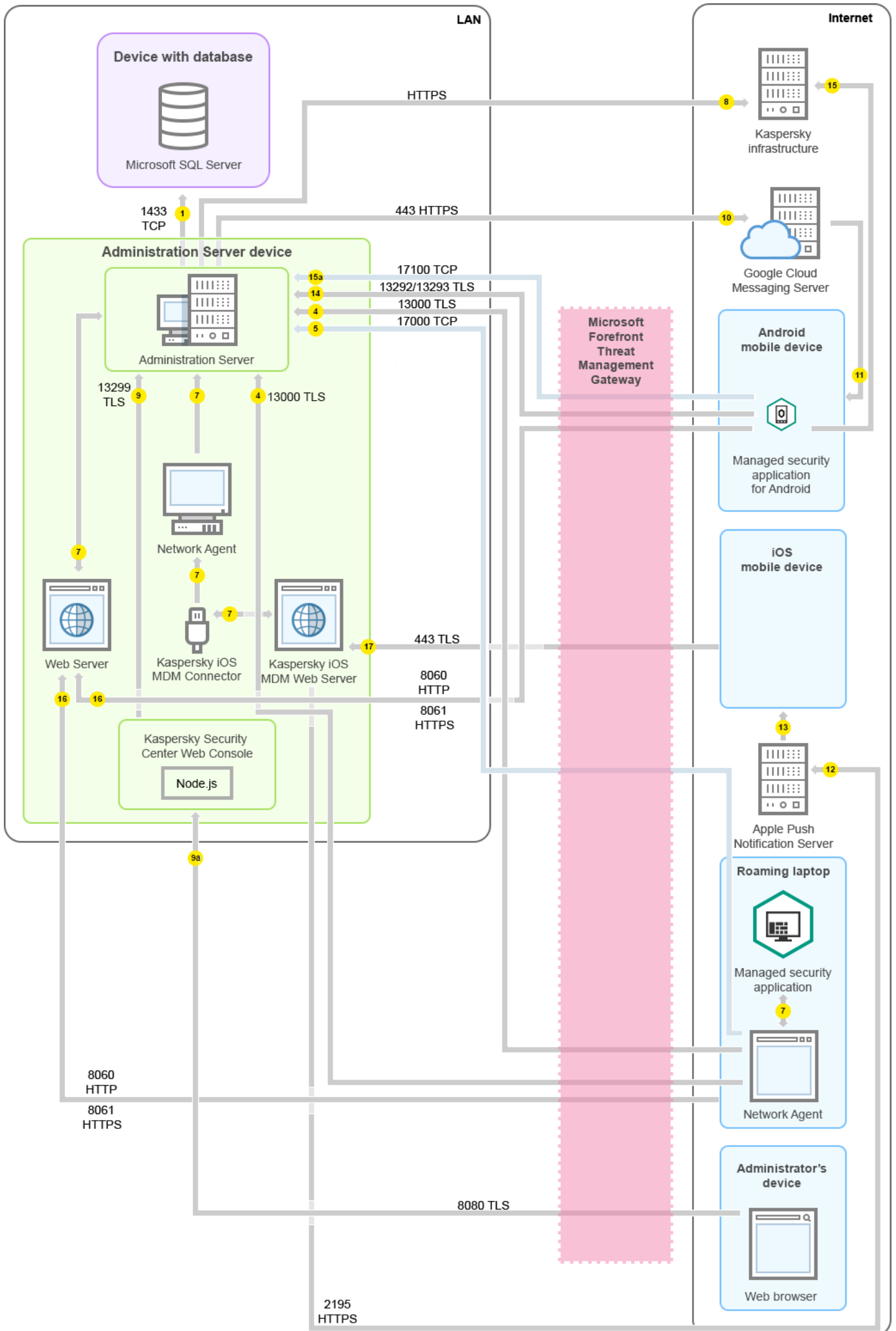
8. يتم نقل البيانات من خادم الإدارة إلى خوادم Kaspersky (مثل: بيانات شبكة KSN أو معلومات عن التراخيص)، والبيانات من خوادم Kaspersky إلى خادم الإدارة (مثل: تحديثات التطبيقات وتحديثات قاعدة بيانات مكافحة الفيروسات) عبر بروتوكول HTTPS. إذا كنت لا تريد أن يكون لخادم الإدارة الخاص بك اتصالاً بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center 14 Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو جهاز آخر، عبر منفذ TLS رقم 13299.

9A. يتم نقل البيانات من المستعرض، المثبت على جهاز منفصل للمسؤول، إلى خادم Kaspersky Security Center 14 Web Console Server [عبر منفذ TLS رقم 8080](#). يمكن تثبيت Kaspersky Security Center 14 Web Console Server على خادم الإدارة أو على جهاز آخر.

خادم الإدارة في شبكة الاتصال المحلية (LAN)، الأجهزة المتصلة بالإنترنت، TMG قيد الاستخدام

يوضح الشكل التالي حالة نقل البيانات إذا كان خادم الإدارة موجودًا في شبكة الاتصال المحلية (LAN) وكانت الأجهزة المتصلة بالإنترنت. في هذا الشكل، تجد (Microsoft Forefront Threat Management Gateway (TMG) قيد الاستخدام. لكن إذا كنت تريد استخدام جدار حماية مؤسسة، فيمكنك استخدام تطبيق مختلف، وراجع وثائق التطبيق الذي تختاره لمزيد من التفاصيل.



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 الموصولة مباشرة بالإنترنت (DMZ).

تشير الأسهم إلى بدء نقل البيانات: يشير كل سهم من جهاز يبدأ الاتصال إلى الجهاز الذي "يرد" على المكالمات. 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 و MariaDB 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).

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 SSL رقم 13000**.

إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر منفذ رقم 14000 غير مستند إلى SSL. كما يدعم Kaspersky Security Center اتصال عملاء الشبكة عبر منفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ SSL 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 المحليّة (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 اتصالاً بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center 14 Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو جهاز آخر، عبر **منفذ TLS رقم 13299**.

9A. يتم نقل البيانات من المستعرض، المثبت على جهاز منفصل للمسؤول، إلى خادم Kaspersky Security Center 14 Web Console Server عبر **منفذ TLS رقم 8080**. يمكن تثبيت Kaspersky Security Center 14 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 يجب عليها الاتصال بخادم الإدارة.

14. بالنسبة إلى الأجهزة المحمولة فقط: يتم نقل البيانات من التطبيق المدار إلى خادم الإدارة (أو إلى بوابة الاتصال) عبر منفذ TLS رقم 13292/13293- مباشرةً أو عبر (Microsoft Forefront Threat Management Gateway (TMG).

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

15A. إذا كان الجهاز المحمول لا يملك صلاحية الوصول إلى الإنترنت، تُرسل البيانات إلى خادم الإدارة عبر منفذ 17100 ثم يُرسلها خادم الإدارة إلى بنية Kaspersky التحتية، ولكن لا يُستخدم هذا السيناريو إلا فيما ندر.

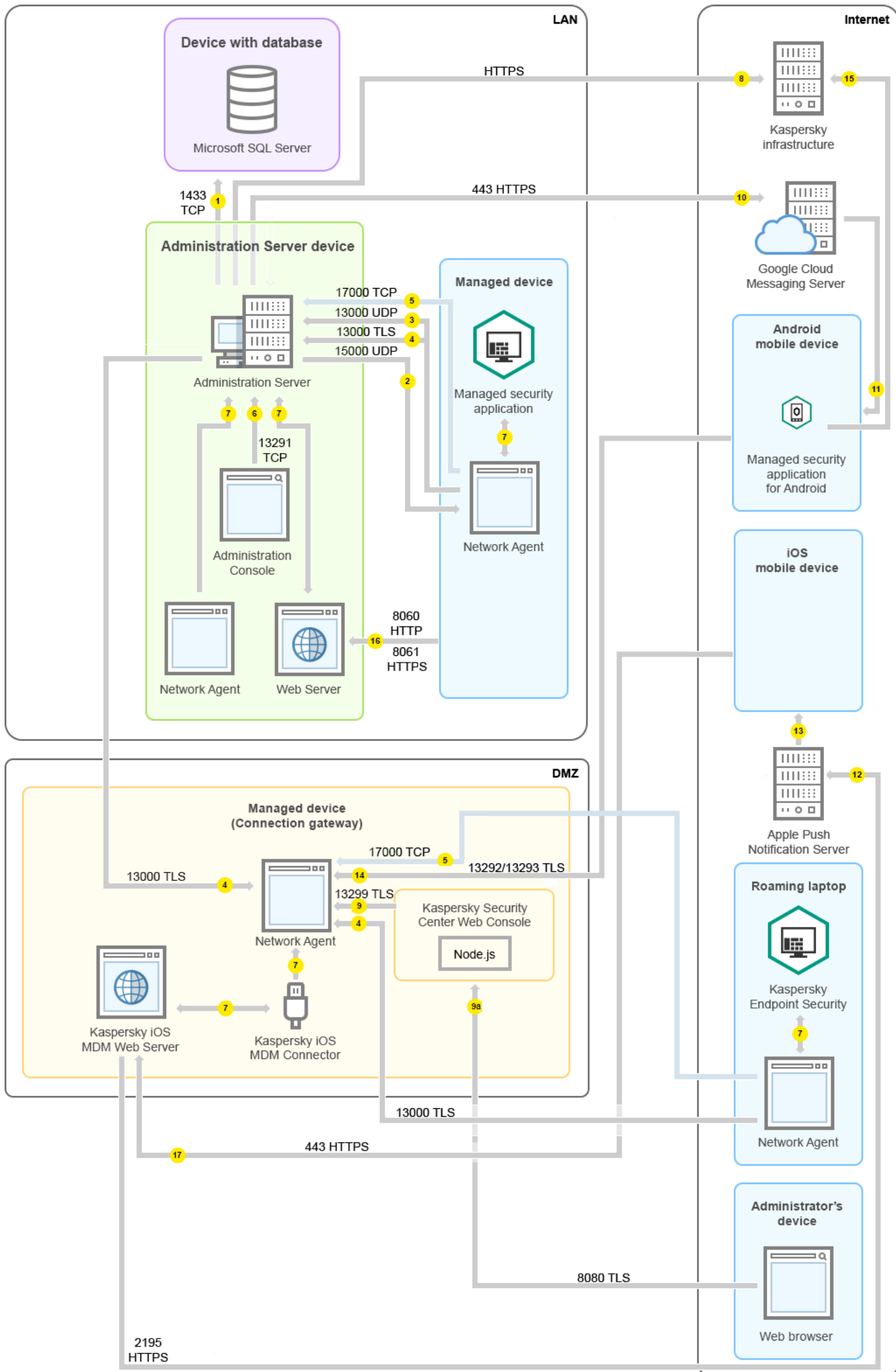
16. يتم نقل طلبات الحرّم من الأجهزة المدارة، وتشمل الأجهزة المحمولة، إلى خادم الويب الموجود على الجهاز نفسه الذي به خادم الإدارة.

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، المثبت على الجهاز نفسه المثبت 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.

يُوصى بمخطط النشر هذا إذا كنت لا ترغب في أن تتصل الأجهزة المحمولة بخادم الإدارة مباشرةً ولا ترغب في استخدام Microsoft Forefront Threat Management Gateway (TMG) أو جدار حماية مؤسسة.



في هذا الشكل، تتصل الأجهزة المدارة بخادم الإدارة عبر بوابة اتصال موجودة في منطقة الأجهزة الموصولة مباشرة بالإنترنت (DMZ). لا يوجد TMG أو جدار حماية مؤسسة قيد الاستخدام.

تشير الأسهم إلى بدء نقل البيانات: يشير كل سهم من جهاز يبدأ الاتصال إلى الجهاز الذي "يرد" على المكالمات. 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 و MariaDB 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).

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 SSL رقم 13000.

إذا كنت تستخدم نسخة أقدم من Kaspersky Security Center، يمكن أن يتلقى خادم الإدارة الموجود في شبكتك الاتصالات من عملاء الشبكة عبر منفذ رقم 14000 غير مستند إلى SSL. كما يدعم Kaspersky Security Center اتصال عملاء الشبكة عبر منفذ رقم 14000، على الرغم من أنه يُوصى باستخدام منفذ SSL 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 المحليّة (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 اتصالاً بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center 14 Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو جهاز آخر، عبر منفذ TLS رقم 13299.

9A. يتم نقل البيانات من المستعرض، المثبت على جهاز منفصل للمسؤول، إلى خادم Kaspersky Security Center 14 Web Console Server عبر منفذ TLS رقم 8080. يمكن تثبيت Kaspersky Security Center 14 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 يجب عليها الاتصال بخادم الإدارة.

14. بالنسبة إلى الأجهزة المحمولة فقط: يتم نقل البيانات من التطبيق المدار إلى خادم الإدارة (أو إلى بوابة الاتصال) عبر منفذ TLS رقم 13292/13293- مباشرة أو عبر (Microsoft Forefront Threat Management Gateway (TMG).

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

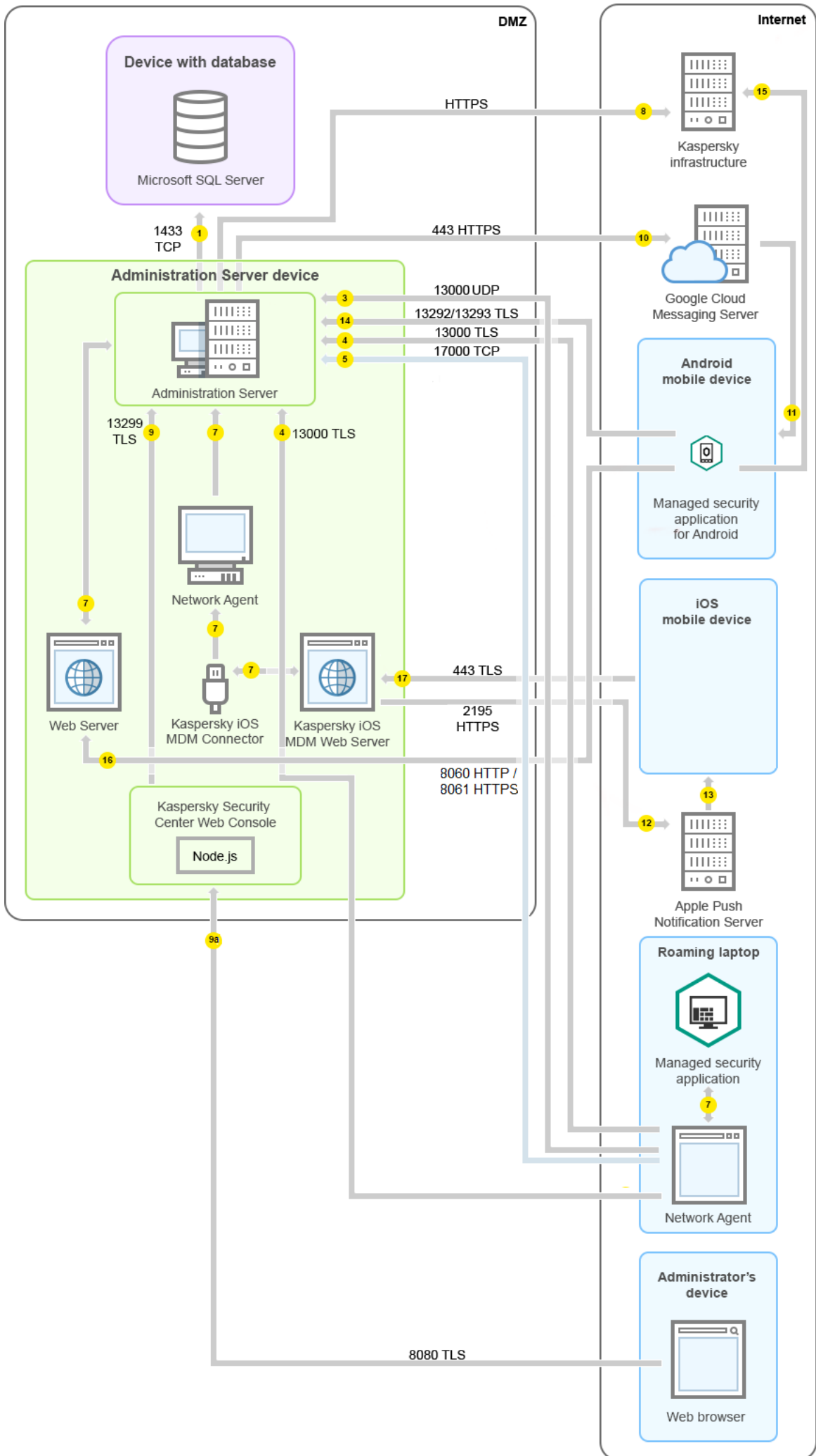
15A. إذا كان الجهاز المحمول لا يملك صلاحية الوصول إلى الإنترنت، تُرسل البيانات إلى خادم الإدارة عبر منفذ 17100 ثم يُرسلها خادم الإدارة إلى بنية Kaspersky التحتية، ولكن لا يُستخدم هذا السيناريو إلا فيما ندر.

16. يتم نقل طلبات الحزم 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، المثبت على الجهاز نفسه المثبت عليه خادم الإدارة أو على بوابة الاتصال.

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

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

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 SSL رقم 13000.

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

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

4A. تستقبل بوابة الاتصال الموجودة في منطقة الأجهزة الموصولة مباشرة بالإنترنت اتصالاً من خادم الإدارة عبر منفذ SSL 13000. نظرًا لأن بوابة الاتصال في منطقة DMZ لا يمكنها الوصول إلى منافذ خادم الإدارة، يقوم خادم الإدارة بإنشاء اتصال إشارة دائم مع بوابة اتصال والحفاظ 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 SSL 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 المحليّة (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 اتصالاً بالإنترنت، فيجب عليك إدارة هذه البيانات يدويًا.

9. يُرسل Kaspersky Security Center 14 Web Console Server البيانات إلى خادم الإدارة، الذي قد يكون مثبتًا على الجهاز نفسه أو جهاز آخر، عبر منفذ TLS رقم 13299.

9A. يتم نقل البيانات من المستعرض، المثبت على جهاز منفصل للمسؤول، إلى خادم Kaspersky Security Center 14 Web Console Server عبر منفذ TLS رقم 8080. يمكن تثبيت Kaspersky Security Center 14 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. بالنسبة إلى الأجهزة المحمولة فقط: يتم نقل البيانات من التطبيق المدار إلى خادم الإدارة (أو إلى بوابة الاتصال) عبر منفذ TLS رقم 13292/13293 – مباشرةً أو عبر (Microsoft Forefront Threat Management Gateway (TMG).

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

15A. إذا كان الجهاز المحمول لا يملك صلاحية الوصول إلى الإنترنت، تُرسل 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 الحزم 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، المثبت على الجهاز نفسه المثبت 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.

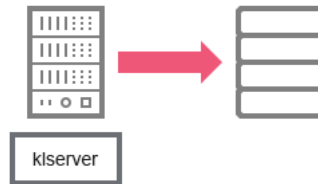
مصطلحات المستندات

الرمز	المعنى
	خادم الإدارة
	خادم الإدارة الثانوي
	نظام إدارة قاعدة البيانات
	جهاز عميل (يحتوي على عميل الشبكة وتطبيق مثبت 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	
عملية تعمل على الجهاز وتفتح منفذاً	
المنفذ ورقمه	13000 TLS 
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 DMZ	

خادم الإدارة ونظام إدارة قواعد البيانات

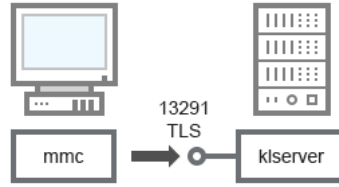
البيانات من خادم الإدارة تدخل قاعدة بيانات SQL Server أو MySQL أو MariaDB.



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 و MariaDB 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

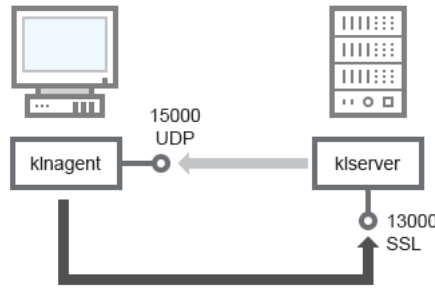
للحصول على توضيحات للمخطط، راجع الجدول أدناه.

خادم الإدارة ووحدة تحكم الإدارة (حركة المرور)

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

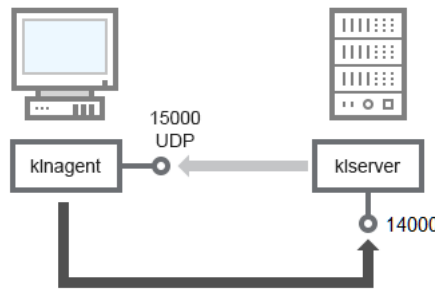
خادم الإدارة والجهاز العميل: إدارة تطبيق الأمان

يتلقى خادم الإدارة الاتصال من عملاء الشبكة عبر منفذ SSL 13000 (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 14 أيضاً اتصال عملاء الشبكة عبر منفذ 14000، على الرغم من أنه من المستحسن استخدام منفذ SSL 13000.



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

لتوضيح المخططات، راجع الجدول الموضح أدناه.

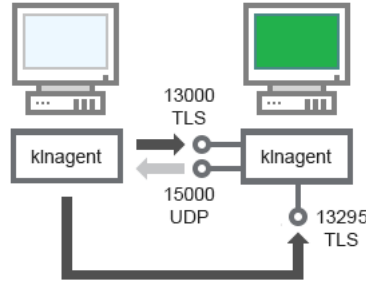
خادم الإدارة والجهاز العميل: إدارة تطبيق الأمان (حركة المرور)

الجهة	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS (لمنفذ TCP فقط)	غرض المنفذ
عميل الشبكة	15000	klnagent	UDP	خالي	الإرسال المتعدد لعملاء الشبكة
خادم الإدارة	13000	kserver	TCP	نعم	تلقي اتصالات من عملاء الشبكة

تلقى اتصالات من عملاء الشبكة	لا	TCP	klserver	14000	خادم الإدارة
------------------------------	----	-----	----------	-------	--------------

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).



ترقية البرنامج على جهاز عميل خلال نقطة توزيع

للحصول على توضيحات للمخطط، راجع الجدول أدناه.

ترقية برنامج من خلال نقطة توزيع (حركة المرور)

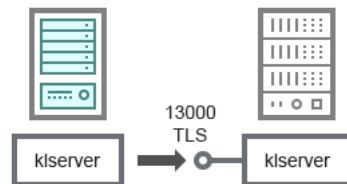
الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS (لمنفذ TCP فقط)	غرض المنفذ
عميل الشبكة	15000	klnagent	UDP	خالي	الإرسال المتعدد لعملاء الشبكة
نقطة توزيع	13000	klnagent	TCP	نعم	تلقى اتصالات من عملاء الشبكة
نقطة توزيع	13295	klnagent	TCP	نعم	إرسال الإشعارات إلى الأجهزة العميلة

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 كلاهما باستخدام وحدة تحكم إدارة متصلة بخادم الإدارة الرئيسي. لذلك، فإن إمكانية الوصول إلى المنفذ 13291 الخاص بالخادم الرئيسي هو المتطلب الأساسي الوحيد.



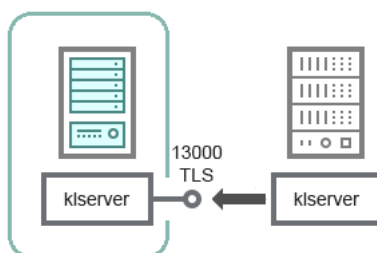
التسلسل الهرمي لخوادم الإدارة: خادم الإدارة الرئيسي وخادم الإدارة الثانوي

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	تلقى اتصالات من خوادم إدارة ثانوية

التسلسل الهرمي لخوادم الإدارة مع خادم إدارة تابع في DMZ



التسلسل الهرمي لخوادم الإدارة مع خادم إدارة تابع في DMZ

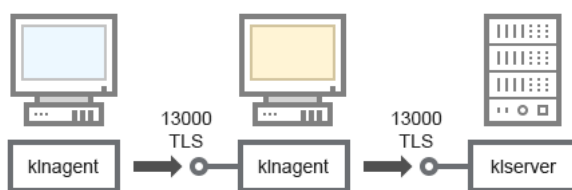
يعرض المخطط تسلسل رقمي لخوادم الإدارة والذي يقوم فيه خادم الإدارة الثانوي الموجودة في DMZ بتلقي اتصال من خادم الإدارة الرئيسي (راجع الجدول أدناه لمطالعة توضيحات المخطط). عند الجمع بين خادمي إدارة في تسلسل هرمي، تأكد من أنه يمكن الوصول إلى المنفذ 13291 على خادمي الإدارة كليهما. تتصل وحدة تحكم الإدارة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

المنفذ	البروتوكول	اسم العملية التي تفتح المنفذ	رقم المنفذ	الجهاز
13000	TCP	kserver	13000	خادم الإدارة الثانوي
	نعم	TLS		تلقى اتصالات من خادم الإدارة الرئيسي

خادم الإدارة وبوابة اتصال في قطاع شبكة وجهاز عميل



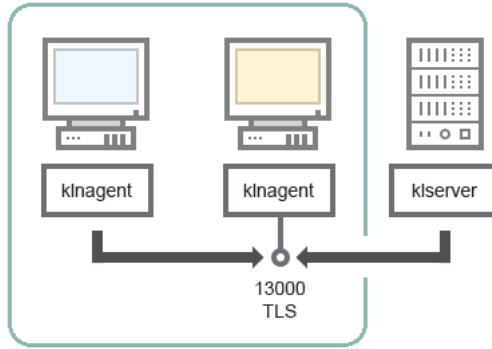
خادم الإدارة وبوابة اتصال في قطاع شبكة وجهاز عميل

للحصول على توضيحات للمخطط، راجع الجدول أدناه.

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

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

خادم الإدارة وجهازان في DMZ: بوابة الاتصال وجهاز عميل



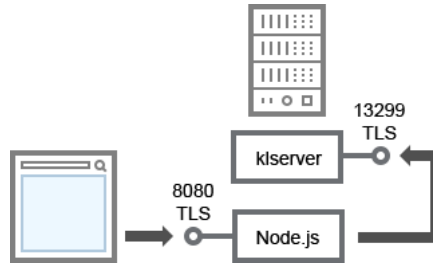
خادم إدارة مع بوابة اتصال وجهاز عميل في DMZ

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 و Kaspersky Security Center 14 Web Console



خادم الإدارة و Kaspersky Security Center 14 Web Console

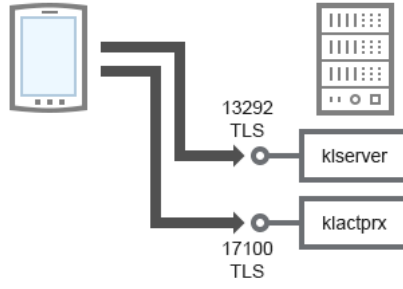
للحصول على توضيحات للمخطط، راجع الجدول أدناه.

خادم الإدارة و Kaspersky Security Center 14 Web Console (حركة المرور)

الجهاز	رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	TLS	غرض المنفذ
خادم الإدارة	13299	kserver	TCP	نعم	تلقي اتصالات من Kaspersky Security Center 14 Web Console إلى خادم الإدارة عبر OpenAPI
Kaspersky Security Center 14 Web Console أو خادم الإدارة	8080	Node.js: جافا سكريبت من جانب الخادم	TCP	نعم	تلقي اتصالات من Kaspersky Security Center 14 Web Console

يمكن تثبيت Kaspersky Security Center 14 Web Console على خادم الإدارة أو على جهاز آخر.

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	klserver	TCP	نعم	تلقي اتصالات لتفعيل التطبيق من الأجهزة المحمولة

أفضل ممارسات النشر

يُعتبر Kaspersky Security Center تطبيقاً موزعاً. 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 يشغلها المسؤول.
- عميل الشبكة—تم تصميمه لإدارة تطبيق الأمان المثبت 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

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

التخطيط لنشر Kaspersky Security Center

يوفر هذا القسم معلومات حول الاختيارات الأكثر ملاءمة 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 بتنصيب 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 14 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 14 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) لكل 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 Security Center على الإنترنت (انظر القسم [التكوين القياسي: مكاتب صغيرة متعددة بعيدة](#)).

يقدم 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 مفيداً في الحالات التالية (قائمة جزئية):

- فحص حركة مرور طبقة مأخذ التوصيل الأمانة (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 للشبكة 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 جغرافياً تُدار بواسطة مسؤوليها

• مكاتب صغيرة متعددة، منفصلة جغرافياً

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 المُدارة.

يمكن لخادم إدارة واحد دعم ما يصل إلى 100000 جهاز. يجب عليك وضع احتمالية زيادة عدد الأجهزة المُدارة 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 مطلوباً أم لا.

في حالة استخدام خوادم متعددة، فمن المستحسن الجمع بينها في ترتيب هرمي. يتيح لك استخدام الترتيب الهرمي لخوادم الإدارة تجنب السياسات والمهام المسماة والتعامل مع مجموعة الأجهزة المُدارة بالكامل كما لو أنها تتم إدارتها بواسطة خادم إدارة واحد (أي البحث عن أجهزة وبناء تحدييدات 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 جغرافياً، 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).

في حالة انتقال بعض الموظفين بين المكاتب مع أجهزتهم (أجهزة الكمبيوتر المحمولة)، يجب إنشاء قاعدة لتحويل عميل الشبكة بين خوادم الإدارة في سياسة عميل الشبكة.

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 موجوداً 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 مباشرةً 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 UDP 15000 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.

كيفية اختيار نظام إدارة قواعد البيانات (DBMS) لخادم إدارة

عند اختيار نظام إدارة قواعد البيانات (DBMS) الذي سيستخدمه خادم الإدارة، يجب عليك الأخذ في الاعتبار عدد الأجهزة التي يغطيها خادم الإدارة.

يحتوي SQL Server Express Edition على قيود على حجم الذاكرة المستخدمة وعدد مراكز وحدة المعالجة المركزية (CPU) المستخدمة وأقصى حجم لقاعدة البيانات. لذا، لا يمكنك استخدام إصدار خادم SQL Express إذا كان خادم الإدارة الخاص بك يغطي أكثر من 10000 جهاز، أو في حال استخدام التحكم في التطبيقات على الأجهزة المدارة.

إذا كان خادم الإدارة الخاص بك يغطي أكثر من 10000 جهاز، ننصحك باستخدام إصدارات خادم SQL Server تحتوي على قيود أقل، مثل: SQL Server Workgroup Edition أو خادم SQL Server® Web Edition أو SQL Server Standard Edition أو SQL Server Enterprise Edition.

إذا كان خادم الإدارة يغطي 50000 جهاز (أو أقل) وفي حال عدم استخدام وحدة التحكم في التطبيقات على الأجهزة المدارة، يمكنك كذلك استخدام MySQL 8.0.20 والإصدارات الأحدث.

إذا كان خادم الإدارة يغطي 20000 جهاز (أو أقل) وفي حال عدم استخدام التحكم في التطبيقات على الأجهزة المدارة، يمكنك استخدام MariaDB 10.3 كنظام إدارة قاعدة البيانات (DBMS).

إذا كان خادم الإدارة يغطي 10000 جهاز (أو أقل) وفي حالة عدم استخدام مكوّن التحكم في التطبيقات على الأجهزة المدارة، يمكنك كذلك استخدام MySQL 5.5 أو 5.6 أو 5.7 كنظام إدارة قواعد البيانات (DBMS).

إصدارات MySQL 5.5.1 و 5.5.2 و 5.5.3 و 5.5.4 و 5.5.5 لم تعد مدعومة.

إذا كنت تستخدم SQL Server 2019 كنظام DBMS ولم يكن لديك التصحيح التراكمي CU12 أو إصدار أحدث، فيجب عليك تنفيذ ما يلي بعد تثبيت Kaspersky Security Center:

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
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. أعد تشغيل خدمة SQL Server 2019.

وإلا، فإن استخدام SQL Server 2019 قد ينتج عنه أخطاء، مثل "لا توجد ذاكرة كافية على النظام في وعاء الموارد 'الداخلي' لتشغيل هذا الاستعلام".

تحديد نظام إدارة قواعد البيانات

عند تثبيت خادم الإدارة، يمكنك تحديد نظام إدارة قواعد البيانات الذي سيستخدمه خادم 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 قيود استخدامها.

قيود استخدام نظام إدارة قاعدة البيانات

القيود	نظام إدارة قاعدة البيانات
لا يوصى به إذا كنت تنوي تشغيل خادم إدارة واحد لأكثر من 10,000 جهاز أو استخدام التحكم في التطبيقات.	إصدار SQL Server Express Edition 2012 أو الإصدار الأحدث.
بلا قيود.	إصدار 2012 أو الإصدارات الأحدث من خادم SQL Server المحلي، غير الإصدار Express.
صالح فقط في حالة وجود الجهازين في مجال Windows® نفسه؛ وفي حالة اختلاف المجالات، يجب إنشاء علاقة ثقة ثنائية بينهم.	إصدار 2012 من SQL Server البعيد، غير الإصدار Express، أو الإصدار الأحدث.
لا يوصى به إذا كنت تنوي تشغيل خادم إدارة واحد لأكثر من 10,000 جهاز أو استخدام التحكم في التطبيقات.	إصدارات MySQL 5.5 أو 5.6 أو 5.7 المحلية أو البعيدة (لم تعد إصدارات MySQL 5.5.1 و 5.5.2 و 5.5.3 و 5.5.4 و 5.5.5 مدعومة)
لا يوصى به إذا كنت تنوي تشغيل خادم إدارة واحد لأكثر من 50,000 جهاز أو استخدام التحكم في التطبيقات.	MySQL 8.0.20 محلي أو عن بُعد أو إصدار أحدث
لا يوصى به إذا كنت تنوي تشغيل خادم إدارة واحد لأكثر من 20,000 جهاز أو استخدام التحكم في التطبيقات.	MariaDB Server 10.3 المحلي أو البعيد

إذا كنت تستخدم SQL Server 2019 كنظام DBMS ولم يكن لديك التصحيح التراكمي CU12 أو إصدار أحدث، فيجب عليك تنفيذ ما يلي بعد تثبيت Kaspersky Security Center:

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
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
GO
```

3. أعد تشغيل خدمة SQL Server 2019.

وإلا، فإن استخدام SQL Server 2019 قد ينتج عنه أخطاء، مثل "لا توجد ذاكرة كافية على النظام في وعاء الموارد 'الداخلي' لتشغيل هذا الاستعلام".

إدارة الأجهزة المحمولة باستخدام Kaspersky Endpoint Security for Android

تتم إدارة الأجهزة المحمولة المثبت عليها Kaspersky Endpoint Security for Android™ (يُشار إليها فيما بعد باسم أجهزة KES) بواسطة خادم الإدارة. يدعم Kaspersky Security Center 10 Service Pack 1، بالإضافة إلى الإصدارات الأحدث، المزايا 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 Windows المنتشرة 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 الطرف الثالث 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 DMZ

إذا كان خادم الإدارة موجودًا في DMZ 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 لعمل الشبكة عبر التثبيت الإجباري على الأجهزة الموجودة في الشبكة الداخلية للمؤسسة.

ينطبق هذا على التثبيت الأولي فقط لعمل الشبكة. يمكن القيام بأي ترقيات إضافية لعمل الشبكة أو تثبيت تطبيق الأمان، من ناحية أخرى، بواسطة خادم الإدارة. في الوقت نفسه، يمكن القيام بالنشر الأولي لعملاء الشبكة بطرق أخرى، على سبيل المثال من خلال سياسات المجموعة الخاصة بـ Microsoft ActiveDirectory®.

• 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. وكنتيجه 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 إعلانات 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 DMZ

يمكن أن يتواجد خادم الإدارة في الشبكة الداخلية للمؤسسة، كما يمكن أن يتواجد في منطقة DMZ 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 الموصولة 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 الموصولة مباشرة بالإنترنت حسب العنوان**.

• لاستخدام اتصال الإنترنت في توصيل أجهزة كمبيوتر سطح المكتب 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 الموصولة 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 الموصولة 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 لعمل 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 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 مباشرة. يمكن أن يكون هذا الوضع مفيداً في السيناريوهات التي لا تسمح بتأسيس اتصال مباشر بين خادم الإدارة والأجهزة المُدارة.

حساب عدد نقاط التوزيع وتكوينهم

كلما زاد عدد الأجهزة العملية 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 العملية كبيراً إلى حد ما ويقوم بتحديد تكوينهم.

استخدام نقاط التوزيع المعينة بشكل حصري

إذا كنت تخطط لاستخدام أجهزة محددة كنقاط توزيع (أي الخوادم المخصصة حصرياً)، 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 حصرياً في شبكة تحتوي على مقطع شبكة واحد بناءً على عدد الأجهزة المتصلة بالشبكة

عدد نقاط التوزيع	عدد الأجهزة العملية في مقطع الشبكة
0 (لا يتم بتعيين نقاط توزيع)	أقل من 300
مقبول: $(N/10,000 + 1)$ ، موصى به: $(N/5000 + 2)$ ، حيث N هو عدد الأجهزة المتصلة بالشبكة	أكثر من 300

عدد نقاط التوزيع التي تم تعيينها حصرياً في شبكة تحتوي على مقاطع شبكات متعددة بناءً على عدد الأجهزة المتصلة بالشبكة

عدد نقاط التوزيع	عدد الأجهزة العملية لكل مقطع شبكة
0 (لا يتم بتعيين نقاط توزيع)	أقل من 10
1	10-100
مقبول: $(N/10,000 + 1)$ ، موصى به: $(N/5000 + 2)$ ، حيث N هو عدد الأجهزة المتصلة بالشبكة	أكثر من 100

استخدام الأجهزة العملية القياسية (محطات العمل) كنقاط توزيع

إذا كنت تخطط لاستخدام أجهزة عملية 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 نقاط التوزيع	عدد الأجهزة العملية في مقطع الشبكة
0 (لا يتم بتعيين نقاط توزيع)	أقل من 300
$(N/300 + 1)$ ، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل	أكثر من 300

عدد محطات العمل التي تعمل كنقاط توزيع في شبكة تحتوي على مقاطع شبكات متعددة بناءً على عدد الأجهزة المتصلة بالشبكة

عدد نقاط التوزيع	عدد الأجهزة العملية لكل مقطع شبكة
0 (لا يتم بتعيين نقاط توزيع)	أقل من 10
1	10-30
2	30-300
$(N/300 + 1)$ ، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل	أكثر من 300

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 لاثنتين 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.

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 المخصص لمجموعات الإدارة للأجهزة المخصصة مع السياسات والمهام، يتميز كل خادم إدارة افتراضي بمجموعته الخاصة من الأجهزة غير المعينة ومجموعات التقارير الخاصة والأجهزة والأحداث المحددة وحزم التثبيت وقواعد النقل... إلخ. يمكن لمزودي الخدمة (xSP) استخدام النطاق الوظيفي لخوادم الإدارة الافتراضية لزيادة عزل العملاء إلى أقصى حد، وكذلك تستخدمها المؤسسات الكبيرة ذات تدفقات العمل المعقدة والعديد من المسؤولين.

خوادم الإدارة الافتراضية تشبه إلى حد كبير خوادم الإدارة الثانوية، ولكن مع الفروق التالية:

- يفقد 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

القيمة	نوع القيد
100,000	العدد الأقصى للأجهزة المدارة لكل خادم إدارة
300	الحد الأقصى لعدد الأجهزة التي تم تحديد خيار عدم قطع الاتصال عن خادم الإدارة عليها
10,000	الحد الأقصى لعدد مجموعات الإدارة
45,000,000	الحد الأقصى لعدد الأحداث التي سيتم تخزينها
2000	الحد الأقصى لعدد السياسات
2000	الحد الأقصى لعدد المهام
1,000,000	الحد الأقصى للعدد الإجمالي لعناصر الوحدات التنظيمية Active Directory، وحسابات المستخدمين، والأجهزة، ومجموعات الأمان
100	الحد الأقصى لعدد ملفات التعريف في سياسة ما
500	الحد الأقصى لعدد خوادم الإدارة الثانوية على خادم إدارة أساسي واحد
500	الحد الأقصى لعدد خوادم الإدارة الافتراضية
10,000	الحد الأقصى لعدد الأجهزة التي يمكن أن تغطيها نقطة توزيع واحدة (تستطيع نقاط التوزيع تغطية الأجهزة غير المحمولة فقط)
10000، بما في ذلك الأجهزة المحمولة	الحد الأقصى لعدد الأجهزة التي قد تستخدم بوابة اتصال واحدة
100000 ناقص عدد الأجهزة المدارة الثابتة	العدد الأقصى للأجهزة المحمولة لكل خادم إدارة

يحتوي هذا القسم على معلومات حول حجم حركة مرور الشبكة التي تتبادلها الأجهزة العميلة و خادم 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 حول قيم حركة المرور بعد تثبيت عميل الشبكة الإصدار 14 و Kaspersky 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 و Kaspersky 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	69,990.4	259,317.76	329,318.4
إجمالي حركة المرور (جهاز عميل فردي)، بالكيلو بايت	71,628.8	267,161.6	339,025.92

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 ميغا بايت
- حركة البيانات من خادم الإدارة إلى جهاز العميل: 113 ميغا بايت
- إجمالي حركة البيانات (جهاز عميل فردي): 114 ميغا بايت

قد تختلف البيانات الموجودة قليلاً اعتمادًا على إصدار قاعدة بيانات مكافحة الفيروسات الحالي.

مزمنة عميل مع خادم الإدارة

يوضح هذا السيناريو حالة نظام الإدارة عند وقوع مزمنة مكثفة للبيانات بين الجهاز العميل وخادم الإدارة. تقوم أجهزة الكمبيوتر العملية 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 آخر اتصال للجهاز العميل، ويقوم بمزمنة 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 اعتماداً 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
المزمنة الأولية قبل تحديث قواعد البيانات على جهاز عميل	699,44	568,42	1267,86
المزمنة الأولية بعد تحديث قواعد البيانات على جهاز عميل	735,8	4474,88	5210,68
مزمنة مع عدم وجود تغييرات في الجهاز العميل وخادم الإدارة	11,99	6,73	18,72
المزمنة بعد تغيير قيمة إعداد في سياسة مجموعة	9,79	11,39	21,18
المزمنة بعد تغيير قيمة إعداد في مهمة جماعية	11,27	11,72	22,99
مزمنة إجبارية مع عدم وجود تغييرات في الجهاز العميل	77,59	99,45	177,04

يختلف حجم حركة المرور الكلي بشكل كبير اعتماداً على ما إذا كان قد تم استخدام البث المتعدد لـ IP ضمن مجموعات الإدارة. إذا تم استخدام IP متعدد الإرسال، فسيزيد حجم حركة المرور الكلي تقريباً بنسبة N مرات للمجموعة، حيث أن N ترمز إلى العدد الكلي للأجهزة المضمنة في مجموعة الإدارة.

يتم تحديد حجم حركة المرور في المزمنة الأولية قبل وبعد تحديث العناوين للحالات التالية:

- تثبيت عميل الشبكة وتطبيق الأمان على جهاز عميل

- نقل جهاز عميل إلى مجموعة إدارة

- تطبيق السياسة والمهام 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 ميغا بايت

- إجمالي حركة البيانات (جهاز عميل فردي): 114 ميغا بايت

قد تختلف البيانات الموجودة في الجدول قليلاً اعتماداً على إصدار قاعدة بيانات مكافحة الفيروسات الحالي.

يختلف حجم حركة المرور بشكل كبير اعتماداً على ما إذا كان قد تم استخدام IP متعدد الإرسال ضمن مجموعات الإدارة أم لا. إذا تم استخدام IP متعدد الإرسال، فسيزيد حجم حركة المرور الكلي تقريباً 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 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 اعتماداً 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 تغييرات في البيانات بواسطة الأجهزة العميلة أو بواسطة خادم الإدارة (انظر الجدول أدناه).

توضح البيانات في الجدول حالة الشبكة بعد التنصيب 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

القيمة	تدفق حركة المرور
3235.84	حركة المرور من الجهاز العميل إلى خادم الإدارة، بالكيلو بايت
64,378.88	حركة المرور من خادم الإدارة إلى الكمبيوتر العميل، بالكيلو بايت
67,614.72	إجمالي حركة المرور (جهاز عميل فردي)، بالكيلو بايت

التحضير لإدارة الجهاز المحمول

هذا القسم يوفر المعلومات التالية:

- حول خادم الأجهزة المحمولة Exchange المخصص لإدارة الأجهزة المحمولة عبر بروتوكول Exchange ActiveSync
- 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 المثبت عليها Kaspersky Endpoint Security for Android

خادم الأجهزة المحمولة Exchange

يسمح لك خادم الأجهزة المحمولة Exchange بإدارة الأجهزة المحمولة المتصلة بخادم إدارة باستخدام بروتوكول Exchange ActiveSync (أجهزة EAS).

كيفية نشر خادم الأجهزة المحمولة Exchange

إذا تم نشر خوادم Microsoft Exchange ضمن مصفوفة خادم وصول العميل في المؤسسة، فيجب تثبيت خادم أجهزة محمولة Exchange على كل خادم من الخوادم الموجودة في تلك المصفوفة. يجب تمكين خيار وضع المجموعة في معالج تثبيت خادم الأجهزة المحمولة Exchange. في هذه الحالة، تُسمى مجموعة المثيلات الخاصة بخادم الأجهزة المحمولة Exchange المثبتة على الخوادم المصفوفة باسم مجموعة خوادم الأجهزة المحمولة Exchange.

في حالة عدم نشر مصفوفة خادم وصول العميل الخاصة بخوادم Microsoft Exchange في المؤسسة، يجب تثبيت خادم أجهزة محمولة Exchange على خادم Microsoft Exchange الذي يمتلك وصول العميل. في هذه الحالة، يجب تمكين خيار **الوضع القياسي** في معالج إعداد خادم الأجهزة المحمولة Exchange.

بالإضافة إلى خادم الأجهزة المحمولة Exchange، يجب تثبيت عميل الشبكة على الجهاز؛ حيث يساعد هذا على تكامل خادم الأجهزة المحمولة Exchange مع Kaspersky Security Center.

نطاق الفحص الافتراضي لخادم الأجهزة المحمولة Exchange هو مجال Active Directory الحالي الذي تم تثبيته فيه. يتيح لك نشر خادم أجهزة محمولة Exchange على خادم مع خادم Microsoft Exchange المثبت (الإصداران 2010 و2013)، توسيع نطاق الفحص ليشمل المجال الرئيسي بأكمله الموجود في خادم الأجهزة المحمولة Exchange (انظر قسم "**تكوين نطاق الفحص**"). تشمل المعلومات المطلوبة أثناء الفحص حسابات مستخدمي خادم Microsoft Exchange، وسياسات Exchange ActiveSync وأجهزة المستخدم المحمولة المتصلة بخادم Microsoft Exchange عبر بروتوكول Exchange ActiveSync.

يتعذر تثبيت مثيلات متعددة لخادم الأجهزة المحمولة Exchange ضمن مجال واحد إذا كانت تعمل في **الوضع القياسي** وتتم إدارتها بواسطة خادم إدارة واحد.

ضمن مجال رئيسي واحد لـ Active Directory واحدة، يتعذر أيضًا تثبيت مثيلات متعددة من خادم الأجهزة المحمولة Exchange (أو مجموعات متعددة من خوادم الأجهزة المحمولة Exchange) – إذا كانت تعمل في **الوضع القياسي** باستخدام نطاق فحص موسّع يشمل المجال الرئيسي بأكمله وإذا كانت متصلة بخادم إدارة واحد.

الحقوق المطلوبة لنشر خادم الأجهزة المحمولة Exchange

يتطلب نشر خادم الأجهزة المحمولة Exchange على خادم Microsoft Exchange (2010، 2013) حقوق مسؤول المجال ودور إدارة المؤسسة. يتطلب نشر خادم الأجهزة المحمولة Exchange على خادم Microsoft Exchange (2007) حقوق مسؤول المجال وعضوية في مجموعة الأمان للمسؤولين عن إدارة Exchange.

حساب لخدمة Exchange ActiveSync

عند تثبيت خادم الأجهزة المحمولة Exchange، يتم إنشاء حساب تلقائيًا في Active Directory:

- في خادم Microsoft Exchange Server (2010، 2013): حساب *****KLMDM4ExchAdmin باستخدام الدور KLMDM Role Group.
- على خادم Microsoft Exchange (2007): حساب *****KLMDM4ExchAdmin والذي يُعد عضو في مجموعة الأمان KLMDM Secure Group.

تعمل خدمة خادم الأجهزة المحمولة Exchange من خلال هذا الحساب.

إذا كنت تريد إلغاء الإنشاء التلقائي للحساب، فعليك إنشاء حساب مخصص باستخدام الحقوق التالية:

- عند استخدام خادم Microsoft Exchange (2010، 2013)، يجب تعيين دور للحساب مسموح له بتنفيذ أوامر cmdlets التالية:

• Get-CASMailbox

• Set-CASMailbox

• Remove-ActiveSyncDevice

• Clear-ActiveSyncDevice

• Get-ActiveSyncDeviceStatistics

• Get-AcceptedDomain

• Set-AdServerSettings

Get-ActiveSyncMailboxPolicy •

New-ActiveSyncMailboxPolicy •

Set-ActiveSyncMailboxPolicy •

Remove-ActiveSyncMailboxPolicy •

- عند استخدام خادم Microsoft Exchange (2007)، يجب منح الحساب حقوق الوصول إلى كائنات Active Directory (راجع الجدول الموجود أدناه).

حقوق الوصول إلى كائنات Active Directory

Cmdlet	الكائن	الوصول
Add-ADPermission -User <User or group name> -Identity "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" -InheritanceType All -AccessRight GenericAll	Thread "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	كاملاً
Add-ADPermission -User <User or group name> -Identity "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>" -InheritanceType All -AccessRight GenericRead	Thread "CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	قراءة
Add-ADPermission -User <User or group name> -Identity "DC=<Domain name>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink,msExchOmaAdminWirelessEnable	Properties msExchMobileMailboxPolicyLink and msExchOmaAdminWirelessEnable for objects in Active Directory	قراءة\كتابة
-MailboxDatabase Add-ADPermission -<User or group name> -ExtendedRights ms-Exch-Store-Admin	مستودعات صندوق البريد الخاص بخادم Exchange، thread "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Organization name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Domain name>"	حق موسّع ms-Exch-Store-Active

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 قياسييين لخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

التكوين القياسي: Kaspersky Device Management for iOS في DMZ

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. يجب تمكين المنفذ 443 (المنفذ الافتراضي) للوصول الخارجي، على سبيل المثال، عن طريق نشر خدمة ويب iOS MDM على Microsoft Forefront® Threat Management Gateway (المشار إليها فيما بعد بـ [TMG](#)).

يتطلب أي تكوين قياسي وصولاً إلى خدمات Apple على الويب الخاصة بخادم iOS MDM (النطاق 17.0.0.0/8) عبر منفذ 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 المثبت عليها Kaspersky Endpoint Security for Android™ (يُشار إليها فيما بعد باسم أجهزة KES) بواسطة خادم الإدارة. يدعم Kaspersky Security Center 10 Service Pack 1، بالإضافة إلى الإصدارات الأحدث، المزايا 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 العملية التي يمكن مزامتها مع خادم الإدارة خلال فواصل زمنية محددة. يمكنك استخدام هذه المعلومات لتحديد المخطط الأمثل لنشر الحماية ضد 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، 478 جيجابايت
نظام التشغيل	Microsoft Windows Server 2019 القياسي، إصدار 10.0.17763 وإصدار 17763
الشبكة	QLogic BCM5709C جيجابايت إيثرنت (عمل NDIS VBD)

تكوين جهاز لجهاز خادم SQL Server.

المعلمة	القيمة
وحدة المعالجة المركزية	Intel Xeon وحدة المعالجة المركزية X5570، سرعة الساعة 2.93 جيجاهرتز، مقبسين، 8 مراكز معالجة، 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 جيجابايت

يدعم خادم الإدارة إنشاء 500 خادم إدارة افتراضي.

كان الفاصل الزمني للمزامنة هو 15 دقيقة لكل 10000 جهاز مُدار (انظر الجدول أدناه).

ملخص نتائج اختبار تحميل خادم الإدارة

عدد الأجهزة المدارة	الفاصل الزمني للمزامنة (بالدقائق)
10,000	15
20,000	30
30,000	45
40,000	60%
50,000	75
60,000	90
70,000	105
80,000	120
90,000	135
100,000	150

إذا قمت بتوصيل خادم الإدارة بخادم قاعدة بيانات MySQL أو SQL Express أو MariaDB، فلا يُوصى باستخدام التطبيق لإدارة أكثر من 10000 جهاز. بالنسبة لنظام إدارة قاعدة بيانات MariaDB، فإن الحد الأقصى الموصى به من الأجهزة المدارة هو 20000 جهاز.

نتائج اختبار أداء خادم وكيل KSN

إذا كانت شبكة المؤسسة الخاصة بك تتضمن عددًا كبيرًا من الأجهزة العملية وتستخدم خادم الإدارة كخادم وكيل KSN، فيجب أن تفي أجهزة خادم الإدارة بمتطلبات معينة لتتمكن من معالجة الطلبات من الأجهزة العملية. 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%

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.

وفي Microsoft Windows XP، قد لا يقوم عميل الشبكة بالعمليات التالية بشكل صحيح: تنزيل التحديثات مباشرة من خوادم Kaspersky (كنقطة توزيع) والعمل كوكيل 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 عميل الشبكة المثبت 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.
- عن طريق استنساخ صورة لمحرك القرص الثابت الخاص بالمسؤول والمثبت عليه نظام التشغيل و عميل الشبكة: استخدام الأدوات المقدمة من Kaspersky Security Center للتعامل مع صور القرص، أو استخدام أدوات الجهة الخارجية.
- باستخدام سياسات مجموعة Windows: باستخدام أدوات الإدارة القياسية من Windows لسياسات المجموعة، أو في الوضع التلقائي، عبر الخيار المخصص المقابل في مهمة التثبيت عن بُعد لـ Kaspersky Security Center.
- 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 مثبتات التطبيق على الأجهزة.

على النظم الأساسية غير Microsoft Windows، يجب إجراء التثبيت الأولي لعمل الشبكة على الأجهزة المدارة عبر أدوات جهة خارجية متوفرة. 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 أجهزة في شبكة المؤسسة ليست أعضاء 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 الشبكات الفرعية هذه.

• 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؛ 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 بالمتبث.

طريقة تحديد الإعدادات هذه غير مناسبة لعملية التثبيت غير التفاعلية ("الصامتة") للتطبيقات على مجموعات من الأجهزة. بشكل عام، يجب على المسؤول تحديد قيم للإعدادات في الوضع المركزي؛ ويمكن استخدام هذه القيم لاحقًا للتثبيت غير التفاعلي 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 التنفيذية الخاصة بالمتبث 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 متداخلة. 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 مثبت 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 كل 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 العملية 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 القرص الثابت لجهاز ما ونسخها

إذا أردت تثبيت عميل الشبكة على أجهزة يجب تثبيت نظام تشغيل وبرنامج آخر عليها (أو إعادة تثبيتها)، يمكنك استخدام آلية التقاط القرص الثابت الخاص بهذا الجهاز ونسخه.

لإجراء النشر عن طريق التقاط قرص صلب ونسخه:

1. أنشئ جهاز مرجعي مثبت 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 مثبت 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.
- تأكد من أن الأداة المساعدة klmover ستعمل باستخدام مفتاح dupfix- (طلب إلزامي) 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.

إذا تم نسخ صورة محرك الأقراص الثابتة بشكل غير صحيح، فيمكنك حل هذه المشكلة.

يمكنك استخدام سيناريو بديل لنشر عميل الشبكة على أجهزة جديدة من خلال صور نظام التشغيل:

• لا تحتوي الصورة الملتقطة على عميل شبكة مثبت.

• تمت إضافة حزمة تثبيت مستقلة لعميل الشبكة الموجود في المجلد المشترك الخاص بـ Kaspersky Security Center إلى قائمة الملفات التنفيذية التي تعمل عند اكتمال نشر الصورة على الأجهزة المستهدفة.

يضيف سيناريو النشر هذا ميزة المرونة: يمكنك استخدام صورة نظام تشغيل واحدة مع العديد من خيارات تثبيت عميل الشبكة و / أو تطبيق الأمان، بما في ذلك قواعد نقل الجهاز المرتبطة بالحزمة المستقلة. يؤدي ذلك إلى تعقيد عملية النشر قليلاً: يجب عليك توفير وصول إلى مجلد الشبكة الذي يحتوي على حزم تثبيت مستقلة من جهاز.

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 مثبت Microsoft (حزمة MSI) في مجلد مشترك (هو المجلد الذي تحتوي فيه حسابات LocalSystem الخاصة بالأجهزة الهدف على أدونات 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 مثبت 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 أدونات كتابة في سياسات مجموعة Active Directory.

إذا أردت تثبيت عميل الشبكة وتطبيق آخر خلال المهمة ذاتها، فسيُسبب 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 الإمكانيات، 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 مخصصة](#) عالية 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 إضافة معالج المهمة 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 مباشرة.

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

إذا أردت بدء نشر عملاء شبكة أو تطبيقات أخرى فوراً، بدون انتظار المرة التالية لدخول الأجهزة الهدف في المجال، أو في حالة توفر أي أجهزة عميلة ليست أعضاء في مجال Active Directory، فيمكنك فرض تثبيت حزم التثبيت المحددة عبر مهمة التثبيت عن بُعد الخاصة بـ Kaspersky Security Center.

في هذه الحال، يمكنك تحديد أجهزة هدف 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. إذا كان إعداد تشغيل المهام الفأنتة ممكناً في خصائص المهمة، فيمكن تشغيل المهمة إما فوراً أو بعد تشغيل الأجهزة الهدف أو عند نقلها إلى مجموعة الإدارة الهدف.

يتكون هذا النوع من التثبيت من نسخ الملفات إلى المصدر الإداري (\$admin) على كل جهاز والقيام بتسجيل عن بُعد للأجهزة الداعمة عليها. يجب الوفاء بالشروط التالية في هذه الحالة:

- يجب أن تكون الأجهزة متاحة للاتصال إما من جهة خادم الإدارة أو من جهة نقطة التوزيع.
- يجب أن يعمل تحليل الاسم للأجهزة الهدف بشكل صحيح في الشبكة.
- يجب أن تظل المشاركات الإدارية (\$admin) ممكنة على الأجهزة الهدف.
- يجب أن تكون خدمة نظام الخادم قيد التشغيل على الأجهزة الهدف (تكون قيد التشغيل بشكل افتراضي).
- يجب أن تكون المنافذ التالية مفتوحة على الأجهزة الهدف للسماح بالوصول عبر أدوات Windows: TCP 139، TCP 445، UDP 137، UDP 138.

- يجب تعطيل وضع "مشاركة الملف البسيطة" على الأجهزة الهدف.
- على الأجهزة الهدف، يجب تعيين مشاركة الوصول ونموذج الأمان على النحو التقليدي - مصادقة المستخدمين المحليين على أنهم أنفسهم، ولا يمكن أن يكون بأي حال "ضعيف" فقط - مصادقة المستخدمين المحليين على أنهم "ضعيف".
- يجب أن تكون الأجهزة الهدف أعضاء في المجال، أو يجب إنشاء حسابات موحدة باستخدام حقوق المسؤول على الأجهزة الهدف مقدماً.

يمكن تعديل الأجهزة الموجودة في مجموعات العمل وفقاً للمتطلبات الموجودة أعلاه باستخدام الأداة المساعدة riprep.exe الموضحة [على الموقع الإلكتروني للدعم الفني في Kaspersky](#).

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.

يُعتبر التثبيت التلقائي طريقة مبسطة لإنشاء مهام للتثبيت الإجمالي للتطبيقات. للقيام بذلك، افتح خصائص مجموعة الإدارة، وافتح قائمة حزم التثبيت وحدد الحزم التي يجب تثبيتها على الأجهزة الموجودة في هذه المجموعة. وكنتيجه لذلك، سيتم تثبيت حزم التثبيت المحددة تلقائياً 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.

يمكن تطبيق التثبيت الإجمالي أيضاً 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 DMZ. لجعل التثبيت الإجمالي ممكناً، يجب عليك توفير نقاط توزيع لكل شبكة من الشبكات المعزولة.

قد يكون استخدام نقاط التوزيع كمراكز تثبيت محلية مفيداً عند القيام بالتثبيت على أجهزة في الشبكات الفرعية التي تتصل بخادم الإدارة عبر قناة منخفضة السرعة في حين تتاح قناة أوسع بين الأجهزة في نفس الشبكة الفرعية. ولكن، لاحظ أن طريقة التثبيت هذه تضع حملاً كبيراً على الأجهزة التي تعمل كنقاط توزيع. لذا، من المستحسن أن تحدد أجهزة قوية ذات وحدات تخزين عالية الأداء لتعمل كنقاط توزيع. علاوة على ذلك، يجب أن تتجاوز مساحة القرص الخالية في القسم الذي يحتوي على المجلد %Application Data\KasperskyLab\adminikit%\ALLUSERSPROFILE%، بعدة مرات، الحجم الإجمالي لـ [حزم توزيع التطبيقات المثبتة](#).

تشغيل الحزم المستقلة التي أنشأها Kaspersky Security Center

لا يمكن تطبيق الطرق الموضحة أعلاه للنشر الأولي لعميل الشبكة والتطبيقات الأخرى دائماً 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، مطالباً 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 لاحقاً.

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 مخزنة في المجلد المشترك الخاص بـ Kaspersky Security Center، سيتم نسخ الحزمة أولاً إلى مجلد محلي مؤقت، ثم سيتم تشغيل مثبت 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 ترفيحتها 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 قبل 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\admindit\1093\working\FTServer% كبيرة متعددة من أنواع مختلفة وتضمن 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\admindit\1103\FTCITmp.

لا يمكن حذف الملفات من المجلد \$FTCITmp 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 محسن 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 أي 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 حال استخدام مهمة التثبيت عن بُعد من Kaspersky Security Center، في إضافة معالج المهمة أو في نافذة خصائص المهمة التي تم إنشاؤها (قسم [إعادة تشغيل نظام التشغيل](#))، يمكنك تحديد الإجراء الذي سيتم اتخاذه عندما تكون إعادة التشغيل مطلوبة:

- **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 تنذير 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 ملاءمة لمحطات العمل حيث يحتاج المستخدمون لإمكانية تحديد الوقت الأكثر ملاءمة 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 لتثبيت 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 المخزن 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 (MSI) Microsoft Windows Installer، 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.

لجعل المهمة لا تنتظر اكتمال العملية قيد التشغيل، قم بتعيين قيم إعداد الانتظار إلى 0 في القسم [SetupProcessResult]:

مثال:
[SetupProcessResult]
Wait=0

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:

مثال:
[SetupProcessResult]
WaitJob=0

لجعل المهمة تكتمل بنجاح أو إرجاع خطأ بناءً على رمز الإرجاع الخاص بالعملية قيد التشغيل، قم بإدراج رموز الإرجاع الناجحة في القسم [SetupProcessResult_SuccessCodes]، على سبيل المثال:

مثال:
[SetupProcessResult_SuccessCodes]
=0
=3010

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:

مثال:
[SetupProcessResult_SuccessCodes]
=0 اكتمل التثبيت بنجاح
=3010 إعادة التشغيل مطلوبة لإكمال التثبيت
[SetupProcessResult_ErrorCodes]
=1602 تم إلغاء التثبيت بواسطة المستخدم
=1603 خطأ فادح أثناء التثبيت

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]:

مثال:
[SetupProcessResult_NeedReboot]
=3010

مراقبة النشر

لمراقبة نشر Kaspersky Security Center وللتأكد من أن تطبيق الأمان و عميل 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 المثبت 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 المدارة 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 و عميل الشبكة في الوضع الصامت.

أدوات تثبيت مكونات Kaspersky Security Center 14 (خادم الإدارة، و عميل الشبكة، ووحدة تحكم الإدارة) مضمنة في تقنية مثبتت Windows Installer. حزمة MSI هي أساس أداة التثبيت. يتيح تنسيق الحزمة استخدام كل الميزات التي يقدمها Windows Installer: وهي قابلية التوسع وتوفير 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 و عميل 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
```

الملف ss_install.xml هو مثيل للتنسيق الداخلي لمعلومات مثبتت Kaspersky Security Center. تحتوي حزمة التوزيع على الملف ss_install.xml مع المعلومات الافتراضية.

الرجاء عدم تعديل الملف ss_install.xml يدويًا. يمكن تعديل هذا الملف عبر أدوات Kaspersky Security Center عند تحرير معلمات حزم التثبيت في وحدة تحكم الإدارة.

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. لتجنب التعارض بين المعلمات المحددة عبر خصائص MSI والمعلومات المحددة في ملف الاستجابة، يمكنك تعطيل ملف الاستجابة عن طريق تعيين الخاصية DONT_USE_ANSWER_FILE=1. مثال على تشغيل مثبتت عميل الشبكة باستخدام حزمة msi يتم كما يلي.

يتطلب تثبيت عميل الشبكة في الوضع غير التفاعلي قبول بنود اتفاقية ترخيص المستخدم النهائي. استخدم معلمة EULA=1، إذا قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها.

مثال:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1  
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

يمكنك أيضًا تحديد معلمات التثبيت الخاصة بحزمة msi عن طريق إعداد ملف الاستجابة مقدمًا (الملف ذي الامتداد .mst). يظهر هذا الأمر كما يلي:

مثال:

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

يمكنك تحديد ملفات استجابة متعددة في أمر واحد.

تكوين التثبيت الجزئي عبر setup.exe

عند تشغيل تثبيت التطبيقات عبر setup.exe، يمكنك إضافة القيم الخاصة بأي خصائص MSI إلى حزمة MSI.

مثال:

"v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2/

معلومات تثبيت خادم الإدارة

يوضح الجدول الموجود أدناه خصائص MSI التي يمكنك تكوينها عند تثبيت خادم الإدارة. جميع المعلومات اختيارية، ماعدا الخاصة باتفاقية ترخيص المستخدم النهائي (EULA) و PRIVACYPOLICY (سياسة الخصوصية).

معلومات تثبيت خادم الإدارة في الوضع غير التفاعلي

القيم المتوفرة	الوصف	خاصية MSI
<ul style="list-style-type: none"> 1- لقد قرأت شروط <u>اتفاقية ترخيص المستخدم النهائي</u> بشكل كامل واستوعبتها وقبلتها. قيمة أخرى أو بلا قيمة- لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت). 	قبول بنود الترخيص (مطلوب)	EULA
<ul style="list-style-type: none"> 1- أنني أدرك وأوافق على التعامل مع بياناتي ونقلها (بما في ذلك، نقلها إلى البلدان الثالثة) كما هو موضح في <u>سياسة الخصوصية</u>. أؤكد على أنني قد قرأت سياسة الخصوصية وفهمتها بالكامل. قيمة أخرى أو بلا قيمة- لا أوافق على بنود سياسة الخصوصية (لا يتم إجراء التثبيت). 	الموافقة على شروط سياسة الخصوصية (مطلوب)	PRIVACYPOLICY
<ul style="list-style-type: none"> قياسي. مخصص. 	نوع تثبيت خادم الإدارة	INSTALLATIONMODETYPE
قيمة السلسلة.	مجلد تثبيت التطبيق	INSTALLDIR
<p>CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86</p> <p>قائمة الحد الأدنى من المكونات الكافية للتثبيت الصحيح لخادم الإدارة:</p> <p>ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86</p>	قائمة بالمكونات التي سيتم تثبيتها (مفصولة بفاصلة)	ADDLOCAL
<ul style="list-style-type: none"> NRT_1_100- من 1 إلى 100 جهاز. NRT_100_1000- من 101 إلى 1000 جهاز. NRT_GREATER_1000- أكثر من 1000 جهاز. 	حجم الشبكة	NETRANGETYPE
<ul style="list-style-type: none"> SrvAccountDefault- سيتم إنشاء حساب المستخدم تلقائيًا. SrvAccountUser- يتم تحديد حساب المستخدم يدويًا. 	طريقة تحديد المستخدم لتشغيل خدمة خادم الإدارة	SRV_ACCOUNT_TYPE

قيمة السلسلة.	اسم المستخدم للخدمة	SERVERACCOUNTNAME
قيمة السلسلة.	كلمة مرور المستخدم للخدمة	SERVERACCOUNTPWD
<ul style="list-style-type: none"> سيتم استخدام خادم قاعدة بيانات MySQL—A MySQL أو MariaDB. سيتم استخدام خادم قاعدة بيانات MSSQL – Microsoft SQL Server Express ((SQL Server Express. 	نوع قاعدة البيانات	DBTYPE
قيمة السلسلة.	الاسم الكامل لخادم قاعدة بيانات MySQL أو MariaDB	MYSQLSERVERNAME
قيمة رقمية.	رقم منفذ الاتصال بخادم قاعدة بيانات MySQL أو MariaDB	MYSQLSERVERPORT
قيمة السلسلة.	اسم خادم قاعدة البيانات MySQL أو MariaDB	MYSQLDBNAME
قيمة السلسلة.	اسم المستخدم للاتصال بخادم قاعدة البيانات MySQL أو MariaDB	MYSQLACCOUNTNAME
قيمة السلسلة.	كلمة مرور المستخدم للاتصال بخادم قاعدة البيانات MySQL أو MariaDB	MYSQLACCOUNTPWD
<ul style="list-style-type: none"> InstallMSSEE – التثبيت من حزمة. ChooseExisting – استخدام الخادم المثبت. 	نوع استخدام قاعدة بيانات MSSQL	MSSQLCONNECTIONTYPE
قيمة السلسلة.	الاسم الكامل لمثيل خادم SQL Server	MSSQLSERVERNAME
قيمة السلسلة.	اسم قاعدة بيانات خادم SQL Server	MSSQLDBNAME
<ul style="list-style-type: none"> Windows. SQLServer. 	طريقة مصادقة الاتصال بخادم SQL Server	MSSQLAUTHTYPE
قيمة السلسلة.	اسم المستخدم للاتصال بخادم SQL Server في وضع SQLServer	MSSQLACCOUNTNAME
قيمة السلسلة.	كلمة مرور المستخدم للاتصال بخادم SQL Server في وضع SQLServer	MSSQLACCOUNTPWD
<ul style="list-style-type: none"> إنشاء—إنشاء مجلد مشترك جديد؛ في هذه الحالة، يجب تحديد الخصائص التالية: SHARELOCALPATH – المسار إلى مجلد محلي. SHAREFOLDERNAME – اسم الشبكة لمجلد ما 	طريقة تحديد مجلد مشترك	CREATE_SHARE_TYPE

• Null – يجب تحديد خاصية EXISTSHAREFOLDERNAME		
قيمة السلسلة.	المسار الكامل لمجلد مشترك موجود	EXISTSHAREFOLDERNAME
قيمة رقمية.	رقم المنفذ الخاص بالاتصال بخادم الإدارة	SERVERPORT
قيمة رقمية.	رقم منفذ إنشاء اتصال SSL بخادم الإدارة	SERVERSSLPORT
قيمة السلسلة.	عنوان خادم الإدارة	SERVERADDRESS
<ul style="list-style-type: none"> • 1 – حجم المفتاح لشهادة خادم الإدارة هو 2,048 بت. • 0 – حجم المفتاح لشهادة خادم الإدارة هو 1,024 بت. • إذا لم يتم تحديد قيمة، يكون حجم المفتاح لشهادة خادم الإدارة هو 1,024 بت. 	حجم المفتاح لشهادة خادم الإدارة (بوحدة البت)	SERVERCERT2048BITS
قيمة السلسلة.	عنوان خادم الإدارة للاتصال بالأجهزة المحمولة، يتم تجاهله إن لم يتم تحديد مكوّن MobileSupport	MOBILESERVERADDRESS

معلومات تثبيت عميل الشبكة

يوضح الجدول الموجود أدناه خصائص MSI التي يمكنك تكوينها عند تثبيت عميل الشبكة. وجميع المعلومات اختيارية باستثناء اتفاقية ترخيص المستخدم النهائي (EULA) وSERVERADDRESS.

معلومات تثبيت عميل الشبكة في الوضع غير التفاعلي

القيم المتوفرة	الوصف	خاصية MSI
<ul style="list-style-type: none"> • 1 – لقد قرأت شروط <u>اتفاقية ترخيص المستخدم النهائي</u> بشكل كامل واستوعبتها وقبلتها. • 0 – لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت). • بلا قيمة – لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت). 	الموافقة على شروط اتفاقية الترخيص	EULA
<ul style="list-style-type: none"> • 1 – عدم الاستخدام. • قيمة أخرى أو دون قيمة – عدم القراءة. 	إعدادات تثبيت القراءة لملف الاستجابة	DONT_USE_ANSWER_FILE
قيمة السلسلة.	مسار لمجلد تثبيت عميل الشبكة	INSTALLDIR
قيمة السلسلة.	عنوان خادم الإدارة (مطلوب)	SERVERADDRESS
قيمة رقمية.	رقم منفذ الاتصال بخادم الإدارة	SERVERPORT
قيمة رقمية.	عدد المنافذ لاتصال مشفر لخادم الإدارة باستخدام بروتوكول SSL	SERVERSSLPORT

USESSL	سواء يتم استخدام اتصال SSL أم لا	<ul style="list-style-type: none"> • 1 – الاستخدام • قيمة أخرى أو دون قيمة – عدم الاستخدام.
OPENUDPPOINT	سواء يتم فتح منفذ UDP أم لا	<ul style="list-style-type: none"> • 1 – فتح. • قيمة أخرى أو دون قيمة – عدم الفتح.
UDPPOINT	رقم منفذ UDP	قيمة رقمية.
USEPROXY	سواء يتم استخدام خادم وكيل أم لا	<ul style="list-style-type: none"> • 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 للحساب للاتصال بالخادم الوكيل (لا تحدد أي تفاصيل عن الحسابات المميزة في معلمات حزم التثبيت).	قيمة السلسلة.
GATEWAYMODE	وضع استخدام عبارة الاتصال	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • GetOnFirstConnection – تلقي شهادة من خادم الإدارة. • GetExistent – تحديد شهادة موجودة إذا كان هذا الخيار محددًا، فيجب تحديد الخاصية .CERTFILE.
CERTFILE	مسار إلى ملف الشهادة	قيمة السلسلة.
VMVDI	تمكين الوضع الديناميكي للبنية الأساسية لسطح المكتب الافتراضي (VDI).	<ul style="list-style-type: none"> • 1 – التمكين. • 0 – عدم التمكين. • بلا قيمة – لا تمكّن.
LAUNCHPROGRAM	سواء بدء خدمة عميل الشبكة بعد اكتمال التثبيت أم لا	<ul style="list-style-type: none"> • 1 – البدء. • قيمة أخرى أو دون قيمة – عدم البدء.

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 تشبيهاً 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 تشبيهاً تفاعلياً 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 (Windows فقط). إذا تم نشر بنية أساسية ظاهرية على شبكة المؤسسة، فيمكن استخدام أجهزة ظاهرية ديناميكية (موقتة) 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، سيتم إزالة هذا الجهاز الظاهري من البنية الأساسية. إذا تم نشر Kaspersky Security Center على شبكة مؤسسة، فستتم إضافة جهاز ظاهري مثبت 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](#))

• بالنسبة 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 لمدة تخزين الأحداث (بالأيام).

دعم نسخ الأجهزة الظاهرية

عملية نسخ جهاز ظاهري باستخدام عميل شبكة مثبت أو إنشاء واحد من قالب باستخدام عميل شبكة مثبت 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®: يكتشف عميل الشبكة عملية نسخ للجهاز الظاهري عن طريق معرفات 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 المثبت عليها عميل الشبكة إلى حالته السابقة

يُعتبر Kaspersky Security Center تطبيقًا مؤرّغًا. ستؤدي عودة نظام الملفات إلى الحالة السابقة على جهاز مثبت 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 المثبت عليها عميل شبكة على المجلد %Application%\ALLUSERSPROFILE 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 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 14.

على قدر الإمكان، تجنب إعادة مجلد %Application Data\KasperskyLab\admindkit% \ALLUSERSPROFILE% إلى حالته السابقة على جهاز مثبت 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 مثبت 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. يتم فتح نافذة تطلبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها.
2. في نافذة تحديد التطبيق، انقر فوق الرابط **تثبيت عميل شبكة Kaspersky Security Center 14 فقط** لبدء تشغيل معالج إعداد عميل الشبكة. اتبع إرشادات المعالج. أثناء تشغيل معالج التثبيت، يمكنك تحديد الإعدادات المتقدمة لعميل الشبكة (انظر أدناه).
3. إذا كنت ترغب باستخدام جهازك كبوابة الاتصال لمجموعة إدارة محددة، ففي النافذة **بوابة الاتصال الخاصة بمعالج الإعداد**، حدد استخدام **عميل الشبكة كبوابة اتصال في DMZ**.
4. لتكوين عميل الشبكة أثناء التثبيت على جهاز ظاهري:

a. إذا كنت تخطط لإنشاء أجهزة ظاهرية ديناميكية من صورة جهاز ظاهري، قم بتمكين الوضع الديناميكي لعميل الشبكة للبنية الأساسية لسطح المكتب الافتراضي (VDI). للقيام بذلك، في النافذة **إعدادات المتقدمة لمعالج الإعداد**، حدد خيار **تمكين الوضع الديناميكي لـ VDI**. تجاوز هذه الخطوة إذا كنت تخطط لإنشاء أجهزة ظاهرية ديناميكية من صورة الأجهزة الظاهرية. لا يتوافق استخدام الوضع الديناميكي لـ VDI إلا للأجهزة التي تعمل بنظام Windows.

b. تحسين تشغيل عميل شبكة VDI. للقيام بذلك، في نافذة الإعدادات المتقدمة لمعالج الإعداد، حدد خيار تحسين إعدادات عميل شبكة Kaspersky Security Center للبنية التحتية الظاهرية.

سيتم تعطيل فحص الملفات التنفيذية لاكتشاف الثغرات الأمنية عند بدء تشغيل الجهاز. وسيؤدي ذلك أيضًا إلى تعطيل إرسال المعلومات حول الكائنات التالية إلى خادم الإدارة:

• سجل الأجهزة

• تم تثبيت التطبيق على الجهاز.

• تحديثات Microsoft Windows التي يجب تثبيتها على الجهاز العميل المحلي

• ثغرات البرامج الأمنية التي تم اكتشافها على الجهاز العميل المحلي

علاوة على ذلك، فسوف تتمكن من تمكين إرسال هذه المعلومات في خصائص عميل الشبكة أو في إعدادات سياسة عميل الشبكة.

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 غير التفاعلي (الصامت)

يمكن تثبيت عميل الشبكة في الوضع غير التفاعلي، أي، دون إدخال تفاعلي لمعلومات التثبيت. يستخدم التثبيت غير التفاعلي حزمة (MSI) (Windows Installer) لعميل الشبكة. يقع ملف MSI في حزمة توزيع Kaspersky Security Center، في المجلد Packages\NetAgent\exec.

لتثبيت عميل الشبكة على جهاز محلي في وضع غير تفاعلي:

1. [اقرأ 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 هو قائمة معلمات وقيمها الخاصة المفصولة بمسافة (PROP1=PROP1VAL PROP2=PROP2VAL).

وفي قائمة المعلمات، يجب عليك تضمين اتفاقية EULA=1. وإلا، فلن يتم تثبيت عميل الشبكة.

إذا كنت تستخدم إعدادات الاتصال القياسية لـ Kaspersky Security Center 11 والإصدارات الأحدث، و عميل الشبكة على الأجهزة البعيدة، فقم بتشغيل الأمر:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log  
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

1 * vx/ هو مفتاح سجلات الكتابات. يتم إنشاء السجل أثناء تثبيت عميل الشبكة وحفظه في C:\windows\temp\nag_inst.log.

بالإضافة إلى nag_inst.log، يقوم التطبيق بإنشاء ملف \$ klsinstlib.log الذي يحتوي على سجل التثبيت. يتم تخزين هذا الملف في المجلد %temp%\windir% أو %temp%. لأغراض استكشاف الأخطاء وإصلاحها، قد تحتاج أنت أو أخصائي الدعم الفني في Kaspersky إلى كلا ملفي السجل – nag_inst.log و \$ klsinstlib.log.

وبالإضافة إلى ذلك، إذا كنت بحاجة إلى تحديد منفذ الاتصال بخادم الإدارة، فقم بتشغيل الأمر:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
```

تتوافق معلمة SERVERPORT مع عدد منافذ الاتصال بخادم الإدارة.

يتم إدراج الأسماء والقيم المحتملة للمعلمات التي يمكن استخدامها عند تثبيت عميل الشبكة في الوضع غير التفاعلي في القسم [معلمات تثبيت عميل الشبكة](#).

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 (غير التفاعلي)، 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.

3. [اقرأ اتفاقية ترخيص المستخدم النهائي](#). لا تتبع الخطوات أدناه إلا إذا فهمت شروط اتفاقية ترخيص المستخدم النهائي ووافقت عليها.

4. قم بتعيين قيمة متغير بيئة KLAUTOANSWERS عن طريق إدخال الاسم الكامل لملف الإجابات (بما في ذلك المسار)، على سبيل المثال، كما يلي:

```
export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
```

5. قم بإنشاء ملف الإجابات (بتنسيق TXT) في الدليل الذي حددته في متغير البيئة. أضف إلى ملف الإجابات قائمة من المتغيرات بتنسيق VARIABLE_NAME=variable_value، 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](#) 9

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 (غير التفاعلي) ممكنًا.	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 المُستخدَم لتسجيل الدخول إلى خادم الوكيل.	أي اسم مستخدم موجود.
KLNAGENT_PROXY_PASSWORD	لا	يحدد كلمة مرور المستخدم المُستخدَم 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 لعميل 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.	أي رقم منفذ موجود.

	القيمة الافتراضية هي 15000.		
أي رقم منفذ موجود.	يحدد المنفذ غير TLS الذي يستخدمه عميل الشبكة. القيمة الافتراضية هي 14000.	لا	KLNAGENT_PORT
أي رقم منفذ موجود.	يحدد منفذ TLS الذي يستخدمه عميل الشبكة. القيمة الافتراضية هي 13000.	لا	KLNAGENT_SSLPORT
1 (افتراضي) — يتم استخدام TLS. أخرى — لا يتم استخدام TLS.	يحدد ما إذا كان أمان طبقة النقل (TLS) يستخدم للاتصال.	لا	KLNAGENT_USESSL
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. 4 — يتم استخدام مثيل عميل الشبكة كبوابة اتصال في المنطقة المنزوعة السلاح (DMZ).	يحدد ما إذا كان سيتم استخدام بوابة الاتصال.	لا	KLNAGENT_GW_MODE
اسم DNS أو عنوان IP.	يحدد عنوان بوابة الاتصال. لا تنطبق القيمة إلا إذا كان KLNAGENT_GW_MODE=3.	لا	KLNAGENT_GW_ADDRESS

6. قم بتشغيل البرنامج النصي postinstall.pl بتنفيذ الأمر التالي:

- لنظام تشغيل 32 بت: \$ sudo /opt/kaspersky/klagent/lib/bin/setup/postinstall.pl
- بالنسبة لنظام تشغيل 64 بت: \$ sudo /opt/kaspersky/klagent64/lib/bin/setup/postinstall.pl

يبدأ تثبيت عميل الشبكة لنظام التشغيل Linux في الوضع الصامت؛ ولا تتم مطالبة المستخدم بأي إجراءات أثناء العملية.

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 غير التفاعلي

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 لمحطات عمل Windows و Kaspersky Anti-Virus for Windows Servers و Kaspersky Security Center، افتح المجلد الفرعي **exec** وقم بتشغيل الملف التنفيذي (ملف له الامتداد .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 واستوعبت وقبلت شروط **اتفاقية ترخيص المستخدم النهائي بالكامل** و **سياسة الخصوصية** على التوالي. كما أنك تترك أنه يتم التعامل جميع بياناتك ونقلها (بما في ذلك، نقلها إلى البلدان الثالثة) كما هو موضح في سياسة الخصوصية. نص اتفاقية الترخيص وسياسة الخصوصية مضمن 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.

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 تثبيت مستقلة. 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 مباشرة. 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\.
لم يكن هذا المجلد موجودًا، فسيتم إنشاؤه تلقائيًا.
يتم تحديد هذا الخيار افتراضيًا.

• التثبيت في المجلد المحدد ④

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 ④

إذا تم تمكين هذا الخيار، بالنقر فوق زر **تعديل**، يمكنك إدخال كلمة مرور إزالة التثبيت (متاحة فقط لعميل الشبكة على الأجهزة التي تعمل بأنظمة التشغيل Windows).
يتم تعطيل هذا الخيار افتراضيًا.

• الحالة ④

حالة كلمة المرور: تم تعيين كلمة المرور أو لم يتم تعيين كلمة مرور.
بشكل افتراضي، تكون كلمة المرور غير مثبتة.

• حماية خدمة عميل الشبكة من عمليات الإزالة أو الإنهاء غير المصرح بها، ومنع إجراء تغييرات في الإعدادات ④

بعد تثبيت عميل الشبكة على جهاز مُدار، يتعذر إزالة المكون أو إعادة تكوينه دون الامتيازات المطلوبة. يتعذر إيقاف خدمة عميل الشبكة.
يتم تعطيل هذا الخيار افتراضيًا.

• التثبيت التلقائي للتحديثات القابلة للتطبيق والتصحيحات المكونت التي لها حالة غير محددة ④

إذا تم تمكين هذا الخيار، فسيتم تلقائيًا تثبيت جميع التحديثات والتصحيحات التي تم تنزيلها لخدام الإدارة، و عميل الشبكة، ووحدة التحكم في الإدارة، وخدام الأجهزة المحمولة Exchange، وخدام الأجهزة المحمولة التي تعمل بنظام iOS MDM (لا يتوفر التحديث والتصحيح التلقائيان إلا بدءًا من إصدار Kaspersky Security Center 10 Service Pack 2).
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 وكيل الشبكة بخادم الإدارة:

في هذا القسم يمكنك تكوين اتصال وكيل الشبكة بخادم الإدارة. لإنشاء اتصال، يمكنك استخدام بروتوكول SSL أو UDP. لتكوين الاتصال، حدد الإعدادات التالية:

• خادم الإدارة ④

عنوان الجهاز المثبت عليه خادم الإدارة.

• المنفذ ④

رقم المنفذ المستخدم في الاتصال.

• منفذ SSL ④

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 افتراضياً. نوصي بعدم تعطيل هذا الخيار حتى يظل اتصالاتك آمنة.

• 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 وكيل الشبكة. لذلك، نوصي بعدم تعطيل هذا الخيار. يتم تمكين هذا الخيار افتراضياً.

• رقم منفذ UDP

في هذا الحقل يمكنك تحديد المنفذ المطلوب لاتصال عميل الشبكة بخادم الإدارة باستخدام بروتوكول UDP. منفذ UDP الافتراضي هو 15000.

• فتح منافذ عميل الشبكة في جدار حماية Microsoft Windows

في حال تمكين هذا الخيار، بعد تثبيت عميل الشبكة على الجهاز العميل، تتم إضافة منفذ UDP إلى قائمة استثناءات جدار حماية Microsoft Windows. ويكون منفذ UDP هذا مطلوباً لتشغيل عميل الشبكة بشكل صحيح. يتم تمكين هذا الخيار افتراضياً.

متقدم

في قسم **الإعدادات المتقدمة**، يمكنك تكوين كيفية استخدام بوابة الاتصال. لهذا الغرض، يمكنك إجراء ما يلي:

- استخدم وكيل الشبكة كبوابة اتصال في المنطقة منزوعة السلاح (DMZ) للاتصال بخادم الإدارة والتواصل معه و **الحفاظ على البيانات الموجودة على وكيل 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 افتراضياً.

• تحسين إعدادات البنية الأساسية لسطح المكتب الافتراضي (VDI) 9

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 افتراضياً.

المكونات الإضافية

في هذا القسم، يمكنك تحديد مكونات إضافية للتثبيت المترامن 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 تلقائياً إلى الأجهزة المدارة أثناء تثبيت عميل الشبكة.

إذا تم إلغاء تحديد خانة الاختيار الموجودة بجوار العلامة، فلن تتم إضافة هذه العلامة تلقائياً إلى الأجهزة المدارة أثناء تثبيت عميل الشبكة. يمكنك إضافة هذه العلامة تلقائياً إلى الأجهزة.

عند إزالة علامة من القائمة، فسيتم إزالة العلامة تلقائياً 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 أو صاف مراجعات وتحريها.

تكون إعدادات حزمة تثبيت عميل الشبكة متاحة مع أنظمة تشغيل محددة والموضحة في الجدول أدناه.

إعدادات حزمة تثبيت عميل الشبكة

Linux	Mac	Windows	قسم الخاصية
✓	✓	✓	عام
—	—	✓	إعدادات
✓ (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)	✓	الاتصال
✓	✓	✓	خيارات

			متقدمة
✓	✓	✓	مكونات إضافية
✓ (باستثناء قواعد وضع العلامات التلقائي)	✓ (باستثناء قواعد وضع العلامات التلقائي)	✓	العلامات
✓	✓	✓	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 مثبت Kaspersky Security Center.

2. في نافذة المثبت، انتقل إلى رابط استخراج حزم التثبيت.

3. في القائمة التي تفتح، حدد عميل شبكة Kaspersky Security Center 14، ثم انقر على التالي.

يظهر ملف `privacy_policy.txt` على جهازك، في المجلد الذي حدده في المجلد الفرعي `NetAgent_ <current version>`.

نشر نظم إدارة الأجهزة المحمولة

يشرح هذا القسم نشر أنظمة إدارة الجهاز المحمول باستخدام بروتوكولات Exchange ActiveSync و iOS MDM و Kaspersky Endpoint Security.

نشر نظام للإدارة عبر بروتوكول Exchange ActiveSync

يتيح لك Kaspersky Security Center إدارة الأجهزة المحمولة المتصلة بخادم الإدارة عبر استخدام بروتوكول Exchange ActiveSync. تُعد الأجهزة المحمولة (EAS Exchange ActiveSync) هي تلك الأجهزة المتصلة بخادم الأجهزة المحمولة Microsoft Exchange والتي تتم إدارتها بواسطة خادم الإدارة.

تدعم أنظمة التشغيل التالية بروتوكول Exchange ActiveSync:

- Windows Phone® 8
- Windows Phone 8.1
- Windows 10 Mobile

تعتمد مجموعة إعدادات الإدارة لجهاز Exchange ActiveSync على نظام التشغيل الذي يتم تشغيل الجهاز المحمول به. للحصول على تفاصيل حول الميزات المدعومة لبروتوكول Exchange ActiveSync لنظام تشغيل معين، يُرجى الرجوع إلى الوثائق المرفقة مع نظام التشغيل.

يشتمل نشر نظام إدارة الأجهزة المحمولة باستخدام بروتوكول Exchange ActiveSync على الخطوات التالية:

1. يقوم المسؤول بتنصيب **خادم الأجهزة المحمولة Exchange** على الجهاز العميل المحدد.
2. يقوم المسؤول بإنشاء ملف (ملفات) تعريف إدارة في وحدة تحكم الإدارة لإدارة أجهزة EAS وإضافة ملف (ملفات) التعريف إلى صناديق بريد مستخدمي Exchange ActiveSync.

ملف تعريف الإدارة للأجهزة المحمولة Exchange ActiveSync هو سياسة ActiveSync تُستخدم على خادم Microsoft Exchange لإدارة الأجهزة المحمولة Exchange ActiveSync. يمكن تعيين **ملف تعريف إدارة جهاز EAS** واحد فقط لصندوق بريد Microsoft Exchange.

يتصل مستخدمو أجهزة EAS المحمولة بصناديق بريد Exchange الخاصة بهم. أي ملف تعريف إدارة يفرض بعض **القيود على الأجهزة المحمولة**.

تنصيب خادم الجهاز المحمول لـ Exchange ActiveSync

تم تنصيب خادم الأجهزة المحمولة Exchange على جهاز عميل مثبت عليه خادم Microsoft Exchange. ننصحك بتنصيب خادم الأجهزة المحمولة Exchange على خادم Microsoft Exchange مع تعيين دور وصول العميل. في حالة تجميع العديد من خوادم Microsoft Exchange مع دور وصول العميل في نفس المجال في مصفوفة وصول العميل، فيوصى بتنصيب خادم الأجهزة المحمولة Exchange على كل خادم Microsoft Exchange في هذه المصفوفة في وضع المجموعة.

لتنصيب خادم الأجهزة المحمولة Exchange على جهاز محلي:

1. قم بتشغيل الملف التنفيذي setup.exe.
- يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها.
2. في نافذة تحديد التطبيقات، انقر على رابط **تنصيب خادم الأجهزة المحمولة Exchange** لتشغيل معالج إعداد خادم الأجهزة المحمولة Exchange.
3. في نافذة **إعدادات التنصيب**، حدد نوع تنصيب خادم الأجهزة المحمولة Exchange:

- لتنصيب خادم الأجهزة المحمولة Exchange باستخدام الإعدادات الافتراضية، حدد **تنصيب قياسي** وانقر على زر **التالي**.
- لتحديد إعدادات تنصيب خادم الأجهزة المحمولة Microsoft Exchange يدويًا، حدد **تنصيب مخصص** وانقر على **التالي**. ثم نفذ ما يلي:

a. حدد المجلد الوجهة في نافذة **المجلد الوجهة**. المجلد الافتراضي هو <Program Files\Kaspersky Lab\Mobile Device Management for Exchange>. في حالة عدم وجود هذا المجلد، يتم إنشاؤه بشكل تلقائي أثناء التنصيب. يمكنك تغيير المجلد الوجهة باستخدام الزر **استعراض**.

b. اختر نوع تنصيب خادم الأجهزة المحمولة Exchange في نافذة **وضع التنصيب**: الوضع العادي أو وضع المجموعة.

c. في نافذة **حدد الحساب**، اختر الحساب الذي سيتم استخدامه لإدارة الأجهزة المحمولة:

- **إنشاء حساب ومجموعة الأدوار تلقائيًا**. سيتم إنشاء الحساب تلقائيًا.

- **تعيين حساب.** يجب تحديد الحساب يدويًا. انقر فوق الزر **استعراض** وحدد المستخدم الذي سيتم استخدام حسابه وكلمة المرور. يجب أن ينتمي المستخدم المحدد إلى مجموعة تمتلك حقوق إدارة الأجهزة المحمولة باستخدام ActiveSync.

d. في نافذة إعدادات IIS قم بالسماح بالتكوين التلقائي أو منعه لخصائص خادم ويب خدمات معلومات الإنترنت (IIS).

إذا قمت بمنع التكوين التلقائي لخصائص خدمات معلومات الإنترنت (IIS)، فقم بتمكين آلية "مصادقة Windows" يدويًا في إعدادات IIS لـ Microsoft PowerShell Virtual Directory. إذا تم تعطيل آلية "مصادقة Windows"، فلن يعمل خادم الأجهزة المحمولة Exchange بشكل صحيح. برجاء الرجوع إلى وثائق IIS للحصول على مزيد من المعلومات حول تكوين IIS.

e. انقر فوق التالي.

4. في النافذة التي يتم فتحها، تحقق من خصائص تثبيت خادم الأجهزة المحمولة Exchange، ثم انقر على **تثبيت**.

عند انتهاء إجراءات المعالج، يتم تثبيت خادم الأجهزة المحمولة Exchange على الجهاز المحلي. سيتم عرض خادم الأجهزة المحمولة Exchange في مجلد إدارة الأجهزة المحمولة في شجرة وحدة التحكم.

اتصال الأجهزة المحمولة بخادم الأجهزة المحمولة Exchange

قبل توصيل أي من الأجهزة المحمولة، يجب تكوين خادم Microsoft Exchange من أجل السماح لاتصال الأجهزة باستخدام بروتوكول ActiveSync.

لتوصيل جهاز محمول بخادم الأجهزة المحمولة Exchange، يقوم المستخدم بالاتصال بصندوق بريد Microsoft Exchange الخاص به من الجهاز المحمول عبر ActiveSync. عند الاتصال، يجب على المستخدم تحديد إعدادات الاتصال في عميل ActiveSync، مثل عنوان البريد الإلكتروني وكلمة مرور البريد الإلكتروني.

يتم عرض الجهاز المحمول الخاص بالمستخدم والمتصل بخادم Microsoft Exchange في المجلد الفرعي **الأجهزة المحمولة** المضمن في المجلد إدارة الجهاز المحمول في شجرة وحدة التحكم.

بعد اتصال الجهاز المحمول Exchange ActiveSync بخادم الأجهزة المحمولة Exchange، يمكن للمسؤول إدارة [الجهاز المحمول Exchange](#) [ActiveSync المتصل](#).

تكوين خادم ويب خدمات معلومات الإنترنت

عند استخدام Microsoft Exchange Server (الإصدارات 2010 و2013)، يجب عليك تنشيط آلية مصادقة Windows للدليل الظاهري Windows PowerShell™ في إعدادات خادم الويب لخدمات معلومات الإنترنت (IIS). يتم تنشيط آلية المصادقة هذه تلقائيًا في حالة تحديد خيار **تكوين Microsoft (Internet Information Services (IIS) تلقائيًا** في معالج تثبيت خادم الأجهزة المحمولة Microsoft Exchange (الخيار الافتراضي).

وإلا، فستضطر لتنشيط آلية المصادقة بنفسك.

لتنشيط آلية مصادقة Windows للدليل الظاهري PowerShell يدويًا:

1. من وحدة تحكم مدير خدمات معلومات الإنترنت (IIS)، افتح خصائص الدليل الظاهري PowerShell.

2. انتقل إلى قسم **المصادقة**.

3. حدد **مصادقة Microsoft Windows**، ثم انقر فوق الزر **تمكين**.

4. افتح **إعدادات متقدمة**.

5. حدد خيار **تمكين مصادقة وضع Kernel**.

6. من القائمة المنسدلة **الحماية الموسعة**، حدد **مطلوب**.

عند استخدام Microsoft Exchange Server 2007، لا يتطلب خادم ويب خدمات معلومات الإنترنت (IIS) أية تكوين.

التثبيت المحلي لخادم الأجهزة المحمولة Exchange

للتثبيت المحلي لخادم الأجهزة المحمولة Exchange، يجب أن يقوم المسؤول بالعمليات التالية:

1. نسخ محتويات المجلد \Server\Packages\MDM4Exchange\ من حزمة توزيع Kaspersky Security Center إلى جهاز عميل.

2. قم بتشغيل الملف التنفيذي setup.exe.

يشمل التثبيت المحلي نوعين من التثبيت:

- التثبيت القياسي هو تثبيت مبسط لا يتطلب من المسؤول تحديد أي إعدادات، وهو التثبيت المستحسن في أغلب الحالات.
- التثبيت الموسع وهو التثبيت الذي يتطلب من المسؤول تحديد الإعدادات التالية:
- مسار تثبيت خادم الأجهزة المحمولة Exchange.
- وضع تشغيل خادم الأجهزة المحمولة Exchange: الوضع القياسي أو وضع المجموعة.
- إمكانية تحديد الحساب الذي سيتم تشغيل خدمة خادم الأجهزة المحمولة Exchange من خلاله.
- تمكين / تعطيل التكوين التلقائي لخادم ويب خدمات معلومات الإنترنت (IIS).

يجب تشغيل معالج تثبيت خادم الأجهزة المحمولة Exchange من خلال حساب يحتوي على جميع الحقوق المطلوبة.

التثبيت عن بُعد لخادم الأجهزة المحمولة Exchange

لتكوين التثبيت عن بُعد لخادم الأجهزة المحمولة Microsoft Exchange، يجب أن يقوم المسؤول بالإجراءات التالية:

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد المجلد **التثبيت عن بُعد**، ثم حدد المجلد الفرعي **حزم التثبيت**.

2. في مجلد **حزم التثبيت الفرعي**، افتح خصائص حزمة خادم الأجهزة المحمولة Exchange.

3. انتقل إلى قسم **الإعدادات**.

يحتوي هذا القسم على الإعدادات نفسها كتلك المستخدمة للتثبيت المحلي للتطبيق.

بعد تكوين التثبيت عن بُعد، يمكنك بدء تثبيت خادم الأجهزة المحمولة Exchange.

لتثبيت خادم الأجهزة المحمولة Exchange:

1. في شجرة وحدة تحكم إدارة Kaspersky Security Center، حدد المجلد **التثبيت عن بُعد**، ثم حدد المجلد الفرعي **حزم التثبيت**.

2. في مجلد **حزم التثبيت الفرعي**، حدد حزمة خادم الأجهزة المحمولة Exchange.

3. افتح قائمة السياق الخاصة بالحزمة وحدد **تثبيت التطبيق**.

4. في معالج التثبيت عن بُعد الذي يتم فتحه، حدد جهازاً (أو أجهزة متعددة) للتثبيت في وضع المجموعة.

5. في الحقل **تشغيل معالج الإعداد أسفل الحساب المحدد**، حدد الحساب الذي ستعمل في إطاره عملية التثبيت على الجهاز البعيد.

يجب أن يحتوي الحساب على الحقوق المطلوبة.

نشر نظام للإدارة باستخدام بروتوكول iOS MDM

يتيح لك Kaspersky Security Center إدارة الأجهزة المحمولة التي تعمل بنظام iOS. وتشير الأجهزة المحمولة iOS MDM إلى الأجهزة المحمولة iOS المتصلة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM والمُدارة بواسطة خادم الإدارة.

يتم إجراء اتصال الأجهزة المحمولة بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بالتسلسل التالي:

1. يقوم المسؤول بتهيئة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على الجهاز العميل المحدد. يتم تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM باستخدام الأدوات القياسية لنظام التشغيل.

2. يقوم المسؤول باسترداد شهادة خدمة (Apple Push Notification) (APN).

تتيح شهادة أسماء نقاط الوصول (APNs) لخادم الإدارة الاتصال بخادم APNs لإرسال إخطارات الرسائل إلى الأجهزة المحمولة iOS MDM.

3. يقوم المسؤول بتثبيت شهادة APN على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

4. يقوم المسؤول بإنشاء ملف تعريف iOS MDM لمستخدم الجهاز المحمول iOS.

يحتوي ملف تعريف iOS MDM على مجموعة من الإعدادات للاتصال بالأجهزة المحمولة iOS بخادم الإدارة.

5. يقوم المسؤول بإصدار شهادة مشتركة إلى المستخدم.

الشهادة العامة مطلوبة لتأكيد أن الجهاز المحمول مملوك للمستخدم.

6. ينقر المستخدم على الرابط المرسل بواسطة المسؤول ويقوم بتنزيل حزمة التثبيت على الجهاز المحمول.

تحتوي حزمة التثبيت على شهادة وملف تعريف iOS MDM.

بعد تنزيل ملف تعريف iOS MDM ومزامنة الجهاز المحمول iOS MDM مع خادم الإدارة، يتم عرض الجهاز في المجلد **الأجهزة المحمولة** وهو المجلد الفرعي للمجلد **إدارة الجهاز المحمول** في شجرة وحدة التحكم.

7. يقوم المسؤول بإضافة ملف تعريف التكوين على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM وتثبيت ملف تعريف التكوين على الجهاز المحمول بعد اتصاله.

يحتوي ملف تعريف التكوين على مجموعة من الإعدادات والقيود للجهاز المحمول iOS MDM، على سبيل المثال، إعدادات لتثبيت التطبيقات، وإعدادات لاستخدام ميزات مختلفة للجهاز، وإعدادات البريد الإلكتروني والجدولة. يتيح لك ملف تعريف التكوين القيام بتكوين الأجهزة المحمولة iOS MDM وفقاً لسياسات أمان المؤسسة.

8. إذا لزم الأمر، فيمكن للمسؤول إضافة ملفات تعريف التزويد على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM ثم تثبيت ملفات تعريف التزويد هذه على الأجهزة المحمولة.

ملف تعريف التزويد هو ملف تعريف يُستخدم لإدارة التطبيقات الموزعة بطرق بخلاف App Store®. يحتوي ملف التزويد على معلومات حول الترخيص، فهو مرتبط بتطبيق معين.

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 `<Program Files>\Kaspersky Lab\Mobile Device Management for iOS`. 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 للاتصال بالأجهزة 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 17.0.0/8.

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 آخر، 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 17.0.0/8 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 للاتصال بخدمة iOS MDM بعميل الشبكة. رقم المنفذ الافتراضي هو 9799.
- **المنفذ المحلي للاتصال بخدمة iOS MDM.** في هذا الحقل يمكنك تحديد منفذًا محليًا للاتصال بعميل 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 الحقل عنوان الويب للاتصال بالخادم الجهاز المحمول، حدد عنوان الجهاز العميل الذي سيتم تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM عليه.

سيتم استخدام هذا العنوان للاتصال بالأجهزة المحمولة المُدارة بخدمة iOS MDM. يجب أن يتوفر الجهاز العميل للاتصال بأجهزة iOS MDM. يمكنك تحديد عنوان كمبيوتر عميل بأيٍ من التنسيقات التالية:

• رقم FQDN (مثل mdm.example.com)

• اسم NetBIOS للجهاز

• عنوان IP الخاص بالجهاز

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 غير التفاعلي

يتيح لك Kaspersky Security Center تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على جهاز محلي في الوضع غير التفاعلي، يعني، بدون الإدخالات التفاعلية لإعدادات التثبيت.

لتثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على جهاز محلي في الوضع غير التفاعلي:

1. أقرأ [اتفاقية ترخيص المستخدم النهائي](#). استخدم الأمر أدناه فقط إذا فهمت ووافقت على شروط اتفاقية ترخيص المستخدم النهائي.

2. قم بتشغيل الأمر التالي:

```
"<exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <setup_parameters\".
```

حيث إن setup_parameters هو قائمة إعدادات وقيمها الخاصة المفصولة بمسافات (PRO1=PROP1VAL PROP2=PROP2VAL). يوجد الملف setup.exe في مجلد الخادم، والذي يُعد جزءًا من مجموعة توزيع Kaspersky Security Center.

يتم إدراج الأسماء والقيم المحتملة للمعلومات التي يمكن استخدامها عند تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الوضع غير التفاعلي في الجدول أدناه. يمكن تحديد المعلومات في أي ترتيب مناسب.

معلومات تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM في الوضع غير التفاعلي

اسم المعلمة	وصف المعلمة	القيم المتوفرة
EULA	الموافقة على شروط اتفاقية ترخيص المستخدم النهائي لبرنامج. هذه المعلمة إلزامية.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 1-لا تستخدم ملف XML مع المعلومات. قيمة أخرى أو بلا قيمة—استخدم ملف XML مع المعلومات.
INSTALLDIR	مجلد تثبيت خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. هذه المعلمة اختيارية.	قيمة السلسلة، على سبيل المثال، "INSTALLDIR="C:\install"
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.	<ul style="list-style-type: none"> رقم FQDN (مثل mdm.example.com) اسم NetBIOS للجهاز عنوان IP الخاص بالجهاز
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، "WORKFOLDER="C:\work"
MTNCY	استخدام خادم الأجهزة المحمولة التي تعمل بنظام iOS	<ul style="list-style-type: none"> 1-سيتم استخدام خادم الأجهزة

<p>المحمولة التي تعمل بنظام iOS MDM بواسطة العديد من خوادم الإدارة الافتراضية.</p> <ul style="list-style-type: none"> • قيمة أخرى أو بلا قيمة—لن يتم استخدام خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بواسطة العديد من خوادم الإدارة الافتراضية. 	<p>MDM بواسطة العديد من الخوادم الافتراضية. هذه المعلمة اختيارية.</p>
--	---

مثال:

```
exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443\
EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

يتم توفير تفاصيل معلومات 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 50000 على الأكثر. لتقليل الحمل، يمكن توزيع مجموعة الأجهزة بالكامل بين خوادم متعددة مثبتت عليها خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

يتم إجراء مصادقة أجهزة iOS MDM عبر شهادة المستخدم (أي ملف تعريف مثبت 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 مقيد (KCD)

نظام النشر المبسط

عند نشر خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بموجب النظام المبسط، 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 مقيد (KCD)

يتطلب نظام النشر باستخدام تفويض Kerberos المقيد (KCD) وجود خادم الإدارة وخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM على إنترانت المؤسسة.

يعمل نظام النشر هذا على ما يلي:

- التكامل مع Microsoft Forefront TMG
- 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 TMG.
- 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 TMG. يمكنك التأكد أن شهادة المستخدم متوافقة مع متطلبات 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 المقيد (KCD) مع الافتراضيات التالية:

- خدمة iOS MDM على الويب قيد التشغيل على المنفذ 443
- اسم الجهاز الذي يحتوي على TMG هو `tmg.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 الخاصة بالجهاز الذي يحتوي على TMG (`tmg.mydom.local`)

لتفويض حركة المرور، قم باعتماد الجهاز الذي يحتوي على TMG (`tmg.mydom.local`) إلى الخدمة المحددة بواسطة SPN (`http/iosmdm.mydom.local`).

لا اعتماد الخدمة التي تحتوي على TMG إلى الخدمة المحددة بواسطة SPN (`http/iosmdm.mydom.local`)، يجب أن يقوم المسؤول بالإجراءات التالية:

1. في أداة الإضافة الخاصة بـ Microsoft Management Console التي تحمل الاسم "مستخدم وأجهزة كمبيوتر Active Directory"، حدد الجهاز المثبت عليه (`tmg.mydom.local`).

2. في خصائص الجهاز، من علامة التبويب **التفويض**، قم بتعيين مؤشر التبدل اعتماد هذا الكمبيوتر للتفويض إلى الخدمة المحددة فقط إلى استخدام أي بروتوكول مصادقة.

3. أضف (`http/iosmdm.mydom.local`) SPN 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 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 أيضاً على سلسلة الشهادات الجذر (المفاتيح العامة).

نشر خدمة iOS MDM على الويب على TMG

على بوابة TMG، بالنسبة 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.

استخدام خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بواسطة العديد من الخوادم الافتراضية

لتمكين استخدام خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM بواسطة العديد من خوادم الإدارة الافتراضية:

1. افتح سجل النظام الخاص بالجهاز العميل المثبت عليه خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM (على سبيل المثال: محلياً، باستخدام الأمر regedit من القائمة بدء > تشغيل).

2. انتقل إلى الخلية التالية:

LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0

3. للمفتاح (ConnectorFlags (DWORD)، قم بتعيين القيمة 02102482.

4. انتقل إلى الخلية التالية:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0

5. للمفتاح (ConnInstalled (DWORD)، قم بتعيين القيمة 00000001.

6. أعد تشغيل خدمة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.

يجب إدخال قيم المفتاح بالتسلسل المحدد.

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 حديثاً، يفقد خادم الإدارة القدرة على إدارة أجهزة iOS المحمولة المتصلة حالياً.

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 لخدام 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 CSR الذي قمت بإنشائه إلى Kaspersky ليتم توقيعه.

لن يتوافر التوقيع على طلب CSR الخاص بك إلا بعد تحميل مفتاح إلى مدخل CompanyAccount يتيح استخدام إدارة الجهاز 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 معرف Apple ID عشوائي.

نوصي بتجنب استخدام معرف Apple شخصي. قم بإنشاء معرف Apple مخصص لاستخدامه كمعرف شركة خاص بك. بعد إنشاء معرف 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 والعامّة 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)

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 ومدینتک ومنطقتک وبدک.
 - 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 CSR الذي قمت بإنشائه إلى Kaspersky ليتم توقيعه.

لن يتوافر التوقيع على طلب CSR الخاص بك إلا بعد تحميل مفتاح إلى مدخل CompanyAccount يتيح استخدام إدارة الجهاز المحمول.

بعد معالجة طلبك على الإنترنت، سنتلقى ملف CSR موقعًا من Kaspersky.

8. قم بإرسال ملف طلب CSR الموقع إلى [موقع ويب Apple Inc](#). باستخدام معرف Apple ID عشوائي.

نوصي بتجنب استخدام معرف Apple شخصي. قم بإنشاء معرف Apple مخصص لاستخدامه كمعرف شركة خاص بك. بعد إنشاء معرف Apple، قم بربطه بصندوق بريد المؤسسة، وليس صندوق بريد موظف.

بعد معالجة طلب CSR الخاص بك في Apple Inc، سنتلقى 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، استخدم معرف 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.
 - 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 يمكنك من إصدار شهادة احتياطية. هذه الشهادة مخصصة للاستخدام في ملفات تعريف تكوين 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 خيارَي 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 صلاحية 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 زر **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 شجرة 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**.

في **القسم الشهادات** في مجموعة إعدادات **شهادة إخطار الرسائل من Apple** انقر فوق الزر **تثبيت**.

1. حدد ملف PFX الذي يحتوي على شهادة أسماء نقاط الوصول (APNs).

2. 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 (المصدر). لذلك، تتطلب خدمة iOS MDM على الويب الوصول إلى المنفذ TCP 2195 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 المثبت عليها خدمة iOS MDM على الويب:

1. قم بإضافة السلاسل التالية إلى السجل:

- لنظام التشغيل 32 بت:


```
"<ApnProxyHost"="<Proxy Host Name"  
"<ApnProxyPort"="<Proxy Port"  
"<ApnProxyLogin"="<Proxy Login"  
"<ApnProxyPwd"="<Proxy Password"
```

• لنظام التشغيل 64 بت:

```
C:\HINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset]  
"<ApnProxyHost"="<Proxy Host Name"  
"<ApnProxyPort"="<Proxy Port"  
"<ApnProxyLogin"="<Proxy Login"  
"<ApnProxyPwd"="<Proxy Password"
```

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 الجهاز 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 النافذة **مصدر الشهادة** من 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 تلقائياً، بواسطة أدوات خادم الإدارة، ثم تسليم الشهادة إلى الجهاز.

• تحديد ملف شهادة مشتركة.

4. في النافذة نوع الجهاز الخاصة بالمعالج، حدد الارتباط بـ Google Play.

5. في النافذة 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 النافذة معلومات الشهادة للمعالج، انقر فوق الزر 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 المجلد الأجهزة المحمولة، وهو المجلد الفرعي للمجلد إدارة الجهاز المحمول الموجود بشجرة وحدة التحكم.

إذا كان Kaspersky Endpoint Security for Android مثبتاً 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 المجلد الأجهزة المحمولة، وهو المجلد الفرعي للمجلد 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

• نظام النشر الذي يتضمن (Forefront® Threat Management Gateway (TMG

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). سنتم 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 Microsoft Forefront TMG.

• 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:

• نوع اتصال أجهزة KES بـ TMG يجب أن يكون "مصادقة SSL ثنائية الاتجاه"، أي أن الجهاز يجب أن يتصل بـ TMG 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 سيتم فتحها، حدد الشهادة ذاتها التي تم تعيينها على بوابة TMG عندما تم 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 بوابة TMG. يمكنك التأكد أن شهادة المستخدم متوافقة مع المتطلب الموضح أعلاه عن طريق استخدام طريقة من الطرق التالية:

• حدد شهادة المستخدم الخاصة في معالج حزمة التثبيت الجديدة وفي معالج تثبيت الشهادة.

• دمج خادم الإدارة مع البنية الأساسية للمفتاح العام (PKI) وتحديد الأعداد 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 الذي يحتوي على TMG هو `tmg.mydom.local`.

• اسم الجهاز المثبت 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.

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 المثبت عليه خادم الإدارة. بالنسبة لجهاز kes4mob.mydom.local المثبت عليه خادم الإدارة، سيظهر الاسم كمل يلي:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

تكوين خصائص المجال الخاصة بالجهاز الذي يحتوي على (TMG (tmg.mydom.local

لتفويض حركة المرور، يجب عليك اعتماد الجهاز الذي يحتوي على (TMG (tmg.mydom.local إلى الخدمة المحددة بواسطة SPN (http/kes4mob.mydom.local:13292).

لا اعتماد الخدمة التي تحتوي على TMG إلى الخدمة المحددة بواسطة SPN (http/kes4mob.mydom.local:13292)، يجب أن يقوم المسؤول بالإجراءات التالية:

1. في أداة الإضافة الخاصة بـ Microsoft Management Console التي تحمل الاسم "مستخدمو وأجهزة كمبيوتر Active Directory"، حدد الجهاز المثبت عليه (TMG (tmg.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 http/kes4mob.mydom.local:13292 SPN.

شهادة خاصة (مخصصة) لعملية النشر (kes4mob.mydom.global)

لنشر بروتوكول الجهاز المحمول الخاص بخادم الإدارة، يجب عليك إصدار شهادة خاصة (مخصصة) لـ kes4mob.mydom.global FQDN 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 TMG

على بوابة TMG، بالنسبة لحركة المرور التي تنتقل من جهة الجهاز المحمول إلى المنفذ 13292 الخاص بـ kes4mob.mydom.global، يجب عليك تكوين KCD على (http/kes4mob.mydom.local:13292) SPN، باستخدام شهادة الخادم التي تم إصدارها لـ kes4mob.mydom.global FQND. الرجاء ملاحظة أن النشر ونقطة الوصول المنشورة (المنفذ 13292 الخاص بخادم الإدارة) يجب أن تتشارك شهادة الخادم نفسها.

استخدام مراسلة Google Firebase Cloud

لضمان الاستجابة الفورية لأجهزة KES على Android لأوامر المسؤول، فيجب عليك تمكين استخدام مراسلة Google™ Firebase Cloud (يُشار إليها فيما بعد باسم FCM) في خصائص خادم الإدارة.

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 Google Firebase Cloud Messaging.

4. في الحقليْن مُعرّف المرسل ومفتاح الخادم، حدد إعدادات FCM: SENDER_ID ومفتاح API.

تعمل خدمة FCM في نطاق العناوين التالي:

• من جهة جهاز KES، مطلوب الوصول إلى المنافذ: (HTTPS) 443 و(HTTPS) 5228 و(HTTPS) 5229 و(HTTPS) 5230 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 (HTTPS) 443 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 خدمة FCM: استرداد SENDER_ID ومفتاح API

لتكوين خدمة FCM، يجب على المسؤول القيام بالإجراءات التالية:

1. التسجيل على [بوابة Google](#).

2. انتقل إلى [بوابة المطورين](#).

3. قم بإنشاء مشروع جديد عن طريق النقر على زر إنشاء مشروع، وحدد اسم المشروع، وحدد المعرف.

4. انتظر حتى يتم إنشاء المشروع.

في الصفحة الأولى من المشروع، في الجزء العلوي من الصفحة، يعرض حقل رقم المشروع معرف SENDER_ID ذي الصلة.

5. انتقل إلى القسم مفاتيح API & المصادقة / مفاتيح API وقم بتمكين خدمة Android لـ Google Firebase Cloud Messaging.

6. انتقل إلى القسم مفاتيح API & المصادقة / بيانات الاعتماد، وانقر على الزر إنشاء مفتاح جديد.

7. انقر على زر **مفتاح الخادم**.

8. قم بفرص القيود (إن وجدت)، انقر على زر **إنشاء**.

9. قم باسترداد مفتاح API من خصائص المفتاح الذي تم إنشاؤه حديثًا (الحقل **مفتاح الخادم**).

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:

- تعيين للمستخدم شهادة خاصة (مخصصة) من ملف في معالج اتصال الجهاز الجديد أو 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 سيستخدم 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 المثبت عليه خادم الإدارة الذي يتم بدء التكامل مع PKI منه.
- أن يملك حق تسجيل الدخول كخدمة.
- يجب أن يعمل الجهاز المثبت 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 مكون 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) و HTTPS (8061). بالإضافة إلى تغيير المنافذ، يمكنك استبدال شهادة الخادم لـ HTTPS وتغيير 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. يمكنك التثبيت المخصص من تحديد مكونات الإدارة الإضافية لـ Kaspersky المراد تثبيتها. إذا لزم الأمر، يمكنك بدء تثبيت مخطط في وضع غير تفاعلي.

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>.exe`.

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، فأنت بحاجة إلى تثبيت Kaspersky Security Center على جميع عقد المجموعة.

الإعدادات للتثبيت

قبل بدء تشغيل التثبيت، تأكد من توافق الأجهزة والبرامج على الجهاز مع متطلبات خادم الإدارة ووحدة تحكم الإدارة.

يوصى بتثبيت خادم الإدارة على خادم مخصص بدلاً من وحدة التحكم بالمجال.

يقوم Kaspersky Security Center بتخزين المعلومات الخاصة به في قاعدة بيانات خادم SQL Server. للقيام بذلك، يجب عليك تثبيت قاعدة بيانات خادم SQL Server بنفسك (تعرف على المزيد حول كيفية تحديد نظام إدارة قواعد البيانات (DBMS)). يمكن استخدام إصدارات أخرى من خادم SQL لتخزين البيانات. يجب أن تكون مثبتة على الشبكة قبل Kaspersky Security Center. يتطلب تثبيت Kaspersky Security Center حقوق المسؤول على الجهاز الذي سيتم تنفيذ التثبيت عليه.

يلزم تثبيت خادم الإدارة و عميل الشبكة ووحدة تحكم الإدارة في مجلدات لا يتم تشغيل ميزة حساسية حالة الأحرف عليها. كذلك، يلزم تعطيل حساسية حالة الأحرف للمجلد المشترك الخاص بخادم الإدارة والمجلد المخفي الخاص بـ Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

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.

بدءًا من الإصدار 10 من Service Pack 3، 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)

تقدّم الجداول التالية معلومات حول كيفية تأثير تحديد نظام إدارة قواعد البيانات على خصائص الحسابات الخاصة بالعمل باستخدام نظام إدارة قواعد البيانات.

نظام إدارة قواعد البيانات (DBMS) المحلي هو نظام إدارة قواعد بيانات مثبت على الجهاز الذي يعمل كخادم إدارة. نظام إدارة قواعد البيانات (DBMS) عن بُعد هو نظام إدارة قواعد بيانات مثبت على جهاز مختلف.

الرجاء منح كل الحقوق المطلوبة لحساب خادم الإدارة قبل بدء خدمة خادم الإدارة.

خادم SQL Server مزود بمصادقة Windows ومزود بمصادقة SQL Server

نظام إدارة قواعد البيانات (DBMS): خادم SQL Server (يشمل Express Edition) مع مصادقة Windows

موقع نظام إدارة قواعد بيانات DBMS	محلي	محلي	عن بُعد	عن بُعد
من بنشئ قاعدة بيانات KAV	المتبّت (تلقائيًا)	المسؤول (يدويًا)	المتبّت (تلقائيًا)	المسؤول (يدويًا)
الحساب الذي يعمل بموجبه المتبّت	محلي أو مجال	محلي أو مجال	المجال	المجال
حقوق الحساب الذي يعمل بموجبه المتبّت	<ul style="list-style-type: none"> النظام: حقوق المسؤول المحلي خادم SQL Server أدوار على مستوى الخادم: عامة و dbcreator Server: دور VIEW ANY DEFINITION مسؤول النظام 	<ul style="list-style-type: none"> النظام: حقوق المسؤول المحلي خادم SQL Server أدوار على مستوى الخادم: عامة و dbcreator Server: دور Sysadmin 	<ul style="list-style-type: none"> النظام: حقوق المسؤول المحلي خادم SQL Server أدوار على مستوى الخادم: عامة و dbcreator Server: دور VIEW ANY DEFINITION 	<ul style="list-style-type: none"> النظام: حقوق المسؤول المحلي خادم SQL Server أدوار على مستوى الخادم: عامة و dbcreator Server: دور VIEW ANY DEFINITION

<p>إذن عرض حالة الخادم (إذا تم تمكين ميزة "التشغيل الدائم") بالنسبة لقواعد البيانات الرئيسية و tempdb: الدور العام ونظام dbo لقاعدة بيانات KAV (فقط في حالة استخدام قاعدة بيانات KAV موجودة): دور db_owner ونظام dbo</p>		<p>بالنسبة لقواعد البيانات الرئيسية و tempdb: الدور العام ونظام dbo لقاعدة بيانات KAV (فقط في حالة استخدام قاعدة بيانات KAV موجودة): دور db_owner ونظام dbo</p>		
<p>المجال.</p>	<p>المجال.</p>	<ul style="list-style-type: none"> تم إنشائه تلقائيًا بتنسيق *-KL-AK الحساب المحلي الذي حدده المسؤول حساب المجال الذي حدده المسؤول 	<ul style="list-style-type: none"> تم إنشائه تلقائيًا بتنسيق *-KL-AK الحساب المحلي الذي حدده المسؤول حساب المجال الذي حدده المسؤول 	<p>حساب خادم الإدارة</p>
<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت. خادم SQL Server دور على مستوى الخادم: العامة إذن VIEW ANY DEFINITION إذن عرض حالة الخادم (إذا تم تمكين ميزة "التشغيل الدائم") بالنسبة لقواعد البيانات الرئيسية و tempdb: الدور العام ونظام dbo بالنسبة لقاعدة بيانات KAV: دور db_owner ونظام dbo 	<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت خادم SQL Server: الحقوق المطلوبة المعيّنة بواسطة المثبت 	<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت. خادم SQL Server دور على مستوى الخادم: العامة إذن VIEW ANY DEFINITION إذن عرض حالة الخادم (إذا تم تمكين ميزة "التشغيل الدائم") بالنسبة لقواعد البيانات الرئيسية و tempdb: الدور العام ونظام dbo بالنسبة لقاعدة بيانات KAV: دور db_owner ونظام dbo 	<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت خادم SQL Server: الحقوق المطلوبة المعيّنة بواسطة المثبت 	<p>حقوق حساب خدمة خادم الإدارة</p>

نظام إدارة قواعد بيانات DBMS: خادم SQL Server (يشمل Express Edition) مع مصادقة SQL Server

<p>عن بُعد.</p>	<p>محلي.</p>	<p>موقع نظام إدارة قواعد بيانات DBMS</p>
<p>المسؤول (يدويًا) أو المثبت (تلقائيًا).</p>	<p>المسؤول (يدويًا) أو المثبت (تلقائيًا).</p>	<p>من ينشئ قاعدة بيانات KAV</p>
<p>المجال.</p>	<p>محلي.</p>	<p>الحساب الذي يعمل بموجبه المثبت</p>
<ul style="list-style-type: none"> النظام: حقوق المسؤول المحلي. خادم SQL Server: لا يتطلب حساب المثبت الوصول إلى خادم SQL Server. 	<ul style="list-style-type: none"> النظام: حقوق المسؤول المحلي. خادم SQL Server: لا يتطلب حساب المثبت الوصول إلى خادم SQL Server. 	<p>حقوق الحساب الذي يعمل بموجبه المثبت</p>

المجال.	محلي أو مجال.	حساب خدمة خادم إدارة
<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت. خادم SQL Server: لا يتطلب حساب خدمة خادم الإدارة الوصول إلى خادم SQL Server. 	<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت. خادم SQL Server: لا يتطلب حساب خدمة خادم الإدارة الوصول إلى خادم SQL Server. 	حقوق حساب خدمة خادم الإدارة
يحدد المسؤول بشكل صريح في المثبت حساب خادم SQL Server الداخلي الذي يتطلب الدور sysadmin.	يحدد المسؤول بشكل صريح في المثبت حساب خادم SQL Server الداخلي الذي يتطلب الدور sysadmin.	معلومات إضافية

MySQL

نظام إدارة قواعد البيانات DBMS: خادم MySQL

محلي أو عن بُعد.	محلي أو عن بُعد.	موقع نظام إدارة قواعد بيانات DBMS
المسؤول (يدويًا).	المثبت (تلقائيًا).	من ينشئ قاعدة بيانات KAV
محلي أو مجال.	محلي أو مجال.	الحساب الذي يعمل بموجبه المثبت
<ul style="list-style-type: none"> النظام: حقوق المسؤول المحلي. خادم MySQL Server: لا يتطلب حساب المثبت الوصول إلى MySQL. 	<ul style="list-style-type: none"> النظام: حقوق المسؤول المحلي. خادم MySQL Server: لا يتطلب حساب المثبت الوصول إلى MySQL. 	حقوق الحساب الذي يعمل بموجبه المثبت
محلي أو مجال.	محلي أو مجال.	حساب خدمة خادم إدارة
<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت. خادم MySQL Server: لا يتطلب حساب خدمة خادم الإدارة الوصول إلى MySQL. 	<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت. خادم MySQL Server: لا يتطلب حساب خدمة خادم الإدارة الوصول إلى MySQL. 	حقوق حساب خدمة خادم الإدارة
يحدد المسؤول بشكل صريح في المثبت حساب داخلي لـ MySQL الذي يتطلب "منح الكل" لقاعدة بيانات KAV، أو "تحديد" أو "طريقة العرض" أو "معالجة" لجداول النظام. الأدونات المطلوبة لخادم MySQL هي:	يحدد المسؤول بشكل صريح في المثبت حساب خادم SQL Server الداخلي الذي يتطلب الوصول إلى الجذر.	معلومات إضافية
<ul style="list-style-type: none"> تحديد إدراج تحديث حذف إنشاء 		

- قطرة
- معالجة
- المراجع
- فهرس
- تغيير
- عرض قواعد البيانات
- إنشاء الجداول المؤقتة
- جداول القفل
- تنفيذ
- إنشاء عرض
- إظهار العرض
- إنشاء روتين
- تغيير الروتين
- الحدث
- المشغل
- SUPER

مطلوب إذن SUPER فقط للاستعادة من نسخة احتياطية.

MariaDB

نظام إدارة قواعد البيانات: MariaDB

موقع نظام إدارة قواعد بيانات DBMS	محلي أو عن بُعد.	محلي أو عن بُعد.
من بنشئ قاعدة بيانات KAV	المسؤول (يدويًا).	المتنبت (تلقائيًا).
الحساب الذي يعمل بموجبه المتنبت	محلي أو مجال.	محلي أو مجال.
حقوق الحساب الذي يعمل بموجبه المتنبت	<ul style="list-style-type: none"> • النظام: حقوق المسؤول المحلي. • خادم MariaDB Server: لا يتطلب حساب المتنبت الوصول إلى MariaDB. 	<ul style="list-style-type: none"> • النظام: حقوق المسؤول المحلي. • خادم MariaDB Server: لا يتطلب حساب المتنبت الوصول إلى MariaDB.

محلي أو مجال.	محلي أو مجال.	حساب خدمة خادم إدارة
<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت. خادم MariaDB Server: لا يتطلب حساب خدمة خادم الإدارة الوصول إلى MariaDB. 	<ul style="list-style-type: none"> النظام: الحقوق المطلوبة المعيّنة بواسطة المثبت. خادم MariaDB Server: لا يتطلب حساب خدمة خادم الإدارة الوصول إلى MariaDB. 	حقوق حساب خدمة خادم الإدارة
يحدد المسؤول بشكلٍ صريح في المثبت حساب داخلي لـ MariaDB يتطلب SHOW VIEW و SELECT و KAV، لقاعدة بيانات KAV، و PROCESS لجداول النظام.	يحدد المسؤول بشكلٍ صريح في المثبت حساب خادم SQL Server الداخلي الذي يتطلب الوصول إلى الجذر.	معلومات إضافية

السيناريو: مصادقة خادم Microsoft SQL

تنطبق المعلومات الواردة في هذا القسم فقط على التكوينات التي يُستخدم فيها Microsoft SQL Server Kaspersky Security Center كنظام 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 (x.13). في (SQL Server 2016 (13.x) والإصدارات الأحدث، استخدم شهادة TLS.

على سبيل المثال، لإنشاء شهادة TLS، أدخل الأمر التالي في PowerShell:

```
New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert: \
LocalMachine -KeySpec KeyExchange
```

بخصوص الأمر، بدلاً من SQL_HOST_NAME، يجب كتابة اسم مضيف SQL Server إذا كان المضيف مضمناً في المجال أو اكتب اسم المجال المؤهل بالكامل (FQDN) للمضيف إذا لم يكن المضيف مدرجاً 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 Kaspersky Security Center و SQL Server

على جهاز خادم الإدارة، اضبط القيمة 1 على متغير البيئة KLBADO_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 KLBADO_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:

o تأكد من أن الإصدار المثبت من خادم SQL Server هو تطبيق 64 بت.

o قم بتثبيت برنامج تشغيل Microsoft OLE DB على جهاز خادم الإدارة. للحصول على التفاصيل، راجع وثائق Microsoft.

o على جهاز خادم الإدارة، اضبط القيمة 1 على متغير البيئة KLBADO_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 KLBADO_UseMSOLEDBSQL، ثم قم بتعيين القيمة 1.

7 تمكين استخدام بروتوكول TCP/IP على مثيل مسمى لخادم SQL Server

إذا كنت تستخدم مثيلاً مسمىاً 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 إعدادات الخادم الإدارة، حدد اسم مضيف خادم SQL Server ورقم المنفذ في حقل اسم مثيل SQL Server.

توصيات حول تثبيت خادم الإدارة

يحتوي هذا القسم على توصيات حول كيفية تثبيت خادم الإدارة. يقدم 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 المثبت تلقائيًا بإنشاء حسابات غير مميزة لخدمات خادم الإدارة. هذا السلوك هو الأكثر ملاءمة 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 المسمى KAdmins.

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، من 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 ينفق 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 افتراضياً

• 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 الموصولة 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 الجهاز 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 14 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. 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**.

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 14 Web Console

يتم عرض هذه الخطوة فقط إذا كنت تستخدم نظام تشغيل 64 بت. وخلافاً لذلك، لا يتم عرض هذه الخطوة، لأن Kaspersky Security Center 14 Web Console لا يعمل مع أنظمة تشغيل 32 بت.

بشكل افتراضي، سيتم تثبيت كل من both Kaspersky Security Center 14 Web ووحدة تحكم الإدارة المستندة إلى MMC.

إذا كنت ترغب في تثبيت Kaspersky Security Center 14 Web Console فقط:

1. حدد تثبيت وحدة التحكم هذه فقط.

2. اختر وحدة تحكم مستندة إلى الويب من القائمة المنسدلة.

تثبيت Kaspersky Security Center 14 Web Console يبدأ ألياً بعد إكمال تثبيت خادم الإدارة.

إذا كنت ترغب في تثبيت وحدة التحكم المستندة إلى MMC فقط:

1. حدد تثبيت وحدة التحكم هذه فقط.

2. اختر وحدة تحكم مستندة إلى MMC من القائمة المنسدلة.

الخطوة 4. تحديد 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 يتطابقا.

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	101 – 1000 جهاز	1001–5000 جهاز	أكثر من 5000 جهاز
عرض مع عقدة خوادم الإدارة الثانوية والظاهرية وجميع الإعدادات المتعلقة بخوادم الإدارة الثانوية والظاهرية في شجرة وحدة التحكم	غير متاح	غير متاح	متاح	متاح
عرض مع أقسام الأمان في نوافذ خصائص خادم الإدارة ومجموعات الإدارة	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 10000 جهاز. بالنسبة لنظام إدارة قاعدة بيانات MariaDB، فإن الحد الأقصى الموصى به من الأجهزة المدارة هو 20000 جهاز.

الخطوة 5. تحديد قاعدة البيانات

عند هذه الخطوة من المعالج، يجب أن تقوم بتحديد آلية – Microsoft SQL Server (SQL Express) أو MySQL – التي سيتم استخدامها لتخزين قاعدة بيانات خادم الإدارة. خيار MySQL مناسب لكل من MySQL وMariaDB.

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) محلياً (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 محلياً.

يتم توفير بنية قاعدة بيانات خادم الإدارة في الملف klakdb.chm، الموجود في مجلد تثبيت Kaspersky Security Center (يتوفر هذا الملف أيضاً في أرشيف يوجد على بوابة Kaspersky: klakdb.zip).

الخطوة 6. تكوين خادم SQL Server

في هذه الخطوة من المعالج، عليك تكوين خادم SQL Server.

بناءً على قاعدة البيانات التي حددتها، حدد الإعدادات التالية:

• إذا اخترت خادم (Microsoft SQL Server Express) SQL Server في الخطوة السابقة:

• في الحقل اسم ممثل 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 مفصلاً بفاصلة، على سبيل المثال:

SQL_Server_host_name,1433

إذا قمت بتأمين الاتصال بين خادم الإدارة و SQL Server عن طريق شهادة، فحدد في حقل اسم ممثل خادم SQL Server نفس اسم المضيف الذي تم استخدامه في إنشاء الشهادة. إذا كنت تستخدم مثيلاً مسمىً من SQL Server، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصلاً بفاصلة، على سبيل المثال:

SQL_Server_name,1433

إذا كنت تستخدم العديد من مثيلات خادم SQL Server على نفس المضيف، فحدد أيضاً اسم المثل مفصلاً بشرطة مائلة للخلف، على سبيل المثال:

SQL_Server_name\SQL_Server_instance_name,1433

إذا تم تمكين ميزة "التشغيل الدائم" في خادم SQL على شبكة المؤسسة، فحدد اسم مستمع مجموعة الإتاحة في حقل اسم ممثل خادم SQL. يرجى العلم أن خادم الإدارة يدعم فقط وضع توفير الالتزام المتزامن عند تمكين ميزة "التشغيل الدائم".

• في الحقل اسم قاعدة البيانات، حدد اسم قاعدة البيانات التي تم إنشاؤها لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

• إذا حددت MySQL في الخطوة السابقة:

• في الحقل اسم ممثل خادم SQL Server، حدد اسم ممثل خادم SQL Server. 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 بقاعدة بيانات خادم SQL Server. رقم المنفذ الافتراضي هو 3306.

- في الحقل اسم قاعدة البيانات، حدد اسم قاعدة البيانات التي تم إنشاؤها 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.

الخطوة 7. تحديد وضع مصادقة

حدد وضع المصادقة الذي سيتم استخدامه عند اتصال خادم الإدارة بخادم SQL Server.

بناءً على قاعدة البيانات المحددة، يمكنك الاختيار من بين أوضاع المصادقة التالية.

- 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. املا حقل الحساب وكلمة 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 ترقيّة 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 لخادم MySQL أو MariaDB، 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 14 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 14 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 14 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 مطالبته 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 الجهاز 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 14** 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 مطالبته أيضًا بعرض اتفاقيات الترخيص وسياسات الخصوصية لمكونات إدارة التطبيق الإضافية المتوفرة في حزمة توزيع Kaspersky Security Center.

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**.

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 و منافذ الاتصال بخادم الإدارة وإعدادات قاعدة البيانات. يمكنك التثبيت المخصص من تحديد مكونات الإدارة الإضافية لـ Kaspersky المراد 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 تثبيتها.

عند هذه الخطوة، يجب أن تحدد مجلدًا لتثبيت مكونات خادم الإدارة. بشكل افتراضي، يتم تثبيت المكونات على <Program Files\Kaspersky>\Disk. 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 14 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 14 Web Console لا يعمل مع أنظمة تشغيل 32 بت.

بشكل افتراضي، سيتم تثبيت كل من Kaspersky Security Center 14 Web Console ووحدة تحكم الإدارة المستندة إلى MMC.

إذا كنت ترغب في تثبيت Kaspersky Security Center 14 Web Console فقط:

1. حدد تثبيت وحدة التحكم هذه فقط.

2. اختر وحدة تحكم مستندة إلى الويب من القائمة المنسدلة.

[تثبيت Kaspersky Security Center 14 Web Console](#) يبدأ آليًا بعد إكمال تثبيت خادم الإدارة.

إذا كنت ترغب في تثبيت وحدة التحكم المستندة إلى MMC فقط:

1. حدد تثبيت وحدة التحكم هذه فقط.

الخطوة 5. تحديد 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	101 – 1000 جهاز	1001–5000 جهاز	أكثر من 5000 جهاز
عرض مع عقدة خوادم الإدارة الثانوية والظاهرية وجميع الإعدادات المتعلقة بخوادم الإدارة الثانوية والظاهرية في شجرة وحدة التحكم	غير متاح	غير متاح	متاح	متاح
عرض مع أقسام الأمان في نوافذ خصائص خادم الإدارة ومجموعات الإدارة	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 10000 جهاز. بالنسبة لنظام إدارة قاعدة بيانات MariaDB، فإن الحد الأقصى الموصى به من الأجهزة المدارة هو 20000 جهاز.

الخطوة 6. تحديد قاعدة البيانات

عند هذه الخطوة من المعالج، يجب أن تقوم بتحديد آلية – Microsoft SQL Server (SQL Express) أو MySQL – التي سيتم استخدامها لتخزين قاعدة بيانات خادم الإدارة. خيار MySQL مناسب لكل من MySQL وMariaDB.

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، عليك تكوين خادم SQL Server.

بناءً على قاعدة البيانات التي حددتها، حدد الإعدادات التالية:

- إذا اخترت خادم (Microsoft SQL Server Express) SQL Server 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 مفصلاً بفاصلة، على سبيل المثال:

SQL_Server_host_name,1433

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 مثيلاً مسمىً من SQL Server، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصلاً بفاصلة، على سبيل المثال:

SQL_Server_name,1433

إذا كنت تستخدم العديد من مثيلات خادم SQL Server على نفس المضيف، فحدد أيضاً اسم المثل مفصلاً بشرطة مائلة للخلف، على سبيل المثال:

SQL_Server_name\SQL_Server_instance_name,1433

إذا تم تمكين ميزة "التشغيل الدائم" في خادم SQL على شبكة المؤسسة، فحدد اسم مستمع مجموعة الإتاحة في حقل اسم مثيل خادم SQL. يرجى العلم أن خادم الإدارة يدعم فقط وضع توفير الالتزام المتزامن عند تمكين ميزة "التشغيل الدائم".

- في الحقل اسم قاعدة البيانات، حدد اسم قاعدة البيانات التي تم إنشاؤها لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

- إذا حددت MySQL في الخطوة السابقة:

- في الحقل اسم مثيل خادم SQL Server، حدد اسم مثيل خادم SQL Server. 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 بقاعدة بيانات خادم SQL Server. رقم المنفذ الافتراضي هو 3306.

- في الحقل اسم قاعدة البيانات، حدد اسم قاعدة البيانات التي تم إنشاؤها 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.

الخطوة 8. تحديد وضع مصادقة

حدد وضع المصادقة الذي سيتم استخدامه عند اتصال خادم الإدارة بخادم SQL Server.

بناءً على قاعدة البيانات المحددة، يمكنك الاختيار من بين أوضاع المصادقة التالية.

- 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. املاً حقل **الحساب وكلمة المرور.**
 - رؤية 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 ترقيّة 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 لخادم MySQL أو MariaDB، 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 ك DBMS**، بما في ذلك **SQL Express** الموجود على جهاز آخر و/أو كنت تخطط **لتحديد موقع المجلد المشترك** على جهاز آخر. بدءًا من الإصدار 10 من Service Pack 3، يدعم Kaspersky Security Center حسابات الخدمة المُدارة وحسابات الخدمة المدارة الجماعية. 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.

إذا قررت لاحقًا تغيير حساب خادم الإدارة، يمكنك استخدام الأداة الإضافية الخاصة بتعديل حساب خادم الإدارة (klsvswch).

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 KIScSvc 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 قبل 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 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 دليلًا 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.

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 مأخذ التوصيل الأمانة (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).

إذا تم تثبيت خادم الإدارة على جهاز يقوم بتشغيل Microsoft Windows XP Service Pack 2، فسيقوم جدار حماية النظام المضمن بحظر منافذ TCP 13000 و 14000. لذلك، للسماح بالوصول إلى خادم الإدارة على الجهاز بعد التثبيت، يجب فتح هذه المنافذ يدويًا.

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 لاحقاً.

إذا قمت بتثبيت Kaspersky Security Center على العقدة المفعلة لمجموعة تجاوز الفشل من Kaspersky وقمت بإنشاء محول شبكة افتراضي 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 الخاص بالاتصال بالأجهزة المحمولة

تتوفر هذه الخطوة من معالج الإعداد إذا قمت بتحديد إدارة الجهاز المحمول للتثبيت.

في نافذة **عنوان الاتصال بالأجهزة 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 تلقائياً 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 متاحاً فقط في حالة اختيارك لتثبيت Kaspersky Security Center 14 Web Console في إحدى الخطوات السابقة.

يمكنك أيضاً النقر فوق **إنهاء** لإغلاق المعالج دون بدء العمل مع Kaspersky Security Center. يمكنك بدء العمل لاحقاً في أي وقت.

عند بدء التشغيل الأول لوحدة تحكم الإدارة أو Kaspersky Security Center 14 Web Console، يمكنك القيام بـ الإعداد الأولي للتطبيق.

نشر مجموعة تجاوز الفشل من Kaspersky

يحتوي هذا القسم على معلومات عامة حول مجموعة تجاوز الفشل من Kaspersky وإرشادات حول إعداد ونشر مجموعة تجاوز الفشل من Kaspersky في شبكتك.

سيناريو: نشر مجموعة تجاوز الفشل من Kaspersky

توفر مجموعة تجاوز الفشل من Kaspersky إتاحةً عاليةً لـ 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. تأكد من أن خادم الملفات يلبي متطلبات الأجهزة والبرامج، وأنشئ مجلدين مشتركين لبيانات Kaspersky Security Center، وقم بتكوين الأذونات للوصول إلى المجلدات المشتركة.

إرشادات كيفية: [إعداد خادم ملفات لمجموعة تجاوز الفشل في Kaspersky](#)

3 إعداد العقد المفعلة والخاملة

قم بإعداد جهازي كمبيوتر بأجهزة وبرامج متطابقة للعمل كعقدة نشطة وخاملة.

إرشادات كيفية: [تحضير عقد لمجموعة تجاوز الفشل من Kaspersky](#)

4 تثبيت نظام إدارة قواعد البيانات (DBMS)

حدد أيًا من [نظام إدارة قواعد البيانات المدعوم \(DBMS\)](#)، ثم قم بتثبيت نظام إدارة قواعد البيانات على جهاز كمبيوتر مخصص.

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 العقدة المفعلة، ثم تثبيته على العقدة الخاملة.

إرشادات كيفية: [تثبيت Kaspersky Security Center على عقد مجموعة تجاوز الفشل من Kaspersky](#)

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. يرجى التعرف على [الأحداث التي تؤدي إلى التبديل بين العقد المفعلة والعقد الخاملة](#).

حول مجموعة تجاوز الفشل من Kaspersky

توفر مجموعة تجاوز الفشل من Kaspersky إتاحةً عاليةً لـ Kaspersky Security Center وتقلل من وقت تعطل خادم الإدارة في حالة حدوث عطل. 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.

متطلبات الأجهزة والبرامج

لنشر مجموعة تجاوز الفشل من Kaspersky، يجب أن يكون لديك الأجهزة التالية:

- جهازي كمبيوتر بأجهزة وبرامج متطابقة. ستعمل أجهزة الكمبيوتر هذه كعقد نشطة وخاملة.
- خادم ملفات يدعم بروتوكول CIFS/SMB، إصدار 2.0 أو أعلى. يجب عليك توفير جهاز كمبيوتر مخصص يعمل كخادم ملفات.

تأكد من توفير نطاق ترددي مرتفع للشبكة بين خادم الملفات والعقد المفعلة والخاملة.

- جهاز كمبيوتر يحتوي على نظام إدارة قواعد البيانات (DBMS).

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 مؤقتاً 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 و klnagent و klactprx و klwebsrv.
- تم قطع اتصال الشبكة بين العقدة المفعلة والتخزين على خادم الملفات أو إنهاؤه.

تحضير خادم ملف لمجموعة تجاوز الفشل من Kaspersky

يعمل خادم الملفات كمكون مطلوب من مجموعة تجاوز الفشل من Kaspersky.

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 KAdmins.

- حسابات المستخدمين \$ <node1> و \$ <node2>. هنا، <node1> و <node2> هما أسماء أجهزة الكمبيوتر الخاصة بالعقد المفعلة والخاملة. تم إعداد خادم الملفات. لنشر مجموعة تجاوز الفشل Kaspersky، اتبع الإرشادات الإضافية في هذا [السيناريو](#).

تحضير العقد لنظام مجموعة تجاوز الفشل من Kaspersky

قم بإعداد جهازي كمبيوتر للعمل كعقد نشطة وخاملة لـ [مجموعة تجاوز الفشل من Kaspersky](#).

لتحضير عقد لمجموعة تجاوز الفشل من Kaspersky

1. تأكد من أن جهازي الكمبيوتر يلبيان [متطلبات الأجهزة والبرامج](#). ستعمل أجهزة الكمبيوتر 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:

- على كل عقد، قم بإنشاء محول شبكة افتراضي. يمكنك القيام بذلك باستخدام برنامج لجهة خارجية. يرجى التأكد من استيفاء الشروط التالية:

- يجب تعطيل محولات الشبكة الافتراضية. يمكنك إنشاء محولات الشبكة الافتراضية في حالة التعطيل أو تعطيلها بعد الإنشاء.

- يجب أن يكون لمحولات الشبكة الافتراضية على كلا العقدتين نفس عنوان IP.

- استخدم موازن تحميل تابع لجهة خارجية. على سبيل المثال، يمكنك استخدام خادم nginx. في هذه الحالة، نفذ ما يلي:

a. قم بتوفير جهاز كمبيوتر يعمل بنظام Linux مع تثبيت nginx.

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 و UDP13000 و TCP 13291 و TCP 13299 و TCP 17000.

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، اتبع الإرشادات الإضافية الواردة في [السيناريو](#).

تثبيت Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky

تم تثبيت Kaspersky Security Center على كلا العقدتين في مجموعة تجاوز الفشل من Kaspersky 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 KAdmins تثبيت Kaspersky Security Center على كل عقدة.

لتثبيت Kaspersky Security Center على العقدة المفعلة لمجموعة تجاوز الفشل من Kaspersky:

1. تشغيل الملف التنفيذي ksc_14_<build number>_full_<language>.exe

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها. في نافذة تحديد التطبيق، انقر فوق رابط تثبيت خادم إدارة Kaspersky Security Center 14 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 جيداً 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 فشل Kaspersky 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 العقدة**.

• حدد وضع اتصال المجموعة: عبر محول شبكة افتراضي أو موازن تحميل تابع لجهة خارجية.

5. قم بإجراء خطوات أخرى للتثبيت المخصص، بدءاً من **الخطوة 3**.

في **الخطوة 13**، حدد عنوان IP لمحول شبكة ظاهري إذا كنت قد أنشأت محولاً أثناء **تحضير عقد 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:

1. تشغيل الملف التنفيذي ksc_14_<build number>_full_<language>.exe

يتم فتح نافذة تُطالبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها. في نافذة تحديد التطبيق، انقر فوق رابط تثبيت خادم إدارة Kaspersky Security Center 14 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 جيداً 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 فشل Kaspersky لتثبيت التطبيق على العقدة الخاملة.

4. في نافذة **المجلد المشترك** و**نافذة مشاركة الحالة**، حدد مساراً 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 للتأكد من أنك قمت بتكوينها بشكل صحيح وأن الكتلة تعمل بشكل صحيح.

بدء تشغيل مهمة وإيقافها يدويًا

قد تحتاج إلى إيقاف مجموعة تجاوز فشل Kaspersky 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 المفصلة، انتقل إلى <Program Files (x86)\Kaspersky Lab\Kaspersky Security Center>.\Disk>.

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

للمحافظة على إحدى العقد:

1. على العقدة المفصلة، قم بإيقاف مجموعة تجاوز الفشل باستخدام الأمر `klfoc -stopcluster --stp klfoc`.

2. في العقدة التي تريد الحفاظ عليها، انتقل إلى <Program Files (x86)\Kaspersky Lab\Kaspersky Security Center>.\Disk>.

3. افتح سطر الأوامر، ثم افصل العقدة عن المجموعة عن طريق تشغيل الأمر `detach_node.cmd`.

4. على العقدة المفصلة، ابدأ تشغيل نظام مجموعة تجاوز الفشل باستخدام الأمر `klfoc -startcluster --stp klfoc`.

5. أداء أنشطة الصيانة.

6. على العقدة المفصلة، قم بإيقاف مجموعة تجاوز الفشل باستخدام الأمر `klfoc -stopcluster --stp klfoc`.

7. في العقدة التي تم الحفاظ عليها، انتقل إلى <Program Files (x86)\Kaspersky Lab\Kaspersky Security Center>.\Disk>.

8. افتح سطر الأوامر، ثم قم بإرفاق العقدة بالكتلة عن طريق تشغيل الأمر `attach_node.cmd`.

9. على العقدة المفصلة، ابدأ تشغيل نظام مجموعة تجاوز الفشل باستخدام الأمر `klfoc -startcluster --stp klfoc`.

يتم الاحتفاظ بالعقدة وإرفاقها بمجموعة تجاوز الفشل.

تثبيت خادم الإدارة على نظام مجموعة تجاوز الفشل

تختلف عملية تثبيت خادم الإدارة على مجموعة تجاوز الفشل عن التثبيت القياسي والمخصص على جهاز مستقل.

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 تطلبك بتحديد تطبيقات Kaspersky التي سيتم تثبيتها. في نافذة تحديد التطبيق، انقر فوق رابط تثبيت خادم إدارة Kaspersky Security Center 14 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. 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**.

الخطوة 2. تحدد نوع التثبيت على نظام مجموعة

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.

• **محلياً (يكون التثبيت على هذا الجهاز فقط)**

إذا حددت هذا الخيار، فسيتم تثبيت خادم الإدارة فقط على العقدة الحالية، كما لو كان مثبتاً 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**، بدءاً 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 14 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 ومرتبطة 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 مثل 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 مثل 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 تثبيتها.

عند هذه الخطوة، يجب أن تحدد مجلدًا لتثبيت مكونات خادم الإدارة. بشكل افتراضي، يتم تثبيت المكونات على <Program Files\Kaspersky>\Disk. 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 9. تحديد 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	101 – 1000 جهاز	1001 – 5000 جهاز	أكثر من 5000 جهاز
عرض مع عقدة خوادم الإدارة الثانوية والظاهرية وجميع الإعدادات المتعلقة بخوادم الإدارة الثانوية والظاهرية في شجرة وحدة التحكم	غير متاح	غير متاح	متاح	متاح
عرض مع أقسام الأمان في نوافذ خصائص خادم الإدارة ومجموعات الإدارة	غير متاح	غير متاح	متاح	متاح
التوزيع العشوائي لوقت بدء التشغيل لمهمة التحديث على الأجهزة العميلة	غير	على مدى فاصل	على مدى فاصل	على مدى فاصل

إذا قمت بتوصيل خادم الإدارة بخادم قاعدة بيانات MySQL 5.7 أو SQL Express، فلا يوصى باستخدام التطبيق لإدارة أكثر من 10000 جهاز. بالنسبة لنظام إدارة قاعدة بيانات MariaDB، فإن الحد الأقصى الموصى به من الأجهزة المدارة هو 20000 جهاز.

الخطوة 10. تحديد قاعدة البيانات

عند هذه الخطوة من المعالج، يجب أن تقوم بتحديد آلية – Microsoft SQL Server (SQL Express) أو MySQL – التي سيتم استخدامها لتخزين قاعدة بيانات خادم الإدارة. خيار MySQL مناسب لكل من MySQL وMariaDB.

يوصى بتثبيت خادم الإدارة على خادم مخصص بدلاً من وحدة التحكم بالمال. ومع ذلك، إذا قمت بتثبيت Kaspersky Security Center على خادم يعمل كوحدة تحكم بالمال للقراءة فقط (RODC)، فلا يجب حينها تثبيت Microsoft SQL Server (SQL Express) محلياً (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 محلياً.

يتم توفير بنية قاعدة بيانات خادم الإدارة في الملف klakdb.chm، الموجود في مجلد تثبيت Kaspersky Security Center (يتوفر هذا الملف أيضاً في أرشيف يوجد على بوابة Kaspersky: [klakdb.zip](https://www.kaspersky.com/klakdb.zip)).

الخطوة 11. تكوين خادم SQL Server

في هذه الخطوة من المعالج، عليك تكوين خادم SQL Server.

بناءً على قاعدة البيانات التي حددتها، حدد الإعدادات التالية:

- إذا اخترت خادم (Microsoft 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 مفصلاً بفاصلة، على سبيل المثال:

SQL_Server_host_name,1433

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 مثيلاً مسمياً من SQL Server، فاستخدم اسم مضيف خادم SQL Server وحدد رقم المنفذ مفصلاً بفاصلة، على سبيل المثال:

SQL_Server_name,1433

إذا كنت تستخدم العديد من مثيلات خادم SQL Server على نفس المضيف، فحدد أيضاً اسم المثيل مفصلاً بفاصلة للخلف، على سبيل المثال:

SQL_Server_name\SQL_Server_instance_name,1433

إذا تم تمكين ميزة "التشغيل الدائم" في خادم SQL على شبكة المؤسسة، فحدد اسم مستمع مجموعة الإتاحة في حقل اسم مثيل خادم SQL. يرجى العلم أن خادم الإدارة يدعم فقط وضع توفير الالتزام المنزمن عند تمكين ميزة "التشغيل الدائم".

- في الحقل اسم قاعدة البيانات، حدد اسم قاعدة البيانات التي تم إنشاؤها لتخزين بيانات خادم الإدارة. القيمة الافتراضية هي KAV.

• إذا حددت MySQL في الخطوة السابقة:

- في الحقل اسم مثيل خادم SQL Server، حدد اسم مثيل خادم SQL Server. 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 بقاعدة بيانات خادم SQL Server. رقم المنفذ الافتراضي هو 3306.
- في الحقل اسم قاعدة البيانات، حدد اسم قاعدة البيانات التي تم إنشاؤها 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.

الخطوة 12. تحديد وضع مصادقة

حدد وضع المصادقة الذي سيتم استخدامه عند اتصال خادم الإدارة بخادم SQL Server.

بناءً على قاعدة البيانات المحددة، يمكنك الاختيار من بين أوضاع المصادقة التالية:

- 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. املا حقل الحساب وكلمة 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 لخادم MySQL أو MariaDB، 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.

سيُتبع عليك تحديد حساب مجال، على سبيل المثال إن كنت تخطط لاستخدام مثيل خادم SQL Server من أي إصدار ك DBMS، بما في ذلك SQL Express الموجود على جهاز آخر و/أو كنت تخطط لتحديد موقع المجلد المشترك على جهاز آخر.

بدءًا من الإصدار 10 من Service Pack 3، يدعم Kaspersky Security Center حسابات الخدمة المُدارة وحسابات الخدمة المُدارة الجماعية. 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 أدوات مختلفة، بناءً على نظام إدارة قواعد البيانات الذي تخطط لاستخدامه.

لأسباب أمنية، يُرجى عدم تعيين الحالة المميزة لحساب يعمل خادم الإدارة بموجبه.

إذا قررت لاحقًا تغيير حساب خادم الإدارة، يمكنك استخدام الأداة الإضافية الخاصة بتبديل حساب خادم الإدارة (klsvswch).

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 KIScSvc 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.

سيُتبع 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 لتنصيب التطبيقات عن بُعد (يتم نسخ الملفات إلى خادم الإدارة أثناء إنشاء حزم التنصيب).
 - تخزين التحديثات التي تم تنزيلها من مصدر محدث إلى خادم الإدارة.
- سيتم تمكين مشاركة الملفات (للقرءاء 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 للتنصيب أو دليلًا 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 Share محلي في مجلد التطبيق يحتوي على مكونات Kaspersky Security Center.

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 مأخذ التوصيل الأمانة (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).

إذا تم تثبيت خادم الإدارة على جهاز يقوم بتشغيل Microsoft Windows XP Service Pack 2، فسيقوم جدار حماية النظام المضمن بحظر منافذ TCP 13000 و 14000. لذلك، للسماح بالوصول إلى خادم الإدارة على الجهاز بعد التثبيت، يجب فتح هذه المنافذ يدويًا.

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 الخاص بالاتصال بالأجهزة المحمولة

تتوفر هذه الخطوة من معالج الإعداد إذا قمت بتحديد إدارة الجهاز المحمول للتثبيت.

في نافذة عنوان الاتصال بالأجهزة 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 14 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 14 Web Console، يمكنك القيام بـ [الإعداد الأولي للتطبيق](#).

تثبيت خادم الإدارة في الوضع غير التفاعلي

يمكن تثبيت خادم الإدارة في الوضع غير التفاعلي، أي، بدون إدخال تفاعلي لإعدادات التثبيت.

لتثبيت خادم الإدارة على جهاز محلي في الوضع غير التفاعلي:

1. أقرأ [اتفاقية ترخيص المستخدم النهائي](#). استخدم الأمر أدناه فقط إذا فهمت ووافقت على شروط اتفاقية ترخيص المستخدم النهائي.

2. أقرأ [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.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters
```

حيث إن setup_parameters هو قائمة معلمات وقيمها الخاصة المفصولة بمسافات (PARAM1=PARAM1VAL PARAM2=PARAM2VAL). يوجد الملف setup.exe في مجلد الخادم، والذي يُعد جزءًا من مجموعة توزيع Kaspersky Security Center.

يتم إدراج الأسماء والقيم المحتملة للمعلمات التي يمكن استخدامها عند تثبيت خادم الإدارة في الوضع غير التفاعلي في الجدول أدناه.

معلومات تثبيت خادم الإدارة في الوضع غير التفاعلي

اسم المعلمة	وصف المعلمة	القيم المتوفرة
EULA	الموافقة على شروط اتفاقية الترخيص.	<ul style="list-style-type: none">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.	<ul style="list-style-type: none">1- أدرك أنه سيتم التعامل مع بياناتي ونقلها (بما يشمل نقل البيانات إلى دول ثالثة) وفقًا لما ورد في سياسة الخصوصية وأوافق على ذلك. أوكد على أنني 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.	<ul style="list-style-type: none">قياسي-تثبيت قياسي.مخصص-تثبيت مخصص.

قيمة السلسلة.	مسار إلى مجلد تثبيت خادم الإدارة.	INSTALLDIR
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	قائمة بمكونات خادم الإدارة (مفصولة بفاصلة) المراد تثبيتها.	ADDLOCAL
• NRT_1_100—من 1 إلى 100 جهاز. • NRT_100_1000—من 101 إلى 1,000 جهاز. • NRT_GREATER_1000—أكثر من 1000 جهاز.	حجم الشبكة (عدد الأجهزة الموجودة على الشبكة).	NETRANGETYPE
• SrvAccountDefault—تم إنشاء الحساب تلقائيًا. • SrvAccountUser—تم تحديد الحساب يدويًا. في هذه الحالة، يجب عليك تحديد قيم لمعاملات SERVERACCOUNTNAME وSERVERACCOUNTPWD	وضع تحديد حساب الذي سيتم تشغيل خادم الإدارة كخدمة من خلاله.	SRV_ACCOUNT_TYPE
قيمة السلسلة.	اسم الحساب الذي سيتم تشغيل خادم الإدارة تحته كخدمة. يجب عليك تحديد قيمة للمعلمة في حالة .SRV_ACCOUNT_TYPE=SrvAccountUser	SERVERACCOUNTNAME
قيمة السلسلة.	كلمة مرور الحساب الذي سيتم استخدامه لبدء خادم الإدارة كخدمة. يجب عليك تحديد قيمة للمعلمة في حالة .SRV_ACCOUNT_TYPE=SrvAccountUser	SERVERACCOUNTPWD
• 1—حجم المفتاح لشهادة خادم الإدارة هو 2048 بت. • بدون قيمة—حجم المفتاح لشهادة خادم الإدارة هو 1024 بت.	حجم المفتاح لشهادة خادم الإدارة (بوحدة البت).	SERVERCER
• MySQL—سيتم استخدام قاعدة بيانات MySQL أو MariaDB؛ في هذه الحالة، يجب تحديد قيم لمعاملات MYSQLSERVERNAME وMYSQLSERVERPORT وMYSQLDBNAME	نوع قاعدة البيانات التي سيتم استخدامها لتخزين قاعدة بيانات خادم الإدارة. هذه المعلمة إلزامية.	DBTYPE

MYSQLACCOUNTNAME و .MYSQLACCOUNTPWD و		
<ul style="list-style-type: none"> • MSSQL—سيتم استخدام قاعدة بيانات A Microsoft SQL Server (SQL Express). في هذه الحالة، يجب عليك تحديد قيم لمعاملات MSSQLSERVERNAME و MSSQLDBNAME و MSSQLAUTHTYPE و 		
قيمة السلسلة.	الاسم الكامل لخادم SQL Server. يجب عليك تحديد قيمة للمعلمة في حالة DBTYPE=MySQL.	MYSQLSERVERNAME
قيمة رقمية.	عدد المنافذ للاتصال بخادم SQL Server. يجب عليك تحديد قيمة للمعلمة في حالة DBTYPE=MySQL.	MYSQLSERVERPORT
قيمة السلسلة.	نوع قاعدة البيانات التي سيتم إنشاؤها لتخزين بيانات خادم الإدارة. يجب عليك تحديد قيمة للمعلمة في حالة DBTYPE=MySQL.	MYSQLDBNAME
قيمة السلسلة.	اسم الحساب الخاص بالاتصال بقاعدة البيانات. يجب عليك تحديد قيمة للمعلمة في حالة DBTYPE=MySQL.	MYSQLACCOUNTNAME
قيمة السلسلة.	كلمة مرور الحساب للاتصال بقاعدة البيانات. يجب عليك تحديد قيمة للمعلمة في حالة DBTYPE=MySQL.	MYSQLACCOUNTPWD
قيمة السلسلة.	الاسم الكامل لخادم SQL Server. يجب عليك تحديد قيمة للمعلمة إذا كانت DBTYPE=MySQL.	MSSQLSERVERNAME
قيمة السلسلة.	اسم قاعدة البيانات. يجب عليك تحديد قيمة للمعلمة إذا كانت DBTYPE=MySQL.	MSSQLDBNAME
<ul style="list-style-type: none"> • Windows—وضع مصادقة Microsoft Windows. • SQL Server—وضع مصادقة خادم SQL Server. في هذه الحالة، يجب عليك تحديد قيم لمعاملات MSSQLACCOUNTNAME و MSSQLACCOUNTPWD و 	نوع التحويل عند الاتصال بخادم SQL Server. يجب عليك تحديد قيمة للمعلمة في حالة DBTYPE=MSSQL	MSSQLAUTHTYPE
قيمة السلسلة.	اسم الحساب للاتصال بخادم SQL Server. يجب عليك تحديد قيمة للمعلمة إذا كانت DBTYPE=MySQL.	MSSQLACCOUNTNAME
قيمة السلسلة.	كلمة مرور الحساب للاتصال بخادم SQL Server. يجب عليك تحديد قيمة للمعلمة إذا كانت DBTYPE=MySQL.	MSSQLACCOUNTPWD
<ul style="list-style-type: none"> • إنشاء—إنشاء مجلد مشترك جديد. في هذه الحالة، يجب عليك تحديد قيم لمعاملات SHARELOCALPATH و SHAREFOLDERNAME و • ChooseExisting—حدد مجلد موجود. في هذه الحالة، يجب عليك تحديد قيم لمعلمة EXISTSHAREFOLDERNAME 	طريقة تحديد المجلد المشترك.	CREATE_SHARE_TYPE

قيمة السلسلة.	المسار الكامل إلى مجلد محلي. يجب عليك تحديد قيمة للمعلمة في حالة CREATE_SHARE_TYPE=Create	SHARELOCALPATH
قيمة السلسلة.	اسم الشبكة لمجلد مشترك. يجب عليك تحديد قيمة للمعلمة إذا كانت CREATE_SHARE_TYPE=Create.	SHAREFOLDERNAME
قيمة السلسلة.	المسار الكامل لمجلد مشترك موجود. يجب عليك تحديد قيمة للمعلمة في حالة CREATE_SHARE_TYPE=ChooseExisting	EXISTSHAREFOLDERNAME
قيمة رقمية.	رقم المنفذ الخاص بالاتصال بخادم الإدارة.	SERVERPORT
قيمة رقمية.	عدد المنافذ لاتصال مشفر لخادم الإدارة باستخدام بروتوكول SSL.	SERVERSSLPORT
قيمة السلسلة.	عنوان خادم الإدارة.	SERVERADDRESS
قيمة السلسلة.	عنوان خادم الإدارة الخاص بالاتصال بالأجهزة المحمولة.	MOBILESERVERADDRESS

للحصول على وصف مفصل لمعاملات 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 14** لتشغيل معالج إعداد وحدة تحكم الإدارة. اتبع إرشادات المعالج.
3. حدد المجلد الوجهة بشكل افتراضي، سيكون هذا المجلد هو <Program Files\Kaspersky Lab\Kaspersky Security Center> Drive:\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:

1. اقرأ [اتفاقية ترخيص المستخدم النهائي](#). استخدم الأمر أدناه فقط إذا فهمت ووافقت على شروط اتفاقية ترخيص المستخدم النهائي.
2. في المجلد Distrib\Console لمجموعة توزيع Kaspersky Security Center، قم بتشغيل ملف setup.exe باستخدام الأمر التالي:
"setup.exe /s /v"EULA=1
إذا كنت ترغب في تثبيت كافة مكونات الإدارة الإضافية من مجلد Distrib\Console\Plugins مع وحدة تحكم الإدارة، فقم بتشغيل الأمر التالي:
setup.exe /s /v"EULA=1" /pALL
إذا كنت تريد تحديد مكونات الإدارة الإضافية التي تريد تثبيتها من مجلد Distrib\Console\Plugins مع وحدة تحكم الإدارة، فحدد المكونات الإضافية بعد المفتاح "/p" وافصل بينها بفاصلة منقوطة:
setup.exe /s /v"EULA=1" /pP1;P2;P3

حيث إن P1 و P2 و P3 هي أسماء المكونات الإضافية التي تتوافق مع أسماء مجلد المكونات الإضافية في مجلد Distrib\Console\Plugins. فمثلاً:

```
setup.exe /s /v"EULA=1" /pKES4Mac;KES5;MDM4IOS
```

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 و عميل الشبكة

يتم تثبيت خادم الإدارة و عميل الشبكة على الجهاز كخدمات تتضمن الخصائص المسردة أدناه. يحتوي الجدول أيضاً على سمات الخدمات الأخرى التي تنطبق على الجهاز بعد تثبيت خادم الإدارة.

Kaspersky Security Center خصائص خدمات

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 -AK-KL * أثناء التثبيت
عميل الشبكة	klagent	عميل شبكة Kaspersky Security Center	النظام المحلي
خادم ويب للوصول إلى Kaspersky Security Center 14 Web Console وإدارة الإنترنت في المؤسسة	klwebserv	خادم ويب Kaspersky	حساب KIScSvc مخصص وغير مميز
خادم وكيل التنشيط	klactprx	خادم وكيل تنشيط Kaspersky	حساب KIScSvc مخصص وغير مميز
خادم وكيل KSN	ksnproxy	خادم وكيل Kaspersky Security Network	حساب KIScSvc مخصص وغير مميز

خدمات Kaspersky Security Center 14 Web Console

إذا قمت بتثبيت Kaspersky Security Center 14 Web Console على الجهاز، فسيتم نشر الخدمات التالية (انظر الجدول أدناه):

الحساب	اسم الخدمة المعروض
حساب KIScSvc مخصص وغير مميز	Kaspersky Security Center Web Console
خدمة الشبكة	Kaspersky Security Center Web Console
حساب KIScSvc مخصص وغير مميز	خدمة المكون الإضافي لـ Kaspersky Security Center
النظام المحلي	خدمة Kaspersky Security Center Web Console
حساب KIScSvc مخصص وغير مميز	قائمة انتظار رسائل Kaspersky Security Center Web Console

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 نظراً 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 مثبت عليه خادم إدارة بالفعل.

يمكنك عرض خصائص كل خدمة لخادم الإدارة و عميل الشبكة، بالإضافة إلى مراقبة تشغيلهما باستخدام أدوات إدارة Microsoft Windows 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 الأمر، يمكنك تعديل حساب خدمة خادم الإدارة باستخدام الأداة المساعدة klsrvswch.

حسابات المستخدمين ومجموعات المستخدمين

يقوم مثبت خادم الإدارة بإنشاء الحسابات التالية بشكل افتراضي:

- KL-AK-*: حساب خدمة خادم إدارة
- KIScSvc: حساب للخدمات الأخرى من مجموعة خادم الإدارة
- KIPxeUser: حساب لنشر أنظمة التشغيل

إذا حددت حسابات أخرى لخدمة خادم الإدارة والخدمات الأخرى أثناء تشغيل المثبت، فيتم استخدام الحسابات المحددة.

سيتم أيضًا إنشاء مجموعات أمان محلية مزودة بمجموعة من الحقوق لكل منهم بشكل تلقائي على الجهاز المثبت 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 المثبت. في هذه الحالة، يقوم المثبت تلقائيًا بإنشاء مجموعات أمان المجال باسم KLOperators و KLAdmins. إذا قمت بتثبيت خادم الإدارة على جهاز كمبيوتر لا يمثل وحدة تحكم المجال، يجب أن تبدأ بحقوق المسؤول المحلي على المثبت بدلاً من ذلك. في هذه الحالة، يقوم المثبت تلقائيًا بإنشاء مجموعات أمان محلية باسم KLOperators و KLAdmins.

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 (Share) أثناء تشغيل المعالج، فيمكنك حذفه يدويًا بعد إكمال جميع المهام ذات الصلة.

بعد إزالة التطبيق، قد تظل بعض ملفاته في المجلد المؤقت للنظام.

سيقوم معالج إزالة التطبيق باقتراح قيامك بتخزين نسخة احتياطية من خادم الإدارة.

وعند إزالة التطبيق من Microsoft Windows 7 و Microsoft Windows 2008، قد يحدث إنهاء مبكر لمعالج الإزالة. 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 [عقد مجموعة تجاوز الفشل من Kaspersky](#).

أثناء الترقية، يُحظر تمامًا الاستخدام المتزامن لنظام إدارة قواعد البيانات بواسطة خادم الإدارة وتطبيق آخر.

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 لكل من وحدة تحكم الإدارة وبرنامج Kaspersky Security Center 14 Web Console).

ترقية Kaspersky Security Center من إصدار سابق

يمكنك تثبيت الإصدار 14 من خادم الإدارة على جهاز مثبت عليه إصدار قديم من خادم الإدارة (بدءًا من الإصدار 10 Service Pack 1). عند الترقية إلى الإصدار 14، 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، يمكنك أيضًا [ترقية Kaspersky Security Center](#) على العقد الخاصة به.

1. قم بتشغيل ملف التثبيت ksc_14_<build number>_full_<language>.exe لإصدار 14 (يمكنك تنزيل هذا الملف من موقع ويب Kaspersky).
2. في النافذة التي يتم فتحها، انقر فوق رابط تثبيت Kaspersky Security Center 14 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. يُطلبك 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 لخادم الإدارة لخاصة لبيانات خادم الإدارة التي يتم فتحها. يتم إنشاء نسخة احتياطية عن طريق الأداة المساعدة kllbackup. يتم تضمين هذه الأداة المساعدة في مجموعة التوزيع، الموجودة في جذر مجلد **تثبيت Kaspersky Security Center**.
5. قم بتثبيت إصدار خادم الإدارة 14 من خلال اتباع معالج الإعداد.
- إذا ظهرت رسالة تفيد بأن خدمة Kaspersky Security Center 14 Web Console مشغولة، فانقر على زر **تجاهل** في نافذة المعالج.

ننصحك بتجنب إنهاء معالج الإعداد. إذا قمت بالغاء 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. بعد إتمام مهمة التثبيت عن بُعد، سيتم ترقية إصدار عميل الشبكة.

ترقية Kaspersky Security Center على عقد نظام مجموعة تجاوز الفشل من Kaspersky

يمكنك تثبيت الإصدار 14 من خادم الإدارة على كل عقدة لمجموعة تجاوز الفشل من Kaspersky حيث يتم تثبيت خادم الإدارة بإصدار سابق (بدءًا من الإصدار 13.2). عند الترقية إلى الإصدار 14، 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:

1. أوقف المجموعة.

2. قم بتنفيذ الإجراءات التالية على العقدة النشطة للمجموعة:

a. تشغيل الملف التنفيذي ksc_14_<build number>_full_<language>.exe

يتم فتح نافذة تُطلبك بتحديد تطبيقات Kaspersky التي ستتم ترقيتها. في نافذة تحديد التطبيق، انقر فوق رابط تثبيت خادم إدارة Kaspersky Security Center 14 لبدء معالج إعداد خادم الإدارة. اتبع إرشادات 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

سيستمر تثبيت التطبيق على جهازك بعد تحديد كلاً من خانتي الاختيار.

إذا كنت لا تقبل اتفاقية الترخيص أو سياسة الخصوصية، فانقر فوق الزر **إلغاء** لإلغاء الترقية.

c. في نافذة **نوع التثبيت على نظام المجموعة**، حدد العقدة التي تقوم بالترقية عليها.

بعد ذلك، يقوم برنامج التثبيت بتكوين وإنهاء ترقية خادم الإدارة. أثناء الترقية، لا يمكنك تغيير إعدادات خادم الإدارة التي تم تعديلها قبل الترقية.

3. نفذ نفس الإجراءات على العقدة الخاملة لمجموعة تجاوز الفشل من Kaspersky كما هو الحال في العقدة النشطة. إذا اخترت خيار **المجموعة (التثبيت على جميع عقد المجموعة)** في نافذة **نوع التثبيت على نظام المجموعة**، فلن تحتاج إلى تشغيل برنامج التثبيت وتنفيذ الخطوة الحالية.

4. ابدأ المجموعة.

نتيجة لذلك، قمت بتثبيت أحدث إصدار لخادم الإدارة على عقد مجموعة تجاوز الفشل من Kaspersky.

الإعداد الأولي لـ Kaspersky Security Center

يُرد في هذا القسم الخطوات التي يجب عليك اتخاذها بعد تثبيت Kaspersky Security Center.

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 لتطبيقات Kaspersky المُدارة. بعد الانتهاء من معالج البدء السريع، يتم عرض حزم تثبيت عميل الشبكة الخاص بنظام التشغيل Windows وتطبيقات Kaspersky المُدارة في قائمة **خادم الإدارة** ← **الإعدادات المتقدمة** ← **التثبيت عن بُعد** ← **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 بـ **مفاتيح** الخاص بـ **خادم الإدارة**.

• قم بتكوين التفاعل مع **(KSN) Kaspersky Security Network** [\[9\]](#).

• 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 بـ **مفاتيح** الخاص بـ **خادم الإدارة**.

• ضبط إعدادات التحديث وإعدادات إصلاح الثغرات الأمنية للتطبيقات المثبتة على الأجهزة.

• إنشاء سياسة حماية لمحطات العمل والخوادم ومهام فحص الفيروسات ومهام تنزيل التحديثات ومهام النسخ الاحتياطي للبيانات لأعلى مستوى بالتسلسل الهرمي للأجهزة المُدارة. 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**.

سيطلبك **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** [\[9\]](#)

عنوان الخادم الوكيل المستخدم لاتصال **Kaspersky Security Center** بالإنترنت.

• **رقم المنفذ** [\[9\]](#)

رقم المنفذ الذي سيتم من خلاله إنشاء اتصال وكيل **Kaspersky Security Center**.

• تجاوز الخادم الوكيل للعناوين المحلية 5

لن يتم استخدام خادم وكيل للاتصال بالأجهزة في الشبكة المحلية.

• مصادقة الخادم الوكيل 5

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 5

حساب المستخدم الذي تم من خلاله إنشاء اتصال بالخادم الوكيل (يكون هذا الحقل متاحًا في حالة تحديد خانة اختيار مصادقة الخادم الوكيل).

• كلمة المرور 5

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.

الخطوة 2. تحديد طريقة تفعيل التطبيق

حدد أحد خيارات تفعيل Kaspersky Security Center التالية:

• عن طريق إدخال رمز التنشيط الخاص بك 5

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. لتنشيط التطبيق باستخدام رمز التنشيط، ستحتاج إلى الوصول إلى الإنترنت لإنشاء اتصال مع خوادم تنشيط Kaspersky. إذا قمت بتحديد خيار التنشيط هذا، فيمكنك تمكين خيار مفتاح ترخيص النشر التلقائي للأجهزة المُدارة. 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 5

ملف المفتاح هو ملف بامتداد key. مقدم لك من Kaspersky. الهدف من ملف المفتاح هو إضافة مفتاح لتنشيط التطبيق. تتلقى ملفك الرئيسي عبر عنوان البريد الإلكتروني الذي حددته بعد شراء Kaspersky Security Center. لتنشيط التطبيق باستخدام ملف المفتاح، لا تحتاج إلى الاتصال بخوادم تنشيط Kaspersky. إذا قمت بتحديد خيار التنشيط هذا، فيمكنك تمكين خيار مفتاح ترخيص النشر التلقائي للأجهزة المُدارة. 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.

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 والمنصات

حدد مناطق الحماية والمنصات 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 ومخزن الملفات.** 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.
- **الظاهرية.** 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.

• [أنظمة التشغيل](#)

يمكنك تحديد المنصات التالية:

- Microsoft Windows
- Linux
- macOS
- Android

بعد تحديد مناطق الحماية والمنصات، تبدأ مكونات الإدارة الإضافية وحزم التوزيع لتطبيقات Kaspersky في التنزيل تلقائيًا.

الخطوة 4. تحديد المكونات الإضافية للتطبيقات المُدارة

حدد المكونات الإضافية للتطبيقات المُدارة لتثبيتها. تُعرض 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 ٤

يتم تحديد المكونات الإضافية المعتمدة على المكونات والمنصات، التي حددتها في الخطوة السابقة.

• إصدار التطبيق ٥

تتضمن القائمة مكونات إضافية لجميع الإصدارات الموجودة على خوادم Kaspersky. حسب الإعدادات الافتراضية، يتم تحديد المكونات الإضافية لأحدث الإصدارات.

• لغة التعريب ٥

حسب الإعدادات الافتراضية، تُعرّف 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 المنسدة**.

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، أعلق نافذة التثبيت.

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. يستخدم هذا النوع من التشفير طول مفتاح 256 بت.
- تشفير لايت. 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 .

تحديثات 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**، يُعرض 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، تُعرض الحالة تم إنشاء حزمة التثبيت. ستستخدم فيما بعد حزم التثبيت لنشر تطبيقات Kaspersky على أجهزة العملاء.

إذا كنت تفضل عدم تشغيل المعالج، فيمكنك إنشاء حزم التثبيت يدويًا من خلال الانتقال إلى خادم الإدارة خادم الإدارة ← إعدادات متقدمة ← التثبيت عن بُعد ← حزم التثبيت لشجرة وحدة تحكم الإدارة.

الخطوة 6. تكوين استخدام Kaspersky Security Network

اقرأ بيان Kaspersky Security Network (KSN) المعروف في النافذة. 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 العملية 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.

إذا قمت بتنزيل المكون الإضافي لـ Kaspersky Endpoint Security for Windows، فسيتم عرض عباراتي KSN على حد سواء—عبارة KSN لـ Kaspersky Security Center وعبارة KSN لـ Kaspersky Endpoint Security for Windows. يتم عرض عبارات KSN لتطبيقات Kaspersky الأخرى المدارة، التي تم تنزيل مكوناتها الإضافية، في نوافذ منفصلة ويتعين عليك قبول (أو عدم قبول) كل عبارة على حدة.

الخطوة 7. تكوين إشعارات البريد الإلكتروني

كُون إرسال الإشعارات حول الأحداث المسجلة أثناء تشغيل تطبيقات Kaspersky على الأجهزة المدارة. 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.

رقم منفذ الاتصال الخاص بخادم SMTP. رقم المنفذ الافتراضي هو 25.

تمكين دعم مصادقة ESMTP. عند تحديد خانة الاختيار الموجودة في الحقول اسم المستخدم وكلمة المرور، يمكنك تحديد إعدادات مصادقة ESMTP. بشكل افتراضي، يتم إلغاء تحديد هذه الخانة، وتكون إعدادات مصادقة ESMTP غير متوفرة.

حدد إعدادات TLS لخادم SMTP:

• اسم الموضوع (اسم موضوع رسالة البريد الإلكتروني)

• 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، 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 للوصول إلى 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 نظام SIEM موقعة أيضًا من جانب جهات إصدار موثوقة أم لا. لا يمكن لـ Kaspersky Security Center الاتصال بخادم نظام SIEM إذا لم يتم استلام شهادة خادم نظام SIEM من جهات 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.

○ حاوية pkcs12:

يجب تحميل ملف واحد يحتوي على الشهادة ومفتاحها الخاص. عند تحميل الملف، يجب عليك 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.

الخطوة 8. تكوين إدارة 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](#) 9

تم إنشاء المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. ويتم تحديد هذا الخيار بصورة افتراضية.

• [بحث عن التحديثات المطلوبة وتثبيتها](#) 9

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 طريقة مزامنة التحديث:

• [استخدام مصادر التحديث المحددة في سياسة المجال](#) 9

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](#) 9

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.

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 تطبيقات Kaspersky المُدارة
- 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. سيطلبك التطبيق بإضافة الموردين الذين تم التحقق منهم بواسطة Kaspersky في المنطقة الموثوقة لأغراض استثناء تطبيقاتهم من عمليات الفحص لمنع حجبتها عن طريق الخطأ. يمكنك الآن إنشاء الاستثناءات الموصى بها أو إنشاء قائمة استثناءات لاحقاً 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 فوق موافق.

انقر فوق التالي. يتوفر هذا الزر بعد إنشاء جميع السياسات والمهام الضرورية.

الخطوة 10. توصيل الأجهزة المحمولة

إذا حددت مسبقاً 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 تلقائياً 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 افتراضياً.

• منفذ لمزامنة الأجهزة المحمولة ④

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 ④

منفذ اتصال Kaspersky Endpoint Security for Android بخوادم تنشيط Kaspersky. رقم المنفذ الافتراضي هو 17100.

• فتح منفذ لأجهزة حماية جهاز UEFI وأجهزة KasperskyOS ④

يمكن لأجهزة حماية UEFI الاتصال بخادم الإدارة.

• منفذ لأجهزة حماية UEFI وأجهزة KasperskyOS ④

يمكنك تغيير رقم المنفذ إذا تم تمكين الخيار فتح منفذ لأجهزة حماية جهاز UEFI وأجهزة KasperskyOS. رقم المنفذ الافتراضي هو 13294.

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 إنشاؤها 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 ④

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 #8 PKCS ((*.prk).

■ **المفتاح العام (.cer).** في هذا الحقل، انقر فوق زر استعراض لتحديد مفتاح عام بتنسيق (*.cer). (PEM).

- **الحاوية #12 PKCS.** 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 الجديدة 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 **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 ④

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 ④

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 وتشغيلها 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 ④

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 ④

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 ④

استخدام شهادة صادرة بواسطة مصدر شهادة خارجي – مركز الشهادات – باستخدام القالب الافتراضي.
يتم تحديد هذا الخيار افتراضيًا.

• قالب آخر ④

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) ٥

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 ٥

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 المُمكن. 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 حدده. 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 أجريتها.

لتمكنك 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 و iOS إلى المجموعة **الأجهزة المُدارة**:

• باستخدام أنظمة تشغيل Android المثبت 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 أخرى.

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.

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.

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 فوق الزر **إنهاء**.

تكوين اتصال وحدة تحكم الإدارة بخادم الإدارة

في الإصدارات السابقة من Kaspersky Security Center، كان يتم توصيل وحدة تحكم الإدارة بخادم الإدارة عبر منفذ SSL TCP 13291 ومنفذ SSL 13000. وابتداءً من الحزمة Kaspersky Security Center 10 Service Pack 2، يتم استخدام منافذ SSL بواسطة التطبيق بصورة منفصلة تمامًا وأصبح من المستحيل إساءة استعمال المنافذ:

• لا يمكن استخدام منفذ SSL TCP 13291 إلا بواسطة وحدة تحكم الإدارة وكائنات التشغيل التلقائي لـ klakaut

• لا يمكن استخدام منفذ SSL TCP 13000 إلا بواسطة عميل الشبكة وخادم الإدارة الثانوي وخادم الإدارة الرئيسي في منطقة DMZ.

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 العملية.

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 (تلقّي بيانات من الأجهزة العملية 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 DMZ.

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:

• لنظام 64 بت:

LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\core\independent\KLLIM

• لنظام 32 بت:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM

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.

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 الموصولة 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 الموصولة 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.

بشكل افتراضي، يوجد ملف التثبيت في: `<server name>\KLSHARE\PkgInst\NetAgent_<version number>`

في نافذة بوابة الاتصال لمعالج 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 فعلياً ببوابة الاتصال في منطقة الأجهزة الموصولة مباشرة بالإنترنت، اسمح بالاتصالات بمنفذ TCP 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 أجهزة الكمبيوتر المكتبية الخارجية بخادم الإدارة

في العادة، لا يتم نقل أجهزة الكمبيوتر المكتبية الخارجية داخل المحيط. لذلك أنت بحاجة إلى تكوينها للاتصال بخادم الإدارة من خلال البوابة عند تثبيت عميل الشبكة.

7 قم بإعداد تحديثات أجهزة الكمبيوتر المكتبية الخارجية

إذا تم تكوين تحديثات تطبيقات الأمان بحيث يتم تنزيلها من خادم الإدارة، فستقوم أجهزة الكمبيوتر 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 أجهزة الكمبيوتر الخارجية التحديثات من خوادم Kaspersky.

قم بما يلي:

1. انقل جميع أجهزة الكمبيوتر الخارجية إلى مجموعة الإدارة المنفصلة التي قمت بإنشائها مسبقًا.

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.

حول توصيل الأجهزة خارج المكتب

دائمًا ما تقع بعض الأجهزة المدارة خارج نطاق الشبكة الرئيسية (على سبيل المثال، أجهزة الكمبيوتر في الفروع الإقليمية للشركة؛ الأكوام وأجهزة الصراف الآلي والمحطات الطرفية المثبتة في نقاط البيع المختلفة؛ أجهزة الكمبيوتر 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 الموصولة 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 الموصولة مباشرة بالإنترنت
- اطلع على نظام حركة مرور البيانات: خادم الإدارة في منطقة الأجهزة الموصولة مباشرة بالإنترنت والأجهزة المدارة على الإنترنت

بوابة اتصال في منطقة الأجهزة الموصولة مباشرة بالإنترنت

الطريقة الموصى بها لتوصيل الأجهزة الموجودة خارج المكتب بخادم الإدارة هي تنظيم منطقة الأجهزة الموصولة مباشرة بالإنترنت في شبكة المؤسسة وتثبيت بوابة اتصال فيها. ستتصل الأجهزة الخارجية ببوابة الاتصال، وسيبدأ خادم الإدارة الموجود بداخل الشبكة بالاتصال 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 فعلياً ولا تنشئ أي اتصالات.

ولا تتطلب بوابة الاتصال أيضاً توفر العديد من موارد الأجهزة.

ومع ذلك، فإن هذه الطريقة بها عملية تكوين أكثر تعقيداً:

- لجعل جهاز يعمل كبوابة اتصال في منطقة الأجهزة الموصولة 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 أيضاً استخدام وضع اتصال مختلف: من خلال بوابة الاتصال.
- كما يتطلب منك تحديد إعدادات اتصال مختلفة لأجهزة الكمبيوتر المحمولة في مواقع مختلفة.

خادم الإدارة في منطقة الأجهزة الموصولة مباشرة بالإنترنت

هناك طريقة أخرى وهي تثبيت خادم إدارة واحد في منطقة الأجهزة الموصولة مباشرة بالإنترنت.

هذا التكوين أقل أماناً 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، ولكن من منطقة الأجهزة الموصولة 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 الموصولة 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 معتاداً 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 100000 جهاز، بينما يمكن لبوابة الاتصال أن تدعم ما يصل إلى 10000 جهاز.

لهذا الحل أيضاً 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 الموصولة مباشرة بالإنترنت)، مما يعقد المراقبة.
- لإدارة جميع الأجهزة، يجب ضم خادم الإدارة في شكل تسلسل هرمي، مما يعقد المراقبة وكذلك الإدارة. يفرض مثل خادم الإدارة الثانوي قيوداً على الهياكل المحتملة لمجموعات الإدارة. عليك أن تقرر طريقة وماهية المهام والسياسات لتوزيعها على مثل خادم الإدارة الثانوي.

- يعد تكوين الأجهزة الخارجية لاستخدام خادم الإدارة في منطقة الأجهزة الموصولة مباشرة بالإنترنت من الخارج واستخدام خادم الإدارة الرئيسي من الداخل معقدًا أكثر من مجرد تكوينها لاستخدام اتصال مشروط من خلال بوابة.
- مخاطر أمنية عالية. يُعرض مثل 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 أجهزة الكمبيوتر المكتبية الخارجية بخادم الإدارة

لا يمكن توصيل أجهزة الكمبيوتر المكتبية التي دائمًا ما تكون خارج الشبكة الرئيسية (على سبيل المثال، أجهزة الكمبيوتر في الفروع الإقليمية للشركة؛ الأكشاك وأجهزة الصراف الآلي والمحطات الطرفية المثبتة في نقاط البيع المختلفة؛ أجهزة الكمبيوتر في المكاتب المنزلية للموظفين) بخادم الإدارة مباشرة. يجب أن تكون متصلة بخادم الإدارة عبر بوابة اتصال مثبتة في منطقة الأجهزة الموصولة مباشرة بالإنترنت (DMZ). يتم إجراء هذا التكوين عند تثبيت عميل الشبكة على تلك الأجهزة.

لتوصيل أجهزة الكمبيوتر 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 لأجهزة الكمبيوتر المستهدفة إما إلكترونياً أو على محرك أقراص قابل للإزالة.

6. قم بتثبيت عميل الشبكة من الحزمة المستقلة.

أجهزة الكمبيوتر 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

يتم تطبيق الإجراء التالي فقط على 1 Kaspersky Security Center Service Pack والأحدث.

الأجهزة المثبت عليها عميل الشبكة يمكنها الاتصال بخادم الإدارة إما من إنترنت 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 DMZ](#))، فيجب عليك تحديد عنوان بوابة الاتصال في الحقل المقابل لملف تعريف الاتصال.

التبديل بين خوادم الإدارة بناءً على الشبكة الحالية

يتم تطبيق الإجراء التالي فقط على Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 وعلى أي إصدارات أحدث.

إذا كان للمؤسسة مكاتب متعددة بها خوادم إدارة مختلفة وتنتقل بعض الأجهزة المثبت 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، ما عدا 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 بتعطيل 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. يكون 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 العملية 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 ذلك، 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 وكيل 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 اتصالاتك 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 للاتصال 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

يوفر Kaspersky Security Center خيار نقل عميل الشبكة على الجهاز العميل إلى خوادم الإدارة الأخرى في حالة تغيير إعدادات الشبكة التالية:

- 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 فقط)— تغيير حالة مجال Windows الذي يتصل به الجهاز العميل. هذا الإعداد متاح 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 الخاص بالشبكة. هذا الإعداد متاح 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 عميل 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 **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 و macOS.

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 النافذة خصائص التي تفتح، في القسم **الاتصال** حدد القسم الفرعي **ملفات تعريف الاتصال**.

4. في القسم **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 العملية إلى سياسات خارج المكتب. يتم استخدام ملف التعريف لتنزيل التحديثات فقط.

6. في القسم **تغيير 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 التغيير 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 (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 (فقط)**—تم تغيير عنوان IP الخاص بخادم WINS الخاص بالشبكة. 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 عميل الشبكة من شهادة الخادم بالإضافة إلى التحقق من إمكانية اتصال SSL. إذا لم تتطابق الشهادة، فسيقشل الاتصال.

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 9

في هذا الحق، يمكنك إضافة قيمة واحدة أو أكثر للشرط الجاري إنشائه.

• مطابقة قيمة واحدة على الأقل من القيم الموجودة في القائمة 9

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 9

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 (↓).

تشفير الاتصال مع SSL/TLS

لإصلاح الثغرات الأمنية الموجودة في شبكة الشركة الخاصة بمؤسستك، يمكنك تمكين تشفير حركة المرور باستخدام SSL/TLS. يمكنك تمكين SSL/TLS على خادم الإدارة وخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM. Kaspersky Security Center يدعم الإصدار 3 وكذلك بروتوكول طبقة المقابس الآمنة (TLS الإصدار 1.0 و1.1 و1.2). يمكنك تحديد بروتوكول التشفير ومجموعات التشفير. يستخدم Kaspersky Security Center شهادات موقعة ذاتيًا. التكوين الإضافي لأجهزة iOS غير مطلوب. يمكنك أيضًا استخدام شهادتك 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. استخدم الأداة المساعدة klsclag لتكوين بروتوكولات التشفير ومجموعات التشفير المسموح بها على خادم الإدارة. أدخل الأمر التالي في موجه أوامر Windows، باستخدام حقوق المسؤول:

```
klsclag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <value> -t d
```

حدد الـ <value> معلمة الأمر:

• 0- تمكين جميع بروتوكولات التشفير ومجموعات التشفير

• 1- تعطيل SSL v2

مجموعات التشفير:

• AES256-GCM-SHA384

• AES256-SHA256

• AES256-SHA

• CAMELLIA256-SHA

• AES128-GCM-SHA256

• AES128-SHA256

• AES128-SHA

• SEED-SHA

• CAMELLIA128-SHA

• IDEA-CBC-SHA

• RC4-SHA

• RC4-MD5

• DES-CBC3-SHA

• تم تعطيل 2- SSL الإصدار 2 و SSL الإصدار 3 (القيمة الافتراضية)

مجموعات التشفير:

• AES256-GCM-SHA384

• AES256-SHA256

• AES256-SHA

• CAMELLIA256-SHA

• AES128-GCM-SHA256

• AES128-SHA256

• AES128-SHA

• SEED-SHA

• CAMELLIA128-SHA

• IDEA-CBC-SHA

• RC4-SHA

RC4-MD5 •

DES-CBC3-SHA •

• 3 – فقط TLS 1.2.

مجموعات التشفير:

AES256-GCM-SHA384 •

AES256-SHA256 •

AES256-SHA •

CAMELLIA256-SHA •

AES128-GCM-SHA256 •

AES128-SHA256 •

AES128-SHA •

CAMELLIA128-SHA •

2. أعد تشغيل خدمات Kaspersky Security Center 14 التالية:

• خادم الإدارة

• خادم الويب

• وكيل التفعيل

خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يتم تشفير الاتصال بين أجهزة iOS وخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM افتراضياً.

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: محلياً، باستخدام الأمر regedit بدء ← تشغيل القائمة).

2. انتقل إلى الخلية التالية:

• لنظام 64 بت:

\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset

• لنظام 32 بت:

OCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset

3. قم بإنشاء مفتاح بالاسم StrictSslSettings.

4. حدد DWORD كنوع المفتاح.

5. قم بتعيين قيمة المفتاح:

• 2 - تم تعطيل SSL الإصدار 3 (مسموح به TLS 1.0 و TLS 1.1 و TLS 1.2)

• 3 - فقط TLS 1.2 (القيمة الافتراضية)

6. أعد تشغيل خدمة خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM الخاص بـ Kaspersky Security Center 14.

إخطارات الأحداث

يوضح هذا القسم كيفية تحديد طريقة لتسليم إخطارات المسؤول حول الأحداث المتعلقة بالأجهزة العملية 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 العملية 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 معلومات أي حدث وقع.

لتكوين إخطار بالأحداث التي تحدث على أجهزة الكمبيوتر العملية:

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 التيوبيد 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 افتراضياً.

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 إعلانات 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 والتحقق 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 للاتصال 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.

■ حاوية 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 معلومات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة من خلال إضافة معلومات بديلة أخرى مع تفاصيل ذات صلة أكثر بالحدث. تتوفر قائمة بالمعلومات 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 9

تتيح لك علامة التبويب رسالة SMS تكوين إرسال إخطارات بمختلف الأحداث عبر رسالة SMS إلى هاتف محمول. سيتم إرسال رسائل SMS عبر بوابة البريد.

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، يمكنك 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، يمكنك 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 لفتح 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** لتحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مدار الفاصل الزمني المحدد.

يتيح لك النقر فوق الزر **إرسال رسالة اختبار** للتحقق 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 وقت 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 العملية.

يمكنك تجاوز إعدادات الإخطار لبعض الأحداث من القسم تكوين الحدث لإعدادات الإدارة، أو لإعدادات السياسة، أو لإعدادات التطبيق.

إخطارات الاختبار

للتحقق من إرسال إشعارات الحدث أم لا، يستخدم التطبيق إشعار الاختبار لاكتشاف فيروس EICAR في الأجهزة العملية.

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 العملية 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 العملية عبر تشغيل الملف التنفيذي. يجب أن يحتوي الملف التنفيذي على ملف تنفيذي آخر مع العناصر النائية للحدث ليتم ترحيله إلى المسؤول.

العناصر النائية لوصف حدث

عناصر نائب	وصف عنصر نائب
%الخطورة%	مستوى أهمية الحدث
%الكمبيوتر%	اسم الجهاز الذي وقع عليه الحدث
%المجال%	المجال
%الحدث%	الحدث
%DESCR%	وصف الحدث
%RISE_TIME%	الوقت الذي تم إنشاؤه

اسم المهمة	%KLCSAK_EVENT_TASK_DISPLAY_NAME%
عمليل شبكة Kaspersky Security Center	%KL_PRODUCT%
رقم إصدار عمليل الشبكة	%KL_VERSION%
عنوان IP	%HOST_IP%
عنوان IP للاتصال	%HOST_CONN_IP%

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 يشغل الملف script2.bat مع العنصر النائب %COMPUTER%. يتلقى المسؤول اسم الجهاز حيث وقع الحدث.

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 وعرض).

لتكوين واجهة Kaspersky Security Center وفقًا لمجموعة المزايا المستخدمة 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 خانة الاختيار التالية:

• 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.

• 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**

- **مراقب الثغرات**

- **التحكم في الجهاز**

- **التحكم في الويب**

إذا تم تعطيل هذا الخيار، فلن يتم عرض الأقسام الفرعية المحددة أعلاه في قسم **عناصر التحكم في الأمان**. يتم تمكين هذا الخيار افتراضياً.

- **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 افتراضياً.

- **عرض خوادم الإدارة الثانوية** 

إذا تم تحديد خانة الاختيار، فإن شجرة وحدة التحكم تعرض العقد 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 افتراضياً.

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 خانة 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. عند اكتشاف جميع الأجهزة المتصلة بالشبكة، يمكنك الحصول على معلومات حولها وإدارتها من خلال السياسات. هناك حاجة لاستطلاعات شبكة منتظمة لاكتشاف وجود أي أجهزة جديدة وما إذا كانت الأجهزة التي تم اكتشافها مسبقًا لا تزال موجودة على الشبكة.

يتم اكتشاف الأجهزة المتصلة بالشبكة على المراحل التالية:

1 اكتشاف الأجهزة الأولى

يوجهك معالج البداية السريعة خلال عملية اكتشاف الأجهزة الأولى، ويساعدك على العثور على الأجهزة المتصلة بالشبكة مثل أجهزة الكمبيوتر والأجهزة اللوحية والهواتف المحمولة. ويمكنك أيضًا إجراء اكتشاف الأجهزة يدويًا.

2 تكوين الاستقصاءات المستقبلية

حدد نوع (أنواع) الاكتشاف الذي تريد استخدامه بانتظام. تأكد من أن هذا النوع ممكن وأن جدول الاستقصاء يلبي احتياجات مؤسستك. عند تكوين جدول الاستقصاء، استخدم التوصيات لتكرار استقصاء الشبكة.

3 إعداد القواعد لإضافة الأجهزة المكتشفة إلى مجموعات الإدارة (اختياري)

إذا ظهرت أجهزة جديدة على شبكتك، سيتم اكتشافها أثناء الاستقصاءات المنتظمة وسيتم تضمينها تلقائيًا في المجموعة الأجهزة غير المخصصة. إذا أردت، يمكنك إعداد القواعد لنقل هذه الأجهزة تلقائيًا إلى المجموعة الأجهزة المُدارة. يمكنك أيضًا إنشاء قواعد الاستبقاء.

إذا تخطيت مرحلة إعداد هذه القاعدة، فستنقل جميع الأجهزة المكتشفة حديثًا إلى المجموعة الأجهزة غير المخصصة وستظل هناك. 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 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 في حالة عدم تكوين أي قواعد، تظل 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 137 و138 و139 TCP 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؛ خلافاً لذلك، فلن 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 افتراضياً. لا يوصى باستخدام هذا النوع من الاستقصاء إذا كنت تستخدم استقصاء شبكة Windows و/أو استقصاء Active Directory.

- **استطلاع شبكة لا تتطلب توكيماً.** تقوم نقطة توزيع باستقصاء شبكة IPv6 باستخدام شبكات التكوين الصفري (كما يشار إلى Zeroconf). يتم تعطيل نوع الاستقصاء هذا افتراضياً. يمكنك استخدام استقصاء شبكة لا تتطلب توكيماً إذا كانت نقطة التوزيع تعمل بنظام Linux.

إذا قمت بإعداد وتمكين قواعد نقل الأجهزة، فسيتم تضمين الأجهزة المكتشفة حديثاً تلقائياً في المجموعة الأجهزة المُدارة. في حالة عدم تمكين أي من قواعد النقل، فسيتم تضمين الأجهزة المكتشفة حديثاً تلقائياً 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 مجال Active Directory بالكامل أو فقط مجال محدد.

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 137/138 و139 و138 و139 و445 و445 و445 و445 TCP متاحة على الشبكة.
- 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**

الفترة 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 6:00:00 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 6:00:00 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**

الفترة 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. بشكل 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. بشكل افتراضي، يعمل الاستقصاء كل يوم جمعة الساعة 6:00:00 مساءً.

• **كل شهر في أيام معينة من الأسابيع المحددة**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد. بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 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؛ خلاًفاً 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.

عرض وتعديل إعدادات استقصاء Active Directory

1. في شجرة وحدة التحكم، في المجلد **اكتشاف الأجهزة**، حدد المجلد الفرعي **Active Directory**. بدلاً 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**

الفترة الافتراضية هي ساعة واحدة. يتم استبدال البيانات التي يتم تلقيها في الاستقصاء التالي بالبيانات القديمة بشكل كامل. تتوفر خيارات جدول الاستقصاء التالية:

• **كل N يوماً**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بداية من الوقت والتاريخ المحددين. بشكلٍ 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 6:00:00 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 6:00:00 مساءً.

• **تشغيل المهام الفائتة**

إذا كان خادم الإدارة مغلقاً أو غير متاح خلال الوقت الذي تمت جدولة الاستقصاء عليه، فيستطيع خادم الإدارة إما أن يبدأ الاستقصاء فوراً بعد تشغيله أو الانتظار للمرة المقبلة التي تمت جدولة الاستقصاء عليها. إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة في الاستقصاء فوراً بعد تشغيله. إذا تم تعطيل هذا الخيار، سينتظر خادم الإدارة للمرة المقبلة التي تمت جدولة الاستقصاء عليها. يتم تمكين هذا الخيار افتراضياً.

• **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، يمكنك 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 فوراً، 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 افتراضياً. لا يوصى باستخدام هذا النوع من الاستقصاء إذا كنت تستخدم استقصاء شبكة Windows و/أو استقصاء Active Directory.

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**.
- افتح 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. بشكل 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. بشكل افتراضي، يعمل الاستقصاء كل يوم جمعة الساعة 6:00:00 مساءً.

• **كل شهر في أيام معينة من الأسابيع المحددة**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد. بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 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 العملية 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 بعنوانين 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)** 9

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 (Windows فقط).

عند تعطيل جهاز ظاهري مؤقت، يقوم عميل الشبكة بإخطار خادم الإدارة بأن الجهاز قد تم تعطيله. إذا تم تعطيل جهاز ظاهري بنجاح، فنتم إزالته من قائمة الأجهزة المتصلة بخادم الإدارة. إذا تم تعطيل جهاز ظاهري مع وجود أخطاء ولم يرسل عميل الشبكة إخطار عن الجهاز الظاهري المُعطّل 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

لا يتوافر استخدام الوضع الديناميكي للبنية الأساسية لسطح المكتب الظاهري (VDI) إلا للأجهزة التي تعمل بنظام Windows.

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 تثبيته عميل الشبكة عليه جزءًا من VDI.

البحث عن الأجهزة التي تُعد جزءًا من VDI

للعثور على الأجهزة التي تُعد جزءًا من VDI:

1. حدد بحث من قائمة سياق المجلد الأجهزة غير المخصصة.
 2. في النافذة البحث عن أجهزة، في علامة التبويب الأجهزة الظاهرية، حدد نعم من القائمة المنسدلة هذا جهاز ظاهري.
 3. انقر على زر بحث الآن.
- يبحث التطبيق عن الأجهزة التي تُعد جزءًا من البنية الأساسية 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 و يدويًا. بعد كل عملية استقصاء للشبكة، تتم إضافة جميع أجهزة الكمبيوتر المكتشفة إلى القائمة تلقائيًا؛ ومع ذلك، يمكنك أيضًا إضافة أجهزة الكمبيوتر يدويًا إذا كنت لا ترغب في استقصاء الشبكة. يمكنك إضافة أجهزة أخرى إلى القائمة يدويًا، على سبيل المثال، أجهزة التوجيه أو الطابعات أو أجهزة الكمبيوتر.

من خصائص جهاز يمكنك عرض معلومات مفصلة حول هذا الجهاز وتحريرها.

قد تحتوي قائمة الأجهزة المكتشفة على أنواع الأجهزة التالية:

- أجهزة الكمبيوتر
- الأجهزة الجواله
- 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 المجلد **المستودعات** الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي **الأجهزة**.

2. في مساحة عمل مجلد **الأجهزة**، انقر على زر **إضافة جهاز** لفتح نافذة **جهاز جديد**.

يتم فتح النافذة **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 املا 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 المجلد 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 المجلد المستودعات الخاص بشجرة وحدة التحكم، حدد المجلد الفرعي الأجهزة.

2. في مساحة عمل المجلد الأجهزة، انقر فوق الزر 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 النافذة **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 14.

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 بعض قيود الترخيص وفقاً للقواعد التالية:

- إذا كان عدد الوحدات المستخدمة حالياً 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 حالياً 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 حالياً 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 استخدام التطبيق لفترة زمنية محدودة، والذي يتم منحه بموجب اتفاقية ترخيص المستخدم النهائي.

ترخيص يمكنك من استخدام أنواع الخدمات التالية:

- استخدام التطبيق وفقاً لبنود اتفاقية ترخيص المستخدم النهائي.
- الحصول على الدعم الفني

يعتمد نطاق استخدام الخدمات وفترة الصلاحية على نوع الترخيص المستخدم في تنشيط التطبيق.

يتم توفير أنواع التراخيص التالية:

- تجريبي – ترخيص مجاني مُعد لتجريب التطبيق. يحتوي الترخيص التجريبي عادة على فترة ترخيص قصيرة. وبمجرد انتهاء صلاحية الترخيص التجريبي، تصبح جميع مزايا Kaspersky Security Center معطلة. للاستمرار في استخدام التطبيق، يجب شراء الترخيص التجاري. يمكنك تنشيط التطبيق بموجب الترخيص التجريبي مرة واحدة فقط.
- تجاري – ترخيص تجاري مقدم عند شراء التطبيق. عند انتهاء فترة صلاحية الترخيص التجاري، يستمر تشغيل التطبيق مع وظائف محدودة (على سبيل المثال، لا تتوفر تحديثات قاعدة البيانات Kaspersky Security Center). للاستمرار في استخدام كافة مزايا Kaspersky Security Center، يجب عليك تجديد الترخيص التجاري الخاص بك. وننصح بتجديد الترخيص قبل انتهاء صلاحيته لضمان الحد الأقصى للحماية 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.

يمكنك عرض شروط اتفاقية ترخيص المستخدم النهائي لعميل الشبكة الخاص بنظام التشغيل Windows و عميل الشبكة الخاص بنظام التشغيل Mac و عميل الشبكة الخاص بنظام التشغيل Linux باستخدام الطرق التالية:

- أثناء تنزيل حزمة توزيع عميل الشبكة من خوادم الويب الخاصة بـ Kaspersky.

- أثناء تثبيت عميل الشبكة الخاص بنظام التشغيل Windows، و عميل الشبكة الخاص بنظام التشغيل Mac و عميل الشبكة الخاص بنظام التشغيل Linux.

- من خلال قراءة وثيقة license.txt المدرجة في عميل الشبكة الخاص بحزمة توزيع نظام التشغيل Windows، و عميل الشبكة الخاص بحزمة توزيع نظام التشغيل Mac و عميل الشبكة الخاص بحزمة توزيع نظام التشغيل Linux.

- عن طريق قراءة وثيقة license.txt في عميل الشبكة الخاص بمجلد تثبيت نظام التشغيل Windows، و عميل الشبكة الخاص بمجلد تثبيت نظام التشغيل Mac و عميل الشبكة الخاص بمجلد تثبيت نظام التشغيل Linux.

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:

- مفتاح 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 وفقاً 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 نشطاً أو إضافياً (أو احتياطياً).

مفتاح الترخيص المفعّل هو مفتاح الترخيص الذي يستخدم حالياً من قبل التطبيق. يمكن إضافة مفتاح ترخيص مفعّل لترخيص تجريبي أو تجاري. لا يمكن أن يستخدم التطبيق أكثر من مفتاح ترخيص واحد مفعّل.

مفتاح الترخيص الإضافي (أو الاحتياطي) هو مفتاح ترخيص يُعطي المستخدم الحق في استخدام التطبيق ولكن لا يتم استخدامه حالياً. يُصبح مفتاح الترخيص الإضافي مفعلاً تلقائياً عند انتهاء صلاحية الترخيص المرتبط بمفتاح الترخيص المفعّل الحالي. لا يمكن إضافة مفتاح ترخيص إضافي إلا إذا كان قد تم بالفعل إضافة مفتاح ترخيص مفعّل.

يمكن إضافة مفتاح الترخيص للتجريبية كمفتاح الترخيص المفعّل. لا يمكن إضافة مفتاح الترخيص للتجريبية كمفتاح الترخيص الإضافي.

حول ملف المفتاح

ملف المفتاح هو ملف بامتداد key. 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.
- تلقى ملف مفتاح عبر [الموقع الإلكتروني لـ Kaspersky](#) باستخدام رمز التنشيط المتوفر لديك.

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 تلقينته 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. يمكنك تجديد اشتراكك على موقع ويب موفر الخدمة.

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 التنشيط من خلال عنوان البريد الإلكتروني الذي قمت بتحديدته عقب شراء Kaspersky Security Center أو عقب طلب الإصدار التجريبي من Kaspersky Security Center.

لتنشيط التطبيق باستخدام رمز تنشيط، ستحتاج إلى الوصول إلى الإنترنت لإنشاء اتصال مع خوادم تنشيط Kaspersky.

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.

1. في شجرة وحدة التحكم، حدد **خادم الإدارة** ← **خيارات متقدمة** ← **اتفاقيات ترخيص المستخدم النهائي المقبولة**.
يتم عرض قائمة باتفاقيات ترخيص المستخدم النهائي المقبولة عند إنشاء حزم التثبيت أو عند التثبيت للسلس 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 السلسلة 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 لخدمة Google 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.

تم تصميم Kaspersky Security Center للتنفيذ المركزي لمهام الإدارة والصيانة الأساسية في شبكة المؤسسة. يُمكن 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 Security Center. 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 المثبتة 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 في شبكة المؤسسة التي تم تلقيها بوصفها نتيجة لاكتشاف الجهاز في شبكة Active Directory أو شبكة Windows، أو من خلال فحص الفواصل الزمنية لـ IP. يجمع خادم الإدارة البيانات بشكل مستقل أو يتلقى البيانات من عميل الشبكة.
- معلومات حول الوحدات التنظيمية والمجالات والمستخدمين والمجموعات التابعة لـ Active Directory المستلمة بوصفها نتيجة لاكتشاف الجهاز في شبكة Active Directory. يجمع خادم الإدارة البيانات بشكل مستقل أو يتلقى البيانات من عميل الشبكة.
- 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 14 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، نوع 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، وبنات 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.

• 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 14 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 14 Web Console.

- تفاصيل الأجهزة المحمولة التي تم نقلها باستخدام بروتوكول Exchange ActiveSync. 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 IMEI، ورقم الهاتف.
- مواصفات الجهاز المحمول ومكوناته: حالة إدارة الجهاز، ودعم الرسائل النصية القصيرة، وإذن بإرسال رسائل نصية قصيرة، ودعم FCM، ودعم أوامر المستخدم، ومجلد تخزين نظام التشغيل، واسم الجهاز.
- تفاصيل الإجراءات على الأجهزة المحمولة: موقع الجهاز (من خلال أمر تحديد الموقع)، ووقت إجراء آخر عملية مزامنة، ووقت إجراء آخر اتصال بخادم الإدارة، وتفاصيل دعم المزامنة.
- 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 ICCID (SIM 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 المُستخدمة 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 المثبتة 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 المثبتة 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 14 Web Console.
- إعدادات مكونات Kaspersky Security Center وتطبيقات Kaspersky المُدارة والمقدمة في السياسات وملفات تعريف السياسات. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- إعدادات مهام مكونات Kaspersky Security Center وتطبيقات Kaspersky المُدارة. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- البيانات التي تمت معالجتها بواسطة ميزة إدارة الثغرات الأمنية والتصحّيات. يقوم عميل الشبكة بنقل البيانات المُدرجة أدناه من الجهاز إلى خادم الإدارة:
- تفاصيل التطبيقات والتصحّيات المثبتة على الأجهزة المُدارة (سجل التطبيقات).

- معلومات حول الأجهزة المكتشفة على الأجهزة المُدارة (سجل الأجهزة).
- تفاصيل الثغرات الأمنية في برامج طرف خارجي المكتشفة على الأجهزة المُدارة.
- تفاصيل التحديثات المتوفرة لتطبيقات الأطراف الخارجية المثبتة 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 المُدارة. يقوم المستخدم بإدخال البيانات ونقلها باستخدام الأداة المساعدة klsclag لخادم الإدارة.
- البيانات الضرورية لعمل Kaspersky Security Center في بيئات السحابة (Amazon Web Services و Microsoft Azure و Google Cloud و Yandex Cloud). يدخل المستخدم البيانات في وحدة تحكم الإدارة أو Kaspersky Security Center 14 Web Console.
- فئات مستخدمي التطبيقات. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- قائمة الملفات التنفيذية التي تم اكتشافها في الأجهزة المُدارة بواسطة ميزة التحكم في التطبيقات. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 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 أخصائيو 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) المثبتة أو المتصلة 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 المشفرة 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.
- البيانات المطلوبة لتكامل برنامج Kaspersky Security Center مع خدمة Kaspersky Managed Detection and Response (وجوب تثبيت المكون الإضافي المخصص لبرنامج Kaspersky Security Center 14 Web Console): رمز بدء التكامل، ورمز التكامل، ورمز جلسة المستخدم. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console. تنتقل خدمة Kaspersky MDR رمز التكامل ورمز جلسة المستخدم عبر المكون الإضافي المخصص.
- تفاصيل رموز التنشيط التي تم إدخالها أو الملفات الرئيسية المحددة. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 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. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 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. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- محفوظات مراجعة كائنات الإدارة. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- سجل كائنات الإدارة المحذوفة. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- حزم التثبيت التي تم إنشاؤها من الملف، وكذلك إعدادات التثبيت. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- البيانات المطلوبة لعرض إعلانات Kaspersky في Kaspersky Security Center 14 Web Console. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- البيانات المطلوبة لتشغيل المكونات الإضافية للتطبيقات المُدارة في Kaspersky Security Center 14 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 14 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. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 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 مطلقاً إلى خادم الإدارة.
- شهادة التوصليل الأمن للأجهزة المُدارة ومكونات Kaspersky Security Center. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.
- البيانات المطلوبة لتشغيل برنامج Kaspersky Security Center في البيئات السحابية، مثل Amazon Web Services (AWS) و Microsoft Azure و Google Cloud و Yandex.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 14 Web Console
 - محطة سطر الأوامر عند استخدام الأداة المساعدة klsconfig
 - تفاعل المكونات مع خادم الإدارة عبر كائنات أتمتة klakout و Kaspersky Security Center OpenAPI
 - أي بيانات يقوم المستخدم بإدخالها في واجهة تحكم الإدارة أو واجهة Kaspersky Security Center 14 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 14 Web Console

• محطة سطر الأوامر عند استخدام الأداة المساعدة klsconfig

• تتفاعل المكونات مع خادم الإدارة عبر كائنات أتمتة و Kaspersky Security Center OpenAPI و klakout

• 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.

• قام خادم الإدارة و عميل الشبكة بتعيين نقطة توزيع لجمع معلومات حول الأجهزة المتصلة بالشبكة.

• يتم نقل البيانات من الجهاز المحمول إلى خادم الإدارة باستخدام بروتوكول Exchange ActiveSync أو 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 التفرغ 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 التفرغ أو ملفات التتبع الخاصة بمكونات Kaspersky Security Center على بيانات عشوائية لخادم الإدارة، و عميل الشبكة، ووحدة تحكم الإدارة، وخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM، وخادم الأجهزة المحمولة Exchange، و Kaspersky Security Center 14 Web Console. يمكن أن تحتوي هذه الملفات على بيانات شخصية وحساسة. يتم تخزين ملفات التفرغ وملفات التتبع وملفات السجل على الجهاز بشكل غير مشفر. لا يتم تلقائيًا نقل ملفات التفرغ 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 14 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

في Kaspersky Security Center، يمكن تطبيق الترخيص على مجموعات مختلفة من الوظائف.

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 حل على قائمة بالتطبيقات المضمنة في هذا الحل. قد يقبل خادم الإدارة مفاتيح الترخيص غير المدعومة، على سبيل المثال مفتاح الترخيص لـ Kaspersky Endpoint Security Cloud، ولكن تكون وظائف Kaspersky Security Center في مثل هذه الحالات غير مدعومة.

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.
- التحكم في حالة أمان مكافحة الفيروسات للمؤسسة
- تثبيت التطبيقات عن بُعد.
- عرض قائمة بصور نظام التشغيل المتوفرة للتثبيت عن بُعد.
- التكوين المركزي للتطبيقات المثبتة على الأجهزة العملية.
- عرض وترخيص مجموعات التطبيقات المرخصة الموجودة.
- إحصاءات وتقارير حول تشغيل التطبيق، بالإضافة إلى إخطارات حول الأحداث الحرجة
- التشفير وإدارة حماية البيانات.
- العرض والتحرير اليدوي لقائمة مكونات الأجهزة التي تم اكتشافها بواسطة استقصاء الشبكة
- عمليات التشغيل المركزية للملفات التي تم نقلها إلى العزل أو النسخ الاحتياطي والملفات ذات المعالجة المؤجلة
- إدارة أدوار المستخدمين.

يتم توفير Kaspersky Security Center مع دعم الوظائف الأساسية لوحدة الإدارة كجزء من تطبيقات Kaspersky لحماية الشبكات المشتركة. يمكنك كذلك تنزيله من [الموقع الإلكتروني لـ Kaspersky](#).

قبل تفعيل التطبيق أو بعد انتهاء صلاحية الترخيص التجاري، يقدم Kaspersky Security Center [الوظائف الأساسية لوحدة الإدارة](#) فقط.

ميزة إدارة الثغرات الأمنية والتصحيحات

تتوفر الوظائف التالية:

- التثبيت عن بُعد لأنظمة التشغيل
- تثبيت تحديثات البرامج عن بُعد، فحص وإصلاح الثغرات الأمنية
- مخزون الأجهزة.
- إدارة مجموعة التطبيقات المرخصة.
- الإذن البعيد للاتصال بالأجهزة العملية عبر مكون من Microsoft® Windows® يُسمى Remote Desktop Connection.
- الاتصال بالأجهزة العملية عن بُعد من خلال مشاركة سطح المكتب لـ Windows

وحدة الإدارة لإدارة الثغرات الأمنية والتصحيحات هي جهاز عميل في مجموعة الأجهزة المدارة.

تتوفر معلومات تفصيلية بشأن الأجهزة أثناء عملية الجرد كجزء من إدارة الثغرات الأمنية والتصحيحات. للتشغيل الصحيح لإدارة الثغرات الأمنية والتصحيحات، يجب توفر مساحة فارغة على القرص تساوي 100 جيجابايت على الأقل.

ميزة إدارة الجهاز المحمول

يتم استخدام ميزة إدارة الجهاز المحمول لإدارة الأجهزة المحمولة (Exchange ActiveSync (EAS و iOS MDM.

تتوفر الوظائف التالية للأجهزة المحمولة Exchange ActiveSync:

- إنشاء وتحرير ملفات تعريف إدارة الأجهزة المحمولة، تعيين ملفات التعريف لصناديق بريد المستخدمين
- تكوين الأجهزة المحمولة (مزامنة البريد الإلكتروني، استخدام التطبيقات، كلمة مرور المستخدم، تشفير البيانات، اتصال محركات الأقراص القابلة للإزالة).
- تثبيت الشهادات على الأجهزة المحمولة

تتوفر الوظائف التالية لأجهزة iOS MDM:

- إنشاء وتحرير ملفات تعريف التكوين، وتثبيت ملفات تعريف التكوين على الأجهزة المحمولة.
- تثبيت التطبيقات على أجهزة محمولة عبر App Store® أو استخدام ملفات البيان (.plist).
- قفل الأجهزة المحمولة، وإعادة تعيين كلمة مرور الجهاز المحمول، وحذف كل البيانات من الجهاز المحمول.

إضافة إلى ذلك، يتيح لك إدارة الأجهزة المحمولة تنفيذ الأوامر المقدمة بواسطة البروتوكولات ذات الصلة.

وحدة الإدارة لإدارة الأجهزة المحمولة هي جهاز محمول. يتم وضع في الاعتبار إدارة جهاز محمول منذ اتصاله بخادم الأجهزة المحمولة.

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 مسبقاً من الحقوق وتعيين هذه الأدوار للمستخدمين اعتماداً على مدى نطاق واجباتهم.

التثبيت 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. 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.

الاندماج باستخدام البيانات السحابية

Kaspersky Security Center لا يعمل مع الأجهزة الموجودة في موقع العمل فحسب، بل يوفر أيضًا ميزات خاصة للعمل في بيئة السحابة، مثل معالجة تكوين بيئة السحابة. يعمل Kaspersky Security Center مع الأجهزة الافتراضية التالية:

- مثيلات Amazon EC2
- أجهزة Microsoft Azure الافتراضية
- مثيلات أجهزة Google Cloud الافتراضية

تصدير الأحداث إلى أنظمة SIEM: QRadar بواسطة IBM و Micro Focus بواسطة ArcSight

يمكن استخدام تصدير الحدث في الأنظمة المركزية التي تتعامل مع مشاكل الأمان على المستوى المؤسسي والتقني، والتي توفر خدمات مراقبة الأمان، وتجمع المعلومات من الحلول المختلفة. وهذه هي أنظمة SIEM التي توفر التحليل الفوري لتحذيرات الأمان والأحداث التي تنشأها أجهزة الشبكة والتطبيقات، أو مراكز تشغيل الأمان (SOC).

بموجب ترخيص خاص، يمكنك استخدام بروتوكولات CEF و LEEF لتصدير الأحداث العامة إلى أنظمة SIEM، وكذلك الأحداث التي ترسلها تطبيقات Kaspersky إلى خادم الإدارة.

LEEF (Log Event Extended Format) أو التنسيق الموسع لحدث السجل) هو تنسيق حدث مخصص لـ IBM Security QRadar SIEM. 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 المعارف لـ IBM.

CEF (تنسيق الحدث العام) هو 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. أنظمة ArcSight و Splunk SIEM تستخدم هذا البروتوكول.

حول قيود الوظائف الرئيسية

قبل تفعيل التطبيق أو بعد انتهاء صلاحية الترخيص التجاري، يقدم Kaspersky Security Center الوظائف الأساسية لوحدة الإدارة فقط. وفيما يلي وصف للقيود المفروضة على عملية تشغيل التطبيق الأساسية هذه.

إدارة الأجهزة المحمولة

لا يمكنك إنشاء ملف تعريف جديد وتخصيصه لجهاز محمول (iOS MDM) أو صندوق بريد (Exchange ActiveSync). تتوفر دائمًا التغييرات على ملفات التعريف الموجودة وتعيين ملفات التعريف لصناديق البريد.

إدارة التطبيقات

يتعذر عليك تشغيل مهمة تثبيت التحديث ومهمة إزالة التحديث. سيتم اكتمال جميع المهام التي بدأت قبل انتهاء صلاحية الترخيص، لكن لن يتم تثبيت آخر التحديثات على سبيل المثال، إذا تم بدء مهمة تثبيت تحديث هامة قبل انتهاء صلاحية الترخيص، فسيتم تثبيت التحديثات المهمة الموجودة قبل انتهاء صلاحية الترخيص.

يتوفر أيضًا مهام تشغيل وتحرير المزامنة وفحص الثغرات الأمنية وتحديث قاعدة بيانات الثغرات الأمنية. أيضًا لا توجد قيود على عرض أو بحث أو فرز الإدخالات في قائمة الثغرات الأمنية والتحديثات.

التثبيت عن بُعد لنظم التشغيل والتطبيقات

يتعذر تشغيل مهام التقاط صورة نظام التشغيل وتثبيتها. سيتم اكتمال المهام التي بدأت قبل انتهاء صلاحية الترخيص.

لا يمكن استرجاع أي معلومات حول الأجهزة الجديدة عبر خادم الجهاز المحمول. يتم الاحتفاظ بالمعلومات حول أجهزة الكمبيوتر والأجهزة المتصلة محدثة. لم يتم إرسال إخطارات حول التغييرات في تكوين الأجهزة.

تتوفر قائمة الأجهزة للعرض والتحرير يدويًا.

إدارة مجموعة التطبيقات المرخصة

يتعذر عليك إضافة مفتاح ترخيص جديد.

لم يتم إرسال إخطارات حول انتهاكات قيود استخدام مفتاح الترخيص.

الاتصال عن بُعد بالأجهزة العميلة

لا يتوفر الاتصال عن بُعد بالأجهزة العميلة.

أمان مكافحة الفيروسات

يستخدم مكافحة الفيروسات قواعد البيانات التي تم تثبيتها قبل انتهاء صلاحية الترخيص.

الاندماج باستخدام البيانات السحابية

عند العمل في بيئة السحابة، لا يمكنك استخدام أدوات AWS API أو Azure API لاستقصاء قطاع السحابة وتثبيت التطبيقات على الأجهزة. لم تتوفر عناصر الواجهة أيضًا التي تعرض وظائف محددة للعمل في بيئة سحابة.

مميزات 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 والتصحیحات 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 والتصحیحات)، 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.

مميزات 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 التنشيط 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 من 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 وفقاً للجدول الخاص بها. يمكنك مقاطعة إجراءات التثبيت عن طريق إيقاف المهمة يدوياً.

في حالة إرجاع خطأ عند تثبيت التطبيق عن بُعد، يمكنك العثور على سبب هذا الخطأ وإصلاحه باستخدام [الأداة المساعدة لتحضير التثبيت عن بُعد](#).

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 تلقائياً إذا كانت نافذة الخصائص الخاصة بحزمة التثبيت لتطبيق الأمان هذا (القسم [تطبيقات غير متوافقة](#)) تم تحديد خيار [إلغاء تثبيت التطبيقات غير المتوافقة تلقائياً](#) بها.

إزالة التطبيقات غير المتوافقة عند تكوين التثبيت عن بُعد لأحد التطبيقات

يمكنك تمكين الخيار [إلغاء تثبيت التطبيقات غير المتوافقة تلقائياً](#) 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 14 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: [تثبيت التطبيقات باستخدام معالج التثبيت عن بُعد](#)

• Kaspersky Security Center 14 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 تمكن 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 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 إنشاؤها في وقت سابق. يمكنك تحديد المجموعة المحددة الافتراضية أو المجموعة المخصصة التي أنشأتها.
- **تعيين مهمة لمجموعة إدارة.** في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في مجموعة إدارة تم إنشاؤها في وقت سابق.

لتنفيذ التثبيت عن بُعد بشكل صحيح على جهاز لم يتم تثبيت عميل الشبكة عليه، يجب أن تكون المنافذ التالية مفتوحة: (أ) TCP 139 و UDP 445؛ (ب) UDP 137 و 138. بشكل افتراضي، تكون هذه المنافذ مفتوحة على جميع الأجهزة المضمنة في المجال. تكون مفتوحة تلقائيًا باستخدام [الأداة المساعدة لتجهيز التثبيت عن بُعد](#).

تثبيت تطبيق على الأجهزة المحددة

لتثبيت تطبيق على الأجهزة المحددة:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في الأجهزة ذات الصلة.
2. في شجرة وحدة التحكم، حدد مجلد المهام.
3. قم بتشغيل إنشاء المهمة بالنقر فوق الزر **إنشاء مهمة**.
يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.
في نافذة **تحديد نوع المهمة الخاصة بإضافة معالج المهمة**، في عقدة **خادم إدارة Kaspersky Security Center 14 حدد تثبيت التطبيق عن بُعد** كنوع المهمة.
يقوم إضافة معالج المهمة بإنشاء مهمة تتعلق بالتثبيت عن بُعد للتطبيق المحدد لأجهزة محددة. يتم عرض المهمة التي تم إنشاؤها حديثاً في مساحة عمل المجلد **المهام**.
4. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقاً 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.

يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.

في نافذة تحديد نوع المهمة الخاصة بإضافة معالج المهمة، في عقدة خادم إدارة Kaspersky Security Center 14 حدد تثبيت التطبيق عن بُعد كنوع المهمة.

تقوم إضافة معالج المهمة بإنشاء مهمة جماعية خاصة بالتثبيت 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.

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 في تكوين تثبيت التطبيق باستخدام [معالج التثبيت عن بُعد](#).

2. في النافذة تحديد إعدادات المهمة التثبيت عن بُعد بمعالج التثبيت عن بُعد، حدد خيار تعيين تثبيت الحزمة في سياسات مجموعة Active Directory.

3. في النافذة تحديد الحسابات للوصول إلى الأجهزة لمعالج التثبيت عن بُعد، حدد الخيار يُلزم وجود حساب (عمل الشبكة غير مستخدم).

4. أضف الحساب الذي يمتلك امتيازات المسؤول على الجهاز المثبت عليه Kaspersky Security Center أو الحساب المضمن مجموعة المجال Group 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.

z. في قائمة إدخال الأذونات، انقر نقرًا مزدوجًا فوق الحساب الذي أضفته للتو.

z. 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 مشاركة، أي مجلد الشبكة المشترك للتطبيق. في مجلد تثبيت Kaspersky Security Center، سيتم إنشاء مجلد متداخل بديل 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 خيار تشغيل المهام الفائتة 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 وربط 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

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 نافذة تحديد نوع المهمة الخاصة بإضافة معالج المهمة، في جزء خادم إدارة **Kaspersky Security Center 14** في مجلد خيارات متقدمة حدد **تثبيت تطبيق خوادم الإدارة الثانوية عن بُعد** كنوع المهمة.
- سيقوم إضافة معالج المهمة 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 إنشاؤها 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 و 445؛ UDP 137 و 138. بشكل افتراضي، تكون هذه المنافذ مفتوحة لجميع الأجهزة المضمنة في المجال. تكون مفتوحة تلقائيًا بواسطة **الأداة المساعدة لتجهيز التثبيت عن بُعد**.

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** ④

إذا تم تحديد هذا الخيار، فسوف يتم إنشاء مهمة التثبيت عن بُعد لمجموعة أجهزة.

• **تحديد أجهزة للتثبيت** ④

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 ⑤

إذا كان هذا الخيار مفعلاً، سيتم تسليم حزم التثبيت إلى الأجهزة العميلة بواسطة عميل الشبكة المثبت على الأجهزة العميلة هذه. في حال تعطيل هذا الخيار، سيتم تسليم حزم التثبيت باستخدام أدوات Microsoft Windows. ننصح بتفعيل هذا الخيار إذا تم تعيين المهمة إلى الأجهزة المثبت عليها عملاء الشبكة. يتم تمكين هذا الخيار افتراضياً.

• استخدام موارد نظام التشغيل من خلال خادم الإدارة ⑤

إذا تم تفعيل هذا الخيار، سيتم نقل الملفات إلى أجهزة الكمبيوتر العميلة باستخدام أدوات Microsoft Windows عبر 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 افتراضياً.

• استخدام موارد نظام التشغيل عبر نقاط التوزيع ⑤

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 افتراضياً لمهام التثبيت عن بُعد التي تم إنشاؤها على خادم إدارة افتراضي.

• عدد محاولات التثبيت ⑤

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، فسيوقف 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 (يدوياً 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 عدد 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 مستعداً لعملية تثبيت التطبيق، يمكنك زيادة قيمة عدد محاولات تثبيت المعلمة وبدء تشغيل المهمة لتثبيت التطبيق. وبدلاً 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 ⑤

سيتم تثبيت التطبيق حتى على الأجهزة التي تدار بواسطة خوادم إدارة أخرى.
يتم تحديد هذا الخيار بشكل افتراضي؛ لا تحتاج إلى تغيير هذا الإعداد إذا كان لديك خادم إدارة واحد فقط في الشبكة الخاصة بك.

• **يتم تثبيت فقط على الأجهزة المُدارة من خلال خادم الإدارة هذا** ⑤

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** ⑤

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** ⑤

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)** ⑤

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** ⑤

يتم توزيع المفتاح على الأجهزة بالإضافة إلى حزمة التثبيت.

لا نوصي بقيامك بتوزيع المفتاح باستخدام هذه الطريقة؛ لأن وصول القراءة المشترك ممكن لمستودع الحزم.

تظهر النافذة **تحديد مفتاح ترخيص** إذا لم تشمل 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** ⑤

في حالة تحديد هذا الخيار، لن يتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

• **أعد تشغيل الجهاز** ④

في حالة تحديد هذا الخيار، فستتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

• **مطالبة المستخدم باتخاذ إجراء** ④

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 افتراضياً.

• **فرض إغلاق التطبيقات في الجلسات المحظورة** ④

إذا تم تمكين هذا الخيار، فسيتم فرض إغلاق التطبيقات المثبتة على الأجهزة المحظورة قبل إعادة تشغيل الجهاز. يتم تعطيل هذا الخيار افتراضياً.

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)** ④

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 كيل الشبكة على الأجهزة العميلة، فلن يتوفر هذا الخيار.

• **يلزم وجود حساب (عميل الشبكة غير مستخدم)** ④

إذا تم تحديد هذا الخيار، فيمكنك تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. يمكنك تحديد الحساب إذا لم يتم تثبيت عميل الشبكة على الأجهزة التي تم تعيين المهمة لها. يمكنك تحديد حسابات مستخدمين متعددة، على سبيل المثال، في حالة عدم امتلاك أي منها لجميع الحقوق الموضحة على جميع الأجهزة التي تم تحديد هذه المهمة من أجلها. في هذه الحالة، يتم استخدام جميع الحسابات التي تمت إضافتها لتشغيل المهمة بترتيب متعاقب من الأعلى إلى الأسفل. في حالة عدم إضافة أي حساب، سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

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 بعد اكتمال معالج التثبيت عن بُعد**، لن تبدأ مهمة التثبيت عن بُعد. يمكنك بدء المهمة يدوياً لاحقاً. 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.

يؤدي هذا الأمر إلى بدء تشغيل معالج التثبيت عن بُعد. اتبع إرشادات المعالج.

4. عند الخطوة النهائية من المعالج، انقر فوق **التالي** لإنشاء وتشغيل مهمة التثبيت عن بُعد على الأجهزة المحددة.

عند انتهاء معالج التثبيت عن بُعد، يقوم Kaspersky Security Center بتنفيذ الإجراءات التالية:

- إنشاء حزمة تثبيت لتثبيت التطبيق (إذا لم يتم الإنشاء مسبقاً). 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 حديثاً في المجلد **المهام** أو يتم إضافتها إلى مهام مجموعة الإدارة التي تم إنشاؤها من أجلها. يمكنك بدء تشغيل المهمة يدوياً لاحقاً. تتطابق اسم المهمة مع اسم حزمة التثبيت الخاصة بالتطبيق **تثبيت <اسم حزمة التثبيت>**.

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 التبويب **التقارير**.
3. في المجلد **التقارير**، حدد قالب التقرير المسمى **تقرير نشر الحماية**.

تعرض مساحة العمل تقريراً 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 مثبتاً 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 يدوياً 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 إنشاؤها في وقت سابق. يمكنك تحديد المجموعة المحددة الافتراضية 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.

الإزالة عن بُعد لتطبيق من الأجهزة العملية الخاصة بمجموعة الإدارة

لإزالة التطبيق عن بُعد من الأجهزة العملية 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 التثبيت المهام.
4. قم بتشغيل إنشاء المهمة بالنقر فوق الزر **إنشاء مهمة**.
يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.
في نافذة **تحديد نوع المهمة الخاصة بإضافة معالج المهمة**، في جزء **خادم إدارة Kaspersky Security Center 14**، في مجلد **خيارات متقدمة** حدد **إلغاء تثبيت التطبيق عن بُعد** كنوع المهمة.
تقوم إضافة معالج المهمة بإنشاء مهمة جماعية خاصة بالإزالة عن بُعد للتطبيق المحدد. تظهر المهمة الجديدة في مساحة عمل مجموعة الإدارة على علامة التثبيت 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 العملية في مجموعة الإدارة.

الإزالة عن بُعد للتطبيق من الأجهزة المحددة

لإزالة التطبيق عن بُعد من الأجهزة المحددة:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في الأجهزة ذات الصلة.
2. في شجرة وحدة التحكم، حدد مجلد المهام.
3. تشغيل إنشاء المهمة بالنقر فوق **مهمة جديدة**.
يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.
في نافذة **تحديد نوع المهمة الخاصة بإضافة معالج المهمة**، في جزء **خادم إدارة Kaspersky Security Center 14**، في مجلد **خيارات متقدمة** حدد **إلغاء تثبيت التطبيق عن بُعد** كنوع المهمة.
تقوم إضافة معالج المهمة بإنشاء مهمة تتعلق بالإزالة عن بُعد للتطبيق المحدد من الأجهزة المحددة. يتم عرض المهمة التي تم إنشاؤها حديثًا في مساحة عمل المجلد المهام.
4. 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 المعلومات 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 لخدام 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.

إنشاء حزمة توزيع

لإنشاء حزمة تثبيت، قم بإجراء ما يلي:

1. قم بالاتصال بخادم الإدارة المطلوب.

2. من شجرة وحدة التحكم، في المجلد **التثبيت عن بُعد**، حدد المجلد الفرعي **حزم التثبيت**.

3. يمكنك بدء إنشاء حزمة التثبيت بإحدى الطرق التالية:

- بتحديد **جديد** ← **حزمة التثبيت** من قائمة السياق الخاصة بمجلد **حزم التثبيت**.
- بتحديد **إنشاء** ← **حزمة التثبيت** من قائمة السياق الخاصة بقائمة حزم التثبيت.
- عن طريق النقر فوق الرابط **إنشاء حزمة التثبيت** في قسم إدارة قائمة حزم التثبيت.

يؤدي هذا الأمر إلى بدء تشغيل معالج الحزمة الجديدة. اتبع إرشادات المعالج.

عند إنشاء حزمة تثبيت لتطبيق Kaspersky، قد تتم مطالبتك بعرض اتفاقية الترخيص وسياسة الخصوصية لهذا التطبيق. يُرجى قراءة اتفاقية الترخيص وسياسة الخصوصية بعناية. إذا وافقت على جميع شروط اتفاقية الترخيص وسياسة الخصوصية، حدد الخيارات التالية في قسم **أؤكد أنني قد قرأت وفهمت وأقبل بالكامل الشروط والأحكام التالية**:

• **شروط وبنود اتفاقية ترخيص المستخدم النهائي هذه**

• **سياسة الخصوصية التي تصف طريقة التعامل مع البيانات**

سيستمر تثبيت التطبيق على جهازك بعد تحديد كلاً من الخيارين. إنشاء حزمة التثبيت ثم السير الذاتية. يتم تحديد المسار إلى ملف اتفاقية الترخيص وسياسة الخصوصية في ملف KUD أو KPD المضمن في مجموعة توزيع التطبيق الذي سيتم إنشاء حزمة التثبيت له.

عند إنشائك حزمة تثبيت لـ Kaspersky Endpoint Security for Mac، يمكنك تحديد لغة اتفاقية الترخيص.

أثناء إنشاء حزمة تثبيت لتطبيق من قاعدة بيانات تطبيقات Kaspersky، يمكنك تمكين التثبيت التلقائي لمكونات النظام (المتطلبات الأساسية) المطلوبة لتثبيت التطبيق. يعرض معالج الحزمة الجديدة قائمة بجميع مكونات النظام المتاحة للتطبيق المحدد. إذا تم إنشاء حزمة تثبيت التصحيح (حزمة توزيع غير مكتملة)، تحتوي القائمة على جميع متطلبات النظام الأساسية لنشر التصحيح، ما يصل إلى حزمة التوزيع الكاملة. يمكنك العثور على هذه القائمة في أي وقت في خصائص حزمة التثبيت.

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. سيطلب منك ترقية مثيلك من Kaspersky Security Center إلى الإصدار الأدنى المطلوب.

بعد إنهاء معالج الحزمة الجديدة، ستظهر حزمة التثبيت الجديدة في مساحة العمل الخاصة بالمجلد **حزم التثبيت**، والموجود في شجرة وحدة التحكم.

لا يلزم إنشاء حزمة تثبيت يدويًا لتثبيت عميل الشبكة عن بُعد. يتم إنشاؤها بشكل تلقائي أثناء تثبيت Kaspersky Security Center ويتم تخزينها في المجلد **حزم التثبيت**. في حالة حذف حزمة التثبيت عن بُعد الخاصة بعميل الشبكة، يمكنك إنشاؤها مرة أخرى عن طريق تحديد الملف `nagent.kud` في المجلد **NetAgent** الخاص بحزمة توزيع Kaspersky Security Center.

لا تقم بتحديد أي من التفاصيل للحسابات المميزة في معلمات حزم التثبيت.

عند إنشاء حزمة تثبيت خادم الإدارة، حدد الملف `sc.kud` في المجلد الجذر لحزمة توزيع Kaspersky Security Center كملف للوصف.

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 و macOS و Linux. 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** ← **متقدم** ← **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 تثبيت مستقلة. انتقل عبر المعالج من خلال استخدام الزر **التالي**.

4. في الصفحة الأولى من المعالج، إذا كنت قد حددت حزمة تثبيت لتطبيق Kaspersky وترغب في تثبيت عميل الشبكة مع التطبيق المحدد، تأكد أن خيار **تثبيت عميل الشبكة بالإضافة إلى هذا التطبيق** مفعّل.

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 التثبيت المستقلة الحالية**. حدد هذا الخيار إذا أردت استخدام حزمة تثبيت مستقلة. لن يتم بدء عملية إنشاء الحزمة.

- إعادة إنشاء حزمة التثبيت المستقلة الحالية. 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> مع السمات.

7. في الصفحة التالية من المعالج، إذا أردت فتح قائمة حزم التثبيت المستقلة، قم بتمكين خيار فتح قائمة الحزم المستقلة.

8. انقر على زر إنهاء.

معالج إنشاء حزمة تثبيت مستقلة يغلق.

يتم إنشاء حزمة التثبيت المستقلة ووضعها في المجلد الفرعي PkgInst الخاص بمجلد 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 الزر 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 زر **تصفح**، وفي نافذة **فتح** على نظام التشغيل Windows القياسي، 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 مخزنة 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 14**

سيتم تثبيت التطبيق من خلال الإعدادات الموصى بها، إذا كانت المعلومات عن التطبيق المحدد مشتملة على قاعدة بيانات Kaspersky. إذا أدخلت المعلمات في الحقل **سطر أوامر الملف التنفيذي**، تتم إعادة كتابتها باستخدام الإعدادات الموصى بها. يتم تمكين هذا الخيار افتراضيًا. قام محلو Kaspersky بإنشاء قاعدة بيانات Kaspersky وصيانتها. يحدد محلو 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 **بمجلد 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 معلومات إضافية للتثبيت الصامت، فيرجى تحديدها في هذا الحقل. راجع وثائق البائع للاطلاع على التفاصيل. يمكنك أيضًا إدخال معلومات 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 `<build number>_<ksc_<version number>_<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:

• محلّيًا 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.

يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.

في نافذة تحديد نوع المهمة الخاصة بمعالج مهمة جديدة، في جزء خادم إدارة Kaspersky Security Center 14، في مجلد خيارات متقدمة حدد توزيع تثبيت الحزمة كنوع المهمة.

سيقوم إضافة معالج المهمة 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 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. للتعديل (على سبيل المثال، في محرر مفكرة Microsoft Windows). يمتلك الملف التنسيق العادي لملف التكوين .ini.

3. قم بإضافة الأسطر التالية إلى الملف:

```
[SetupProcessResult]
```

```
Wait=1
```

يقوم هذا الأمر بتكوين Kaspersky Security Center حتى ينتظر إكمال إعداد التطبيق الذي تم إعداد حزمة التثبيت من أجله وتحليل رمز إرجاع برنامج المثبت إذا كان عليك تعطيل نقل بيانات التشخيص، فقم بتعيين قيمة مفتاح الانتظار إلى 0.

4. أضف وصفاً إلى رموز الإرجاع الخاصة بالتثبيت الناجح. لتنفيذ هذا الأمر، أضف الأسطر التالية إلى الملف:

```
[SetupProcessResult_SuccessCodes]
```

```
<رمز الإرجاع>=[<الوصف>]
```

```
<رمز الإرجاع 1>=[<الوصف>]
```

...

تحتوي الأقواس المربعة على مفاتيح اختيارية.

بناء الجملة الخاص بهذه الأسطر:

- <رمز الإرجاع>. أي رقم مقابل لرمز إرجاع المثبت. يمكن تغيير عدد رموز الإرجاع.
- <وصف>. 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]
```

```
<رمز الإرجاع>=[<الوصف>]
```

```
<رمز الإرجاع 1>=[<الوصف>]
```

...

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 المُحدّثة

يسمح لك Kaspersky Security Center بتلقي إصدارات تطبيقات الشركة المُحدّثة التي يتم تخزينها على خوادم Kaspersky.

لتلقي الإصدارات المُحدّثة 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 على **إجراءات إضافية** ومن القائمة المنسدلة، حدد **عرض الإصدار الحالي من تطبيق Kaspersky**.

يتم عرض قائمة الإصدار الحالي من تطبيقات Kaspersky.

2. حدد التطبيق المطلوب من القائمة.

3. 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. سيطلب 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 حديثاً في المجلد التثبيت عن بُعد في شجرة وحدة التحكم، في المجلد الفرعي حزم التثبيت.

يمكنك أيضاً فتح نافذة إصدارات التطبيق الحالية بالنقر على رابط عرض الإصدار الحالي لتطبيقات Kaspersky في مساحة عمل المجلد حزم التثبيت.

تحضير جهاز للتثبيت عن بُعد. الأداة المساعدة riprep.exe

تثبيت التطبيق عن بُعد 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 و عميل الشبكة المثبت على الجهاز العميل. لتحديد سبب المشكلة، استخدم الأداة المساعدة المصممة لتشخيص الأجهزة العميلة عن بُعد (klastgui).
- 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.
- لحل المشاكل التي تحدث أثناء تثبيت التطبيق على جهاز عميل بدون تثبيت عميل الشبكة، يمكنك استخدام الأداة المساعدة المصممة لتحضير الأجهزة للتثبيت عن بُعد (riprep).

يحتوي هذا القسم على وصف الأداة المساعدة التي تتيح لك تحضير الجهاز للتثبيت عن بُعد (riprep). توجد الأداة المساعدة في مجلد تثبيت Kaspersky Security Center الموجود على الجهاز الذي تم تثبيت خادم الإدارة عليه.

لا يمكن تشغيل الأداة المستخدمة لتحضير الجهاز للتثبيت عن بُعد من خلال إصدار Microsoft Windows XP Home Edition.

تحضير الجهاز للتثبيت عن بُعد في الوضع التفاعلي

لتحضير الجهاز للتثبيت عن بُعد في الوضع التفاعلي:

1. قم بتشغيل الملف riprep.exe على جهاز عميل.
2. في النافذة الرئيسية للأداة المساعدة لتحضير التثبيت عن بُعد، حدد الخيارات التالية:

- تعطيل مشاركة الملفات البسيطة
- بدء خدمة خادم الإدارة

• فتح المنافذ

• إضافة حساب

• تعطيل التحكم في حساب المستخدم (UAC) (غير متوفر إلا للأجهزة التي تعمل بنظام التشغيل Microsoft Windows Vista أو Microsoft Windows Server 2008 أو Windows 7)

3. انقر فوق الزر بدء.

تظهر نتائج مراحل تحضير الجهاز للثبيت عن بُعد في الجزء الأسفل من النافذة الرئيسية للأداة المساعدة.

إذا قمت بتحديد خيار إضافة حساب، فستتم مطالبتك بإدخال اسم الحساب الذي قمت بإنشائه وكلمة المرور عندما يتم إنشاء الحساب. سيؤدي هذا إلى إنشاء حساب محلي، ينتمي إلى مجموعة المسؤولين المحليين.

في حالة تحديد خيار تعطيل التحكم في حساب المستخدم (UAC)، سيتم إجراء محاولة لتعطيل التحكم في حساب المستخدم حتى في حالة تعطيل UAC قبل أن يتم بدء تشغيل الأداة المساعدة. بعد تعطيل UAC، ستتم مطالبتك بإعادة تشغيل الجهاز.

تحضير الجهاز للثبيت عن بُعد في الوضع غير التفاعلي

تحضير الجهاز للثبيت عن بُعد في الوضع غير التفاعلي:

قم بتشغيل الملف riprep.exe الموجود على جهاز عميل من سطر الأوامر باستخدام مجموعة متطلبات المفاتيح.

بناء جملة سطر الأوامر للأداة المساعدة:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

مواصفات المفاتيح:

- -silent - بدء تشغيل الأداة في وضع غير تفاعلي.
- -cfg CONFIG_FILE - تعريف تكوين الأداة المساعدة، حيث CONFIG_FILE - المسار إلى ملف التكوين (ملف له الامتدادات .ini).
- -tl traceLevel - تعريف مستوى التتبع، حيث traceLevel - رقم من 0 إلى 5. في حالة عدم تحديد مفتاح، يتم استخدام القيمة 0.

يمكنك تنفيذ المهام التالية عن طريق بدء تشغيل الأداة المساعدة في الوضع الصامت:

• تعطيل المشاركة البسيطة للملفات

• بدء تشغيل خدمة الخادم على الجهاز العميل

• فتح المنافذ

• إنشاء حساب محلي

• تعطيل التحكم في حساب المستخدم (UAC)

يمكنك تحديد المعلمات الخاصة بتحضير الجهاز للثبيت عن بُعد في ملف التكوين المحدد في المفتاح -cfg. لتحديد هذه المعلمات، قم بإضافة المعلومات التالية إلى ملف التكوين:

• في القسم مشترك، حدد المهام المطلوب تنفيذها:

• DisableSFS - تعطيل المشاركة البسيطة للملفات (0 - يتم تعطيل المهمة، 1 - يتم تمكين المهمة).

- StartServer—بدء خدمة الخادم (0—تم تعطيل المهمة؛ 1—تم تمكين المهمة).
- OpenFirewallPorts—فتح المنافذ الضرورية (0—تم تعطيل المهمة، 1—تم تمكين المهمة).
- DisableUAC—تعطيل التحكم في حساب المستخدم (0) (UAC—يتم تعطيل المهمة، 1—يتم تمكين المهمة).
- RebootType—تعريف السلوك في حالة طلب إعادة تشغيل الكمبيوتر عندما يتم تعطيل UAC. يمكنك استخدام القيم التالية:
 - 0—عدم إعادة تشغيل الجهاز مطلقًا
 - 1—إعادة تشغيل الجهاز، إذا تم تمكين UAC قبل بدء الأداة المساعدة
 - 2—فرض إعادة التشغيل، إذا تم تمكين UAC قبل بدء الأداة المساعدة
 - 4—إعادة تشغيل الكمبيوتر دائمًا
 - 5—فرض إعادة تشغيل دائمًا
- في القسم UserAccount، حدد اسم الحساب (المستخدم) وكلمة المرور الخاصة به (كلمة المرور).

نموذج لسياق ملف التكوين:

```
[Common]
DisableSFS=0
StartServer=1
OpenFirewallPorts=1

[UserAccount]
user=Admin
Pwd=Pass123
```

بعد إكمال الأداة المساعدة، سيتم إنشاء الملفات التالية في مجلد بدء تشغيل الأداة المساعدة:

- riprep.txt—تقرير التشغيل، حيث يتم سرد مراحل عمليات الأداة المساعدة مع أسباب هذه العمليات.
- riprep.log—ملف التتبع (يتم إنشاؤه إذا تم تعيين مستوى التتبع أعلى من 0).

إعداد جهاز يعمل بنظام Linux لتثبيت عميل الشبكة عن بُعد

لإعداد جهاز يعمل بنظام Linux لتثبيت عميل الشبكة عن بُعد:

1. تأكد من تثبيت sudo على جهاز Linux الهدف.

2. 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:

لا PasswordAuthentication

نعم ChallengeResponseAuthentication

احفظ الملف (إذا لزم الأمر) ثم أعد تشغيل خدمة SSH باستخدام الأمر `sudo service ssh restart`.

b. قم بتعطيل كلمة مرور sudo الخاصة بحساب المستخدم الذي سيتم توصيل الجهاز بموجبه.

c. استخدم الأمر visudo في برنامج sudo لفتح ملف تكوين sudoers.

في الملف الذي فتحت، ابحث عن السطر الذي يبدأ بـ % sudo (أو بـ % wheel إذا كنت تستخدم نظام التشغيل CentOS). تحت هذا السطر، حدد ما يلي: < ALL = (ALL) NOPASSWD: ALL > username. في هذه الحالة، يكون < username > عبارة عن حساب المستخدم الذي يجب استخدامه لاتصال الجهاز باستخدام SSH.

d. احفظ ملف sudoers ثم أغلقه.

e. اتصل بالجهاز مجدداً عبر SSH وتأكد من عدم مطالبة خدمة Sudo بإدخال كلمة مرور؛ ويمكنك القيام بذلك باستخدام الأمر sudo whoami.

3. 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.

لتطبيق الإعداد الذي تم تغييره، أعد تشغيل جهاز Linux أو نفذ الأمر التالي:

```
sudo systemctl systemd-logind.service $ إعادة تشغيل
```

4. 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.

5. تنزيل وإنشاء حزمة تثبيت:

a. قبل تثبيت الحزمة على الجهاز، تأكد من أن كل التبعيات مثبتة بالفعل (البرامج والمكتبات) لهذه الحزمة.

يمكنك عرض تبعيات 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. تنزيل حزمة تثبيت عميل الشبكة.

c. لإنشاء حزمة تثبيت عن بُعد، استخدم الملفات التالية:

• klnagent.kpd

• akinstall.sh

• حزمة DEB أو RPM لعميل الشبكة

6. إنشاء مهمة تثبيت عن بُعد بالإعدادات التالية:

• في صفحة الإعدادات من معالج المهمة الجديدة، حدد خانة الاختيار 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.

7. وقم بتشغيل مهمة التثبيت عن بُعد.

قد يظهر خطأ إذا كنت تثبت عميل شبكة بنظام SSH على الأجهزة التي تقوم بتشغيل إصدارات Fedora الأقدم من الإصدار 20. في هذه الحالة، وكي يتم تثبيت عميل الشبكة بنجاح، قم بتعطيل خيار المتطلبات الافتراضية (إحاطته بجملة تعليق لإزالته من الرمز الذي يتم تحليله) للملف /etc/sudoers. للاطلاع على وصف تفصيلي لشرط خيار المتطلبات الافتراضية الذي قد يسبب مشكلات أثناء اتصال SSH، يرجى الرجوع إلى موقع الويب [Bugzilla bugtracker](#).

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-com
```

يمكنك هذا من تثبيت حزمة insserv-Compatibile وتكوين عميل الشبكة بشكل صحيح.

قم بتشغيل دورة في الدقيقة -q insserv- متوافق مع 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-Compatibile 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.

إلى جانب تثبيت حزمة insserv-Compatibile، 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 الجهاز العميل: في **تفضيلات النظام**، افتح جزء **المشاركة** وتأكد من تحديد خانة الاختيار **تسجيل الدخول عن بُعد**. 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 فتحت، في إدخال مواصفات امتياز المستخدم حدد ما يلي: اسم المستخدم ALL = (ALL) NOPASSWD: ALL. في هذه الحالة، يكون اسم المستخدم هو حساب المستخدم، الذي يجب استخدامه لاتصال الجهاز باستخدام (Secure Shell (SSH).

c. احفظ ملف sudoers ثم أغلقه.

d. اتصل بالجهاز مجددًا عبر SSH وتأكد من عدم مطالبة خدمة Sudo بإدخال كلمة المرور؛ 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

4. إنشاء مهمة تثبيت عن بُعد بالإعدادات التالية:

• في صفحة إعدادات الخاصة بإضافة معالج المهمة، انقر على زر استخدام موارد النظام التشغيل من خلال خادم الإدارة. قم بإلغاء جميع خانات الاختيار الأخرى.

• في الصفحة 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 المثبتة على الأجهزة المُدارة من خلال تطبيق ملف المفتاح أو رمز التنشيط على كل تطبيق من التطبيقات. يمكن نشر ملف المفتاح أو رمز التنشيط بالطرق التالية:

- النشر التلقائي
- حزمة تثبيت التطبيق المُدار
- مهمة مفتاح ترخيص الإضافة للتطبيق المُدار
- 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 مُدارة مختلفة وكان عليك نشر ملف مفتاح محدد أو رمز تنشيط للأجهزة، فقم باختيار طرق أخرى لنشر ملف المفتاح أو رمز التنشيط 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 الترخيص 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 التنشيط إلى مستودع خادم الإدارة.

تعليمات للمساعدة:

• وحدة تحكم الإدارة:

• [إضافة مفتاح ترخيص إلى مستودع خادم الإدارة](#)

• [التوزيع التلقائي لمفتاح الترخيص](#)

أو

• Kaspersky Security Center 14 Web Console:

• [إضافة مفتاح ترخيص إلى مستودع خادم الإدارة](#)

• [التوزيع التلقائي لمفتاح الترخيص](#)

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 التنشيط 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 العملية](#)

أو

• Kaspersky Security Center 14 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 14 Web Console](#)

• [إضافة مفتاح ترخيص إلى مستودع خادم الإدارة](#)

• [نشر مفتاح ترخيص على الأجهزة العميلة](#)

إضافة رمز التنشيط أو ملف المفتاح إلى الأجهزة يدويًا

يمكنك تنشيط تطبيق Kaspersky المثبت محليًا من خلال استخدام الأدوات المتوفرة في واجهة التطبيق. يرجى الرجوع إلى وثائق التطبيق المثبت.


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 المستخدمة على الأجهزة العميلة.

يظهر رمز بجوار كل مفاتيح التراخيص يطابق نوع الاستخدام:

•  — يتم تلقي معلومات حول مفتاح الترخيص المستخدم 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 المستخدمة 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.

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 معالج إضافة مفتاح.

3. حدد كيف تريد تنشيط خادم الإدارة: باستخدام رمز تنشيط أو باستخدام ملف مفتاح.

4. حدد رمز التنفيع 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 معالج إضافة مفتاح. يمكنك الآن رؤية مفتاح الترخيص المضاف في قائمة تراخيص Kaspersky.

حذف مفتاح ترخيص خادم الإدارة

لحذف 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. احذف مفتاح الترخيص عن طريق النقر على زر **إزالة**.

يؤدي هذا إلى حذف مفتاح الترخيص.

في حالة إضافة مفتاح ترخيص احتياطي، يصبح مفتاح الترخيص الاحتياطي تلقائيًا مفتاح الترخيص المفعّل بعد حذف مفتاح الترخيص المفعّل السابق.

بعد حذف مفتاح الترخيص المفعّل لخادم الإدارة، لا يتوفر **إدارة الثغرات الأمنية والتصحيحات وإدارة الجهاز المحمول**. يمكنك **إضافة** مفتاح محذوف 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.

لتوزيع مفتاح ترخيص على الأجهزة العميلة:

1. في شجرة وحدة التحكم، حدد المجلد **تراخيص Kaspersky**.

2. في مساحة عمل قائمة مفاتيح التراخيص، انقر فوق زر **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها**.

يبدأ تشغيل معالج إنشاء مهمة تفعيل التطبيق. اتبع إرشادات المعالج.

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 الترخيص على خادم الإدارة.

لتوزيع أحد مفاتيح الترخيص 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. في نافذة خصائص مفتاح الترخيص التي تفتح، حدد خانة الاختيار **توزيع المفتاح تلقائيًا إلى الأجهزة التي يتم إدارتها**. 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.

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. 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 الترخيص على الأجهزة العملية:

1. في شجرة وحدة التحكم، حدد العقدة التي تحمل اسم خادم الإدارة المطلوب.
 2. في مساحة عمل العقدة، حدد علامة التبويب **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 المستخدمة على أجهزة العملاء. ويحتوي التقرير أيضًا على معلومات حول الأجهزة التي تُستخدم بها مفاتيح الترخيص، وحول التقييدات المحددة في خصائص مفاتيح الترخيص هذه.

عرض معلومات حول مفاتيح ترخيص التطبيق

لمعرفة مفاتيح الترخيص المستخدمة لتطبيق Kaspersky:

1. في شجرة وحدة التحكم Kaspersky Security Center، حدد العقدة **الأجهزة المدارة** وانتقل إلى علامة التبويب **الأجهزة**.
2. انقر بزر الماوس الأيمن لفتح قائمة سياق الجهاز ذي الصلة وحدد **خصائص**.

3. في نافذة 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.

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 قبل 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 14 المثبت](#)
- [Kaspersky Security Center 14 Web Console المثبت \(اختياري\)](#)
- 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

1 إعداد ونشر سياسات وملفات تعريف السياسة لتطبيق Kaspersky

لتكوين ونشر إعدادات تطبيقات 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 14 Web Console. يمكن تنفيذ نهج إدارة الأمان المرتكز على المستخدم من خلال Kaspersky Security Center 14 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 14 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 العملية.

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 14 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 وفقاً 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 نجاح تثبيت [خادم إدارة Kaspersky Security Center 14 Web Console](#) و [Kaspersky Security Center 14 Web Console](#) (اختياري). إذا قمت بتثبيت Kaspersky Security Center 14 Web Console، فقد ترغب أيضًا في اعتبار إدارة الأمان [المرتكز 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 المثبتة 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 for Windows. إذا قمت باستكمال عملية التكوين باستخدام هذا المعالج، فليس عليك إنشاء سياسة جديدة لهذا التطبيق. الانتقال إلى [الإعداد البديهي 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 بشكل 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 المفصلة متاحة للتعديل في السياسات التالية. سوف ينتج لك [التسلسل الهرمي للسياسات](#) الذي قمت بإنشائه إدارة الأجهزة بفعالية في مجموعات الإدارة. تعليمات للمساعدة:

- وحدة تحكم الإدارة: [إنشاء سياسة](#)

- [Kaspersky Security Center 14 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 [علامات](#) محددة. استخدم العلامات لتصنيف 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 14 Web Console](#):

- [إنشاء ملف تعريف سياسة](#)

3 نشر السياسات وملفات تعريف السياسة على الأجهزة المدارة

بشكل افتراضي، يعمل خادم الإدارة تلقائيًا على المزامنة مع الأجهزة المدارة كل 15 دقيقة. وأثناء المزامنة، يتم نشر السياسات وملفات تعريف السياسة الجديدة أو التي تم تغييرها إلى الأجهزة المدارة. يمكنك تجنب المزامنة التلقائية وتشغيل المزامنة يدويًا باستخدام الأمر فرض المزامنة. عند اكتمال المزامنة يتم تسليم السياسات وملفات تعريف السياسة وتطبيقها على تطبيقات Kaspersky المثبتة.

إذا كنت تستخدم Kaspersky Security Center 14 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 14 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 المضافة إلى مجموعات الإدارة.

حول نهج 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 14 Web Console. يمكن تنفيذ نهج إدارة الأمان المرتكز على المستخدم من خلال Kaspersky Security Center 14 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 في Active 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 وقلها 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 الحوادث الأمنية 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 العملية 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، الرجاء مراعاة أنه يجب عليك النقر على أيقونة القفل فوق الإعداد ذي الصلة للسماح باستخدام القيمة الخاصة به على محطة العمل.

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 لـ 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 قسم **Kaspersky Security Network** الفرعي، نوصي بتمكين خيار **استخدام وكيل KSN**. يساعد استخدام هذا الخيار في إعادة توزيع وتحسين حركة المرور على الشبكة. يمكنك أيضًا تمكين استخدام خوادم KSN إذا لم تكن خدمة KSN Proxy متوفرة. قد تتواجد خوادم KSN إما على جانب Kaspersky (عند استخدام شبكة KSN العالمية) أو على جانب أطراف خارجية (عند استخدام شبكة KSN الخاصة).

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.

موضح أدناه إجراءات الإعداد الإضافية، والتي ننصحك بإجرائها في نافذة خصائص السياسة الخاصة بـ Kaspersky Endpoint Security for Windows، في قسم **الحماية من التهديدات الأساسية**.

قسم الحماية من التهديدات الأساسية، القسم الفرعي "جدار الحماية"

تحقق من قائمة الشبكات الموجودة في خصائص السياسة. قد لا تحتوي القائمة على كل الشبكات.

للتحقق من قائمة الشبكات:

1. من نافذة خصائص السياسة، ابحث عن قسم **الحماية من التهديدات الأساسية** وحدد القسم الفرعي **جدار الحماية**.

2. في قسم **الشبكات المتوفرة**، انقر فوق الزر **الإعدادات**.

يؤدي ذلك إلى فتح النافذة **جدار الحماية**. تعرض هذه النافذة قائمة بالشبكات الموجودة في علامة التبويب **الشبكات**.

قسم الحماية من التهديدات الأساسية، القسم الفرعي الحماية من تهديدات الملفات

يمكن أن يؤدي تمكين 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. من نافذة خصائص السياسة، ابحث عن قسم الحماية من التهديدات الأساسية وحدد القسم الفرعي الحماية من تهديدات الملفات.
2. في قسم مستوى الأمان، انقر فوق الزر الإعدادات.
3. من نافذة الحماية من تهديدات الملفات التي تفتح، في علامة التبويب عام، قم بإلغاء تحديد 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.

موضح أدناه إجراءات الإعداد المتقدمة، والتي ننصحك بإجرائها في نافذة خصائص السياسة الخاصة بـ Kaspersky Endpoint Security for Windows، في قسم الإعدادات العامة.

قسم الإعدادات العامة، القسم الفرعي التقارير وعمليات التخزين

في القسم نقل البيانات إلى خادم الإدارة، يُرجى ملاحظة الإعدادات التالية:

خانة اختيار حول التطبيقات التي تم بدؤها: في حالة تحديد خانة الاختيار هذه، تقوم قاعدة بيانات خادم الإدارة بحفظ معلومات حول كل 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

في حالة وجوب إدارة الحماية ضد الفيروسات في شبكة المؤسسة في الوضع المركزي عبر وحدة تحكم الإدارة، يجب عليك تعطيل عرض واجهة مستخدم Kaspersky Endpoint Security for Windows على محطات العمل (عن طريق إلغاء تحديد خانة الاختيار عرض واجهة التطبيق الموجودة في القسم التفاعل مع المستخدم)، وتمكين الحماية باستخدام كلمة المرور (عن طريق تحديد خانة الاختيار تمكين الحماية بكلمة المرور في القسم حماية بكلمة مرور).

تكوين السياسة في القسم تكوين الحدث

في القسم تكوين الحدث، ينبغي عليك تعطيل حفظ أي أحداث على خادم الإدارة ما عدا الأحداث التالية:

• في علامة تبويب حدث حرج :

• تم تعطيل التشغيل التلقائي للتطبيق

• تم رفض الوصول

• تم حظر بدء التطبيق

• التنظيف غير ممكن

• انتهاك اتفاقية الترخيص

- تعذر تحميل الوحدة النمطية للتشفير
- يتعذر تشغيل مهمتين في الوقت نفسه
- تم اكتشاف تهديد نشط. بدء التنظيف المتقدم
- تم اكتشاف هجوم على الشبكة
- لم يتم تحديث كل المكونات
- خطأ في التفعيل
- خطأ في تمكين الوضع المحمول
- خطأ في التفاعل مع Kaspersky Security Center
- خطأ في تعطيل الوضع المحمول
- خطأ في تغيير مكونات التطبيق
- خطأ في تطبيق قواعد تشفير / فك تشفير الملف
- يتعذر تطبيق السياسة
- تم إنهاء العملية
- تم حظر نشاط الشبكة
- في علامة التبويب **الفشل الوظيفي**: إعدادات المهمة غير صالحة. لم يتم تطبيق الإعدادات
- في علامة التبويب **تحذير**:
- تم تعطيل الدفاع الذاتي
- مفتاح حجز غير صحيح
- قام المستخدم بإلغاء اشتراكه في سياسة التشفير
- في علامة التبويب **"معلومات"**: يحظر 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 7:00 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 6:30 م، فلن يتم تشغيل مهمة فحص الجهاز أبدًا. يجب عليك إعداد الجدول الأكثر ملاءمة 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 7:00 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 ملاءمة 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 01:00 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 ملاءمة 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 تعيين 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.

إذا وصل عدد الأحداث في قاعدة البيانات إلى الحد الأقصى المحدد من قبل المسؤول، فيقوم التطبيق بحذف الأحداث الأقدم ويعيد أحداث جديدة عليها. عند قيام خادم الإدارة بحذف الأحداث القديمة، فلا يمكن حفظ الأحداث الجديدة في قاعدة البيانات. وأثناء هذه الفترة الزمنية، تتم كتابة معلومات حول الأحداث المرغوبة في سجل أحداث Kaspersky. يتم وضع الأحداث الجديدة في قائمة الانتظار ثم حفظها في قاعدة البيانات بعد اكتمال عملية الحذف.

لتعيين 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 المخزنة في قاعدة البيانات.

3. انقر على موافق.

يتم تعيين عدد الأحداث التي يمكن تخزينها في قاعدة البيانات إلى القيمة المحددة.

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 يوماً.

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 تقسيماً 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 التي سيتم إنشاء مهمة لها، من خلال إحدى 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 المثبت 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 العملية. يجب أن يكون خادم الإدارة الافتراضي الذي تم إنشاء المهمة منه في نفس مجموعة الإدارة أو في مستوى 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.

يبدأ تشغيل معالج إضافة مهمة. 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.

يبدأ تشغيل معالج إضافة مهمة. 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:

- 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

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 المنزلة 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.

يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.

يمكن إنشاء مهام تنزيل التحديثات إلى مستودع خادم الإدارة، وإجراء مزامنة Windows Update، وصيانة قاعدة البيانات، والنسخ الاحتياطي لبيانات خادم الإدارة مرة واحدة فقط. إذا تم إنشاء مهام تنزيل التحديثات إلى مستودع خادم الإدارة وصيانة قاعدة البيانات والنسخ الاحتياطي لبيانات خادم الإدارة وإجراء مهام مزامنة Windows Update بالفعل لخادم الإدارة، فلن يتم عرضها في نافذة تحديد نوع المهمة في معالج إضافة المهمة.

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 عن بُعد على خوادم الإدارة الثانوية](#)
- [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.
- يبدأ تشغيل معالج إضافة مهمة. 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.يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.
- تتوفر إرشادات تفصيلية حول كيفية إنشاء وتكوين المهام المحلية في أدلة تطبيقات Kaspersky المعنية.

عرض مهمة جماعية موروثية 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 موروثية من مجموعة تم إنشاؤها على خادم إدارة أساسي.
-  — إذا كانت موروثية من مجموعة مستوى أعلى.

في حالة تمكين وضع التوربث، 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 يتم مستخدم 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

لتحديد 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 تفتح، حدد خانة الاختيار 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 تتاح مهام خادم الإدارة والمهام المحلية للتصدير.

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 تتاح مهام خادم الإدارة والمهام المحلية للاستيراد.

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 مشتملة على اسم مطابق للمهمة التي تم استيرادها حديثاً الموجودة بالفعل في القائمة المحددة، تتم إضافة الفهرس (**رقم التسلسل التالي**) إلى اسم المهمة التي تم استيرادها على سبيل المثال: (1)، (2).

تحويل المهام

يمكنك استخدام Kaspersky Security Center لتحويل المهام من الإصدارات الأقدم لتطبيقات Kaspersky إلى تلك الإصدارات الأحدث للتطبيقات.

- 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 تطبيقات Kaspersky .

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 KLAAdmins**.

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 بتحديد. تبدأ المهمة.

- من خلال النقر فوق الزر  أو  في القسم **المهام** لنافذة 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 القسم 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. لا يمكن عرض نتائج التشغيل للمهام المحلية.

لعرض نتائج المهام:

1. في نافذة خصائص المهمة، حدد القسم عام.

2. انقر فوق الرابط النتائج لفتح النافذة نتائج المهمة.

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 القسم 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، والأجهزة، والوقت. 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 نافذة 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 نافذة 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 نفس النوع: على سبيل المثال، يمكنك المقارنة بين مهمتين لفحص الفيروسات، لكن لا يمكنك مقارنة مهمة لفحص الفيروسات 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 الفيروسات على الأقراص المحلية لأجهزة الكمبيوتر الخاصة بهم 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، ولتتم 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 للتثبيت / إلغاء تثبيت أحد التطبيقات في حالة عدم تثبيت عميل الشبكة أو عدم توفره. إذا تم تثبيت عميل الشبكة وتوفره، فسيتم استخدام الحساب وفقاً 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).

معالجة 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.

يمكنك "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 وكلمة 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 لاتخاذها في الخطوة التالية من المعالج.

الخطوة 2. اختيار إجراء لاتخاذها

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 لاتخاذها للمهام التي تم العثور عليها.

لكل مهمة تنتم 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 لـ خادم 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 لخادم 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 14 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. كما يقدم هذا القسم معلومات حول ملفات تعريف السياسة المدعومة في Kaspersky Security Center، بدءًا من الإصدار 10 من Service Pack 1.

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.

لن تكون سياسة الوجود خارج المكتب مدعومة في الإصدارات الأخرى من Kaspersky Security Center. سيتم استخدام ملفات تعريف السياسة بدلاً من سياسات خارج المكتب.

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، ومزمنة المحتويات الخاصة بهذه السياسات في المستقبل.

للمساعدة في تجنب مثل هذه المشكلات، فإن Kaspersky Security Center - بدءًا من الإصدار 10 من Service Pack 1 - يدعم 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:

- ملفات التعريف الاسم ذات الأسماء المتشابهة تؤثر 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 أجريت 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 المطبقة. إعدادات السياسة المعدلة 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 المطبقة 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 المجلد 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 المفعله 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 المطبقة 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 بالقفلة) على الأجهزة العملية بغض النظر عن أي الإعدادات التي تم تحديدها مسبقاً للتطبيق.

عرض سياسة موروثه 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 موروثه من مجموعة تم إنشاؤها على خادم إدارة أساسي.

•  — إذا كانت موروثه 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 بوراثةها.

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 العملية، 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

لتحرير سياسة:

1. من شجرة وحدة التحكم، حدد المجلد 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 المجلد 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 وأبها 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.

لمقارنة سياسة بأخرى:

1. من شجرة وحدة التحكم، حدد المجلد **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 مدار واحد.
 2. في قائمة السياق، حدد **مقارنة**.
- يتم عرض تقرير بتنسيق HTML لمقارنة سياستين لنفس التطبيق.

يقدم أيضًا التقرير المعني بمقارنة إعدادات السياسة لـ **Kaspersky Endpoint Security for Windows** تفاصيل مقارنة ملفات تعريف السياسات. يمكنك تصغير نتائج مقارنة ملف تعريف السياسة. لتصغير القسم، انقر فوق الرمز  بجوار اسم القسم.

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 المفعله 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 الرابط تصدير السياسة إلى ملف في خانة المعلومات الخاصة بالسياسة المحددة.
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 بعد ذلك في قائمة السياسات.

في حالة وجود اسم سياسة مطابق لاسم السياسة المستوردة حديثاً في قائمة السياسات بالفعل، سيتم توسيع اسم السياسة المستوردة باستخدام المؤشر (رقم التسلسل التالي) الفهرس، على سبيل المثال: (1)، (2).

تحويل السياسات

يمكن أن يقوم Kaspersky Security Center بتحويل السياسات من الإصدارات الأقدم لتطبيقات Kaspersky إلى تلك الإصدارات الأحدث لنفس التطبيقات.

يتوفر التحويل لسياسات التطبيقات التالية:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4.

• Kaspersky Endpoint Security 8 for Windows

• Kaspersky Endpoint Security 10 for Windows

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 السياسات من إصدارات أقدم لتطبيقات Kaspersky.

إدارة ملفات تعريف السياسة

يصف هذا القسم إدارة ملفات تعريف السياسة ويوفّر 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.

حول ملف 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 "ساح". 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 10 Service Pack 1 for Windows أو أحدث

• سياسات Kaspersky Endpoint Security 10 Service Pack 1 for Mac

• سياسات المكون الإضافي لـ Kaspersky Mobile Device Management تتراوح بين الإصدار Service Pack 1 10 والإصدار Service 10 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 العملية 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 موروثه 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 الإعدادات للاتصال، 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 مباشرة في الوحدة المحددة) أو بشكل ضمني (الجهاز يوجد في وحدة توجد في الوحدة المحددة على أي مستوى من التداخل) في وحدة محددة من Active Directory®، الجهاز أو مالكة 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 و X2 و X3 (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 و X4 و X5. سيتم تعديل السياسة P(B) مع السياسة P(A) بحيث تظهر قائمة ملفات التعريف في السياسة P(B) على النحو التالي: X5، X4، X3، X2، X1 (بترتيب تنازلي من حيث درجة الأولوية). سوف تعتمد أولوية ملف التعريف X2 على الحالة الأولية لـ X2 للسياسة P(B) و X2 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 المفعله 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 أي 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 Service Pack 110 الإصدار Service Pack 3 10 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 التويب 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 المفعله 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 وفقاً 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 نشطاً)، 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 2 والذي 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، بذلك يكون لملف التعريف 2 الأولوية القصوى، وسوف يأخذ الإعداد القيمة 2.

في قائمة ملفات تعريف السياسة، يتم عرض ملفات التعريف وفقاً لأولويات كل منها. يأتي ملف التعريف ذو الأولوية القصوى في المرتبة الأولى. يمكنك تغيير

أولوية أحد ملفات التعريف باستخدام الزرين  و .

إزالة ملف تعريف سياسة

لإزالة ملف تعريف سياسة:

1. في شجرة وحدة التحكم، حدد مجموعة الإدارة التي ترغب في إزالة 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**.
- ستتم إزالة ملف تعريف السياسة. سيتم تمرير الحالة المفعلة إما لملف تعريف سياسة آخر الذي سيتم تشغيل قواعده لتنشيطه 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 إلى 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 السياسة الجديد.
7. في النافذة **قواعد تفعيل ملف تعريف السياسة**، حدد خانة 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 بناءً 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 9

حدد خانة الاختيار هذه لإعداد قواعد تفعيل ملف تعريف السياسة على الجهاز بناءً على حجم الذاكرة وعدد المعالجات المنطقية.

يعتمد عدد النوافذ الإضافية للمعالج على الإعدادات التي تحددها في هذه الخطوة. 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 9

الجهاز موجود في شبكة خارجية، وهذا يعني أن خادم الإدارة غير متاح.

• لا 9

الجهاز موجود على الشبكة، لذا يتوفر خادم الإدارة.

• لم يتم تحديد قيمة 9

لن يتم تطبيق المعيار.

- في خانة 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 9

الشرط الخاص بتفعيل ملف تعريف السياسة (سواء تم تنفيذ القاعدة أو لم يتم تنفيذها).

• اسم القاعدة 9

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 9

في قائمة العلامات، حدد قاعدة لتضمين الجهاز في ملف تعريف السياسة عن طريق تحديد خانة 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 خانة الاختيار، لن يتم تطبيق المعيار. بشكل افتراضي، خانة الاختيار هذه غير محددة.

• التطبيق على الأجهزة بدون العلامات المحددة

مكّن هذا الخيار إذا كان يتعين عليك عكس تحديد علامتك. 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 افتراضياً.

يتم عرض نافذة 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 مالكة عضوًا في مجموعة الأمان المحددة. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضياً.

• 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 افتراضياً.

• 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 افتراضياً.

يتم عرض نافذة شروط استخدام Active Directory في حال تحديد خانة الاختيار قواعد استخدام Active Directory.

11. في نافذة شروط استخدام مالك الجهاز، حدد الإعدادات التالية:

• مالك الجهاز

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف وتمكينها على الجهاز وفقاً 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 وفقاً 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 افتراضياً.

• 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 فتح النافذة شروط استخدام مالك الجهاز إذا تم تحديد خانة الاختيار قواعد مالك جهاز معين.

12. في نافذة 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 (علامة ">").
 - 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 نافذة شروط استخدام مواصفات المعدات في حال تحديد خانة الاختيار قواعد مواصفات الأجهزة.

13. في النافذة اسم قاعدة تفعيل الخاصة بملف تعريف السياسة، 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 إلزالتها.

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 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 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.

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 (وبخاصة في مناطق حقوق الوصول والأحداث والتقارير). يجب العثور على حل آخر، على سبيل المثال، من خلال استخدام **ملفات تعريف السياسة**، والمهام الخاصة بـ **تحديدات الأجهزة**، وتعيين **عملاء الشبكة حسب السيناريو القياسي**، وما إلى ذلك.

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 مفيديًا 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.

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 المعدة 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 يمكن إنشاء فئات يتم تحديثها تلقائيًا على أساس المجلدات "%windir"، "%My Documents"، و"%ProgramFiles%". 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 قسم **خيارات متقدمة**، حدد خانة الاختيار **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 المستخدمة 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، فيمكنك تحديد طريقة التنزيل في النافذة **إعدادات** الخاصة بهذا المعالج.
- يجب أن يمتلك الحساب المستخدم بواسطة نقطة التوزيع للتحويل 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 برمز القفل (🔒) في السياسة).

تحديث Kaspersky Security Center والتطبيقات والتطبيقات 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 المدارة 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 المثبتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

عند إكمال هذا 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 أمن Kaspersky على الأجهزة المُدارة وفق سيناريو نشر تطبيقات Kaspersky عبر Kaspersky Security Center 14 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 تشغّل "المعالج"، قم بإنشاء المهمة الآن.

المهمة المطلوبة 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 المضمنة 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 14 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 تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع، 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 14 Web Console: إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

4 تكوين نقاط التوزيع

عندما تقوم شبكتك بتخصيص نقاط توزيع، تأكد أن خيار نشر التحديثات 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 توزيع الملفات عبر نقاط التوزيع فقط 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 **تنزيل التحديثات وقواعد بيانات مكافحة الفيروسات من خادم الإدارة مقدماً (مستحسن)** في **سياسة وكيل 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 يشعل 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 **تنزيل ملفات تفاضلية** في خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة و/أو مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع.

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 14 Web Console: [تمكين النموذج غير المتصل بالإنترنت لتنزيل التحديثات وتعطيله](#)

6 التحقق من التحديثات المُنزلة (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 الفيروسات 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 التحكم الإدارية أو خيار **التحقق من صحة التحديث** في Kaspersky Security Center 14 Web Console.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [التحقق من التحديثات المُنزلة](#)
- Kaspersky Security Center 14 Web Console: [التحقق من التحديثات المُنزلة](#)

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 دائماً. 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 مسبقاً، سيحاول Kaspersky Security Center إلغاء تثبيت ذلك التحديث من جميع الأجهزة. لا يمكن إلغاء تثبيت التحديثات لمكونات Kaspersky Security Center.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [الموافقة على تحديثات البرامج ورفضها](#)
- Kaspersky Security Center 14 Web Console: [الموافقة على تحديثات البرامج ورفضها](#)

8 تكوين التثبيت التلقائي للتحديثات والتصحيحات المخصصة لمكونات Kaspersky Security Center

بدءاً من الإصدار Service Pack 2 10، يتم تلقائياً تثبيت التحديثات والتصحيحات المنزلة لعميل الشبكة ومكونات [Kaspersky Security Center الأخرى](#). إذا تركت خيار **التثبيت التلقائي للتحديثات القابلة للتطبيق والتصحيحات المكونات التي لها حالة غير محددة** مفعلاً في خصائص عميل الشبكة، عندها سيتم جميع التحديثات تلقائياً 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.

بالنسبة لإصدارات وكيل الشبكة الأقدم من Service Pack 2 10، تأكد من تمكين الخيار **تحديث الوحدات النمطية لعميل الشبكة** في خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة أو مهمة تنزيل التحديثات إلى مستودعات توزيع النقاط.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center](#)
- Kaspersky Security Center 14 Web Console: [تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center](#)

تحديثات البرامج لخادم الإدارة لا تعتمد على حالات التحديث. لم يتم تثبيتها تلقائيًا ويجب أن تتم الموافقة عليها بشكل مبدئي من قبل المسؤول في تويوب المراقبة في وحدة تحكم الإدارة (خادم الإدارة > اسم الخادم < ← المراقبة) أو في قسم الإخطارات في وحدة تحكم الويب Kaspersky Security Center 14 (المراقبة والإبلاغ ← الإخطارات). يجب أن يقوم المدير بعد ذلك بتشغيل تثبيت التحديثات بشكل صريح.

10 تكوين التثبيت التلقائي لتحديثات تطبيقات الأمان.

قم بإنشاء مهام التحديثات للتطبيقات المُدارة من أجل توفير تحديثات 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 **عند تنزيل تحديثات جديدة إلى المستودع 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) وعمل الشبكة (الإصدار الأقدم من 13.2) على الإدارة الأجهزة.

بشأن افتراضي، لا يتم تثبيت تحديثات Kaspersky Endpoint Security for Windows و Kaspersky 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 14 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 DNS العام. يُعد ذلك ضروريًا للتأكد من تحديث قواعد بيانات مكافحة الفيروسات والحفاظ على مستوى الأمان للأجهزة المُدارة.

- تطبيقات Kaspersky المثبتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان
- 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:

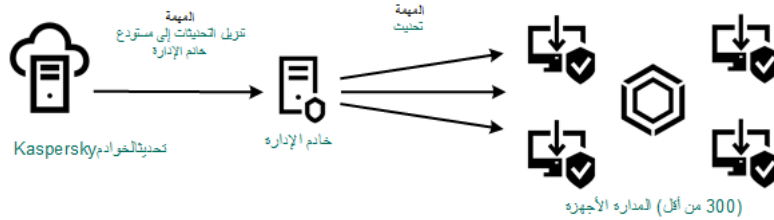
- مهمة تنزيل التحديثات إلى مستودع خادم الإدارة

- 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 for Windows على الأجهزة المُدارة

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).

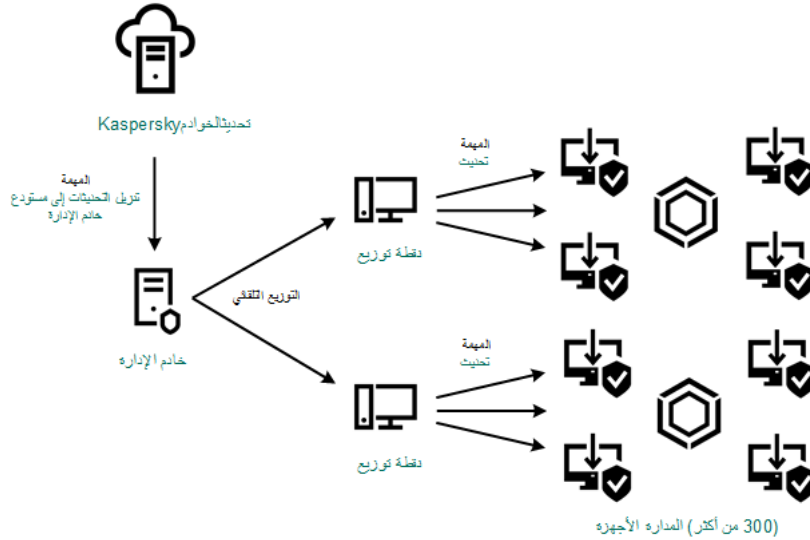


التحديث باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة دون نقاط توزيع

يتصل خادم الإدارة افتراضياً 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 المطلوبة لشبكتك وتكوينها.

وفي هذا المخطط، يتم تنزيل التحديثات تلقائياً من مستودع خادم الإدارة إلى مستودعات نقاط التوزيع. تقوم الأجهزة المُدارة المضمنة 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 تلقائياً.
- قواعد بيانات Kaspersky والوحدات النمطية للبرامج لتطبيقات الأمان على الأجهزة المُدارة

يتم تثبيت هذه التحديثات من خلال مهمة تحديث لـ [Kaspersky Endpoint Security for Windows](#).

• تحديثات خادم الإدارة

لا يتم تثبيت هذه التحديثات تلقائيًا. ويجب على المسؤول الموافقة صراحة على تثبيت التحديثات وتشغيلها.

تلازم 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 الأمان

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 14 Web Console](#)). ويتم تثبيت التحديثات من خلال المهمة تحديث ويمكن تكوينها في خصائص هذه المهمة.

لا تتوفر تنزيل التحديثات إلى مستودع مهمة خادم الإدارة على خوادم الإدارة الافتراضية. مستودع خادم الإدارة الافتراضي يعرض التحديثات المنزلة 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

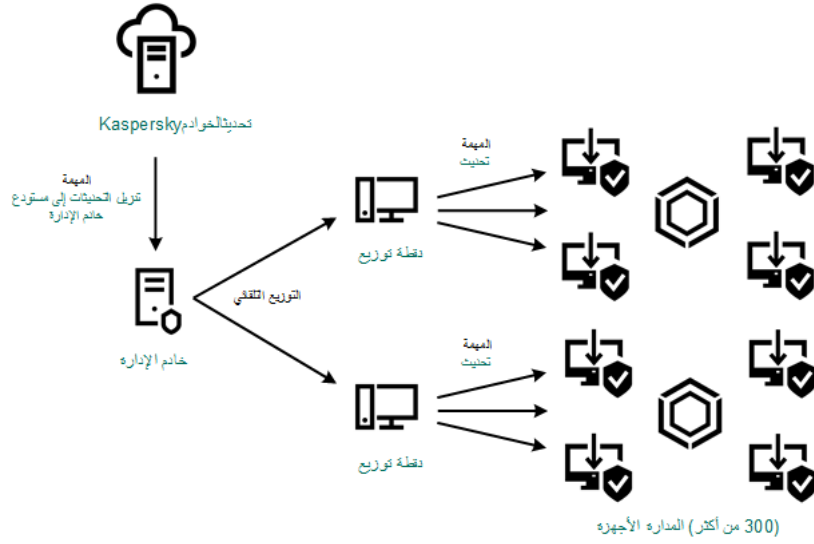
• معرف المفتاح المفعّل

• معرف تشغيل تنزيل التحديثات إلى مستودع مهمة خادم الإدارة

لا تحتوي أي 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 افتراضياً 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 التوزيع بالإضافة إلى مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. وبعد ذلك، ستقوم نقاط التوزيع بتنزيل التحديثات من خوادم تحديث Kaspersky وليس من مستودع خادم الإدارة.

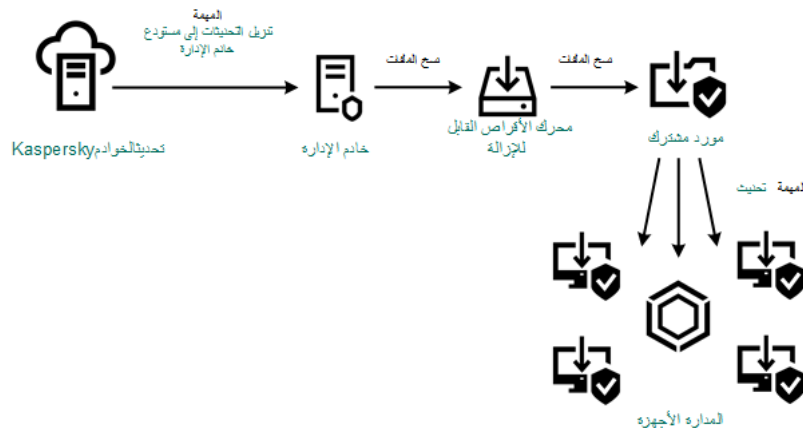
لا يمكن لأجهزة نقاط التوزيع التي تعمل بنظام macOS تنزيل التحديثات من خوادم تحديث Kaspersky.

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، نظراً 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

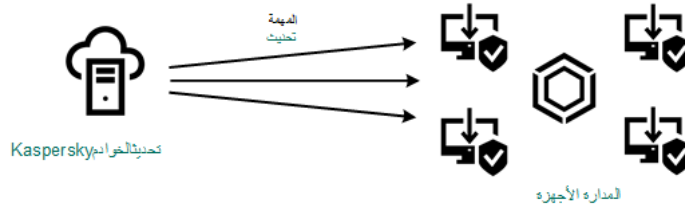
إذا لم تتمتع الأجهزة العملية باتصال بخادم الإدارة، يمكنك استخدام مجلد محلي أو مورد مشترك كمصدر لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. وفي هذا المخطط، تحتاج إلى نسخ التحديثات اللازمة من مستودع خادم الإدارة إلى محرك الأقراص القابل للإزالة ونسخ التحديثات إلى المجلد المحلي أو المورد المشترك المحدد كمصدر تحديث في إعدادات Kaspersky Endpoint Security for Windows (انظر الشكل أدناه).



التحديث من خلال مجلد محلي أو مجلد مشترك أو خادم FTP

مباشرة من خوادم تحديث Kaspersky إلى Kaspersky Endpoint Security for Windows على الأجهزة المُدارة

على الأجهزة المُدارة، يمكنك تكوين Kaspersky Endpoint Security for Windows 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. وتلقي التحديثات مباشرة من خوادم تحديث Kaspersky، حدد خوادم تحديث Kaspersky كمصدر تحديث في واجهة تطبيق الأمان. للحصول على وصف كامل لهذه الإعدادات، يرجى الرجوع إلى وثائق [Kaspersky Endpoint Security for Windows](#).

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 داخل شبكة شركتك لأن 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 الأحدث.

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: سيناريو

المتطلبات الأساسية

المتطلبات الأساسية لهذا السيناريو كالتالي:

- تمت ترقية خوادم الإدارة ونقاط التوزيع إلى الإصدار 11 أو الأحدث.
- 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 القسم [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 تنزيل التحديثات إلى مستودع مهمة خادم الإدارة الخاص بخادم الإدارة تلقائيًا بواسطة معالج البدء السريع من Kaspersky Security Center. يمكنك إنشاء مهمة واحدة فقط لتنزيل التحديثات إلى مستودع مهمة خادم الإدارة. ولهذا السبب، يمكنك إنشاء تنزيل التحديثات إلى مستودع مهمة خادم الإدارة إذا تمت إزالة تلك المهمة من قائمة مهام خادم الإدارة فقط.

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.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر التالي.

3. في صفحة المعالج تحديد نوع المهمة، حدد تنزيل التحديثات إلى مستودع خادم الإدارة.

4. في صفحة المعالج إعدادات، حدد إعدادات المهمة كما يلي:

• [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 افتراضياً 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 المثبت 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.

إذا قمت بتمكين الخيار **لا تستخدم الخادم الوكيل** لخوادم تحديث Kaspersky أو مصادر التحديث المجلد المحلي أو مجلد الشبكة، فلن يستخدم خادم الإدارة خادمًا وكيلاً لتنزيل التحديثات.

- 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. بخلاف ذلك، تبدأ مهام التحديث على خوادم الإدارة الثانوية بالعمل وفقاً للجداول الزمنية الخاصة بهم. يتم تعطيل هذا الخيار افتراضياً.

- **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 يدوياً 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 إلى مستودع المهام لخوادم إدارة أخرى، قم بتحديد نفس مشاركة الشبكة كمصدر تحديث.

يتم تعطيل هذا الخيار افتراضياً.

- **لا تفرض تحديث الأجهزة وخوادم الإدارة الثانوية إلا عند اكتمال النسخ**

تبدأ مهام تنزيل التحديثات على الأجهزة العملية وخواص الإدارة الثانوية فقط بعد نسخ تلك التحديثات من مجلد التحديث الرئيسي إلى مجلدات التحديث الإضافية.
يجب تمكين هذا الخيار إذا كانت الأجهزة العملية وخواص الإدارة الثانوية تقوم بتنزيل تحديثات من مجلدات شبكة إضافية.
يتم تعطيل هذا الخيار افتراضياً.

• تحديث الوحدات النمطية لعمل الشبكة (إصدارات عميل الشبكة الأقدم من Service Pack 2 10)

إذا تم تمكين هذا الخيار، فسيتم تثبيت التحديثات الخاصة بالوحدات النمطية لبرامج عميل الشبكة تلقائياً بعد انتهاء خادم الإدارة من مهمة تنزيل التحديثات إلى المستودع. خلافاً لذلك، يمكن تثبيت التحديثات التي يتم تلقيها للوحدات النمطية لعمل الشبكة يدوياً.
ينطبق هذا الخيار فقط على إصدارات Network Agent التي تسبق Service Pack 2 10. بدءاً من الإصدار Service Pack 2 10، يتم تحديث وكلاء الشبكة تلقائياً.
يتم تمكين هذا الخيار افتراضياً.

• تنزيل التحديثات باستخدام النظام القديم

بدءاً 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 بيانات تعريف متوافقة مع النظام الجديد. إذا كان مصدر التحديث يحتوي على ملفات تحديث بيانات 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 افتراضياً.

5. 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 وفقاً له، و قم 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 ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• **كل N يوماً:**

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 ④

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 ④

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) ④

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 ④

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• حسب أيام الأسبوع ④

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهريًا ④

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 ④

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط. يتم تمكين هذا الخيار افتراضيًا.

• كل شهر في أيام معينة من الأسابيع المحددة ④

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد. بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• عند انتشار الفيروس ④

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 المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار تشغيل الجهاز وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• 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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تمكين هذا الخيار افتراضيًا.

• استخدام 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 المترامنة 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 المترامنة 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 المعالج إنهاء عملية إنشاء المهمة، انقر على زر إنهاء لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار 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 بتحديددها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

عندما يقوم خادم الإدارة بتنفيذ تنزيل التحديثات إلى مستودع مهمة خادم الإدارة، يتم تنزيل تحديثات قواعد البيانات والوحدات النمطية للبرنامج 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 العملية 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.

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 زر إنشاء مهمة.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر التالي.

3. في صفحة المعالج تحديد نوع المهمة، حدد عقدة خادم إدارة Kaspersky Security Center 14 وقم بتوسيع المجلد خيارات متقدمة ثم حدد مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع.

4. في صفحة المعالج إعدادات، حدد إعدادات المهمة كما يلي:

• [مصادر التحديثات](#)

يمكن استخدام الموارد التالية كمصدر لتحديثات نقطة التوزيع:

- خوادم تحديث Kaspersky (خوادم HTTP(S)) 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 المُثبَّت 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.

إذا قمت بتمكين الخيار **لا تستخدم الخادم الوكيل** خوادم تحديث Kaspersky أو مصادر التحديث المجلد المحلي أو مجلد الشبكة، فلن تستخدم نقطة التوزيع خادمًا وكيلاً لتنزيل التحديثات، حتى عند تمكين الخيار **استخدام الخادم الوكيل في إعدادات سياسة عميل الشبكة** الخاصة بنقطة التوزيع.

• **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 14** 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 14 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، انقر فوق **استعراض** وقم بتحديد مجموعة الإدارة التي يتم تطبيق المهمة عليها.

6. 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 ⑤

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• كل N يومًا ⑤

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 ⑤

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 ⑤

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) ⑤

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 ⑤

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• حسب أيام الأسبوع ⑤

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهريًا ⑤

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 9

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.
يتم تمكين هذا الخيار افتراضيًا.

• كل شهر في أيام معينة من الأسابيع المحددة 9

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.
بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• عند انتشار الفيروس 9

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوفر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع المحيط
- مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.
قد ترغب في تشغيل مهام مختلفة وفقًا لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى 9

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار تشغيل الجهاز وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• تشغيل المهام الفائتة 9

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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل، ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.
يتم تمكين هذا الخيار افتراضيًا.

• استخدام التأخير العشوائي لبدء المهام تلقائيًا 9

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) 9

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 المترامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة. إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقاً للجدول. يتم تعطيل هذا الخيار افتراضياً. 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 المعالج إنهاء عملية إنشاء المهمة، انقر على زر إنهاء لإغلاق المعالج. إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار تشغيل المهمة بعد انتهاء المعالج.

عندما ينتهي المعالج من عملياته، 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 بتحديد ما 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 يدوياً أو تلقائياً. 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 المنزلة

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 تلقائياً كجزء من مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. 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 (>Share\Updates\Kaspersky Security Center installation folder). 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. أيضاً لن يتم بدء الهام ذات نوع الجدول عند تنزيل تحديثات جديدة إلى المستودع 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 صحيحاً 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 عليها.

نوصى 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. إنشاء مهمات التحديث وفحص الفيروسات لتطبيق مدعوم من Kaspersky Security Center، على سبيل المثال، Kaspersky Endpoint Security لـ Windows أو Kaspersky Security لـ Windows Server. عند إنشاء مهمات التحديث وفحص الفيروسات، حدد مجموعة الإدارة مع أجهزة الاختبار.

تقوم مهمة التحقق من صحة التحديث بتشغيل مهمات التحديث وفحص الفيروسات بالتتابع على أجهزة الاختبار للتحقق من صحة جميع التحديثات. بالإضافة إلى ذلك، عند إنشاء مهمة التحقق من صحة التحديث، تحتاج إلى تحديد مهمتي التحديث وفحص الفيروسات.

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 المهمة بإحدى الطرق التالية:

• بالنقر فوق رابط تكوين المهمة في خانة معلومات المهمة المحددة.

3. إذا كانت مهمة التحقق من صحة التحديث موجودة، فانقر 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 مسبقاً، فانقر فوق الزر إنشاء.

يبدأ معالج مهمة التحقق من صحة التحديث. اتبع إرشادات المعالج.

5. انقر فوق موافق لإغلاق نافذة الخصائص بالمهمة تنزيل التحديثات إلى مستودع خادم الإدارة.

يتم تفعيل التحقق التلقائي من التحديثات. يمكنك الآن تشغيل مهمة تنزيل التحديثات إلى مستودع خادم الإدارة وستبدأ من التحقق من صحة 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 القيام بمهمة التحقق من صحة التحديث أثناء تنفيذ مهمة تنزيل التحديثات إلى المستودع. تتضمن مدة مهمة تنزيل التحديثات إلى المستودع تحديث المجموعة الإضافية ومهام الفحص حسب 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 الخاصة بالكائنات المصابة: **تنظيف**، **حذف** إذا ما **تعذر التنظيف** / **تنظيف**، **حظر** إذا ما **تعذر التنظيف** / **حظر**. (الحماية من التهديدات الأساسية ← الحماية من تهديدات الملفات ← العمل على اكتشاف التهديدات).

• 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 بالتأكد أولاً. ينبغي تعطيل هذه القيود في إعدادات سياسات الاختبار والمهام الإضافية.

عرض التحديثات المُنزَلة

لعرض قائمة التحديثات المنزلة:

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.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر التالي.

3. في صفحة المعالج تحديد نوع المهمة، حدد Kaspersky Endpoint Security كنوع المهمة، ثم حدد تحديث كالنوع الفرعي للمهمة.

4. اتبع بقية إرشادات المعالج.

بعد انتهاء المعالج، يتم إنشاء مهمة تحديث لـ Kaspersky Endpoint Security. يتم عرض المهمة التي تم إنشاؤها حديثاً 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 جنباً 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 تعذر إنشاء أي اتصال بين عميل الشبكة وخادم الإدارة، يكون التحديث مستحيلًا. 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 وقت واحد إلى خادم الإدارة لتلقي التحديثات. في هذه الحالة، قد يتوقف خادم الإدارة عن الاستجابة للطلبات (وبالمثل لهجوم DDoS).

لتجنب حدوث مشكلات كذلك 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 بشكل 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 قبل 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 كنفذات 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، سيبتعين 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 الخاصة بالسياسة، 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 (بدءًا من الإصدار 10: Service Pack 2):

- عميل الشبكة لنظام التشغيل Windows
- وحدة تحكم الإدارة
- خادم الأجهزة المحمولة Exchange
- خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

يتوفر التحديث والتصحيح التلقائيان 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 الخاصة بالسياسة، حدد **خصائص**.

افتح نافذة خصائص سياسة عميل الشبكة.

5. في نافذة خصائص السياسة، حدد قسم **إدارة التصحيحات والتحديثات**.

6. حدد أو ألق تحديد خانة الاختيار **التثبيت التلقائي للتحديثات القابلة للتطبيق وتصحيحات المكونات التي لها حالة غير محددة لتمكين أو تعطيل التحديث والتصحيح تلقائيًا على التوالى**.

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 وحوادم 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.

يبدأ تشغيل معالج إضافة مهمة. اتبع تعليماته ونفذ 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 مباشرة 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 على الرابط 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.

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 يقوم خادم الإدارة الرئيسي باستعادة التحديثات، تبدأ مهمة تنزيل التحديثات تلقائيًا على خوادم الإدارة الثانوية بصرف النظر عن جدولها.

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 معينة 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 التنصيب 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 التنصيب، 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 التنصيب 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. يوجد بيان KSN افتراضيًا في %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula%. يتم تعطيل هذا الخيار افتراضيًا. يسري تمكين هذا الخيار فقط في حالة [تمكين](#) الخيارين استخدام خادم الإدارة ووكيل وأوافق على استخدام Kaspersky Security Network في نافذة خصائص خادم الإدارة. يمكنك تعيين عقدة مجموعة نشط-خامل إلى نقطة توزيع، وتمكين وكيل 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 / شبكة KSN الخاصة مباشرة عبر الإنترنت](#)

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المُدارة إلى KSN Cloud أو شبكة KSN الخاصة. يتم أيضًا إرسال طلبات KSN – التي تم إنشاؤها على نقطة التوزيع نفسها – مباشرةً إلى KSN Cloud أو Private KSN.

لا يمكن لنقاط التوزيع التي لديها الإصدار 11 المثبت لعملاء الشبكة (أو الأقدم)، الوصول إلى شبكة KSN الخاصة مباشرة. إذا كنت ترغب في إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KSN الخاصة، 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 شبكة KSN الخاصة مباشرةً.

• تجاهل إعدادات خادم وكيل KSC عند الاتصال بشبكة KSN الخاصة ④

قم بتمكين هذا الخيار، إذا كانت إعدادات خادم الوكيل مكوّنة في خصائص نقطة التوزيع أو في سياسة Network Agent، لكن كانت بنية شبكتك تتطلب استخدام شبكة KSN الخاصة مباشرةً. وإلا، لا يمكن وصول الطلبات الصادرة من التطبيقات المُدارة إلى شبكة KSN الخاصة.

• منفذ TCP ④

رقم منفذ TCP الذي ستستخدمه الأجهزة المُدارة للاتصال بخادم وكيل KSN. رقم المنفذ الافتراضي هو 13111.

• منفذ UDP ④

إذا احتجت أن تكون الأجهزة المُدارة متصلة بخادم وكيل KSN عبر منفذ UDP، فقم بتمكين خيار استخدام منفذ UDP وحدد رقم منفذ UDP. يتم تمكين هذا الخيار افتراضياً. والمنفذ الافتراضي لـ UDP للاتصال بخادم وكيل KSN هو 15111.

• في القسم اكتشاف الأجهزة، قم بنكوبن استقصاء مجالات Windows، و Active Directory، ونطاقات IP بواسطة نقطة التوزيع.

• مجالات Windows ④

يمكنك تمكين اكتشاف الأجهزة لمجالات Windows وتعيين الجدول للاكتشاف.

• Active Directory ④

يمكنك تمكين استقصاء الشبكة لـ Active Directory وتعيين الجدول للاستقصاء.

إذا قمت بتحديد خانة الاختيار تمكين استقصاء الشبكة، فيمكنك 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.

• نطاقات IP ④

يمكنك تمكين اكتشاف الجهاز لنطاقات IPv4 وشبكات IPv6.

إذا مكنت خيار تمكين استقصاء النطاق، فيمكنك إضافة نطاقات مسوحة ضوئياً وتعيين الجدول الزمني لها. يمكنك إضافة نطاقات IP لقائمة النطاقات التي تم فحصها.

إذا مكنت خيار تمكين الاستقصاء باستخدام تقنية شبكة لا تتطلب تكويناً فستقوم نقطة التوزيع تلقائياً باستقصاء شبكة IPv6 باستخدام شبكات التكوين الصفري (وكما يشار إليها باسم شبكة لا تتطلب تكويناً). في هذه الحالة، يتم تجاهل نطاقات IP المحددة لأن نقطة التوزيع تستقصي الشبكة بالكامل.

- 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 كقاط 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 **تلقائياً**.

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.

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 افتراضياً.

- 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. يبدأ تشغيل معالج إضافة مهمة. 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 المجال خيارات متقدمة ← إدارة التطبيق بشجرة وحدة التحكم، حدد المجال الفرعي تحديثات البرامج.

2. في مساحة عمل المجال 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 المفردة.

3. انتظر حتى اكتمال تثبيت التصحيح بنجاح.

4. قم بتشغيل التصحيح على كل العقد الفرعية في المجموعة تبعاً.

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.

تثبيت تحديثات برامج الجهات الخارجية

يتيح Kaspersky Security Center لك إدارة تحديثات البرامج المثبتة على الأجهزة العميلة وإصلاح الثغرات الأمنية في تطبيقات Microsoft ومنتجات الصانع 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.

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 لفحص الملفات بشكل تلقائي، كما تتضمن فحصًا مضادًا للفيروسات، 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، بجانب عدم إجراء أنواع أخرى من تحليل التحديثات بخلاف ما هو محدد 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.

يمكنك العثور على تفاصيل البرامج التابعة لجهة خارجية التي يمكن تحديثها عن طريق Kaspersky Security Center من خلال زيارة موقع خدمة الدعم الفني على صفحة Kaspersky Security Center في قسم [إدارة الخادم](#).

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](#) و**بائعي 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 Windows المنتشرة 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 المدارة، قم بتشغيل مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. عند اكتمال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المكتشفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة.

يتم إنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائيًا بواسطة معالج البدء السريع لخادم الإدارة. إذا لم تشغّل "المعالج"، قم بإنشاء المهمة أو تشغيل معالج البدء السريع الآن.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [فحص التطبيقات بحثًا عن الثغرات الأمنية](#)، [جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة](#)

- [Kaspersky Security Center 14 Web Console](#): إنشاء بحث عن الثغرات الأمنية والتحديثات المطلوبة المهمة، والبحث عن الثغرات الأمنية وإعدادات مهمة التحديثات المطلوبة

2 تحليل قائمة التحديثات التي تم العثور عليها

اعرض قائمة تحديثات البرنامج وحدد التحديثات التي ترغب في تثبيتها. لعرض معلومات تفصيلية حول كل تحديث، انقر على اسم التحديث في القائمة. لكل تحديث في القائمة، يمكنك أيضاً عرض إحصاءات حول تثبيت التحديث على أجهزة العميل. تعليمات للمساعدة:

- وحدة تحكم الإدارة: [عرض معلومات حول التحديثات المتوفرة](#)

- [Kaspersky Security Center 14 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 المهام أو باستخدام قائمة تحديثات البرنامج.

تستخدم مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية في تثبيت التحديثات لتطبيقات Microsoft، بما في ذلك التحديثات التي توفرها خدمة Windows Update وتحديثات منتجات 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 ترخيصاً، 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 بحث عن الثغرات الأمنية والتحديثات المطلوبة.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [إصلاح الثغرات الأمنية في التطبيقات](#)، [عرض معلومات حول التحديثات المتوفرة](#)

- [Kaspersky Security Center 14 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 مُحدّثة دائماً، قم بجدولة مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة لتشغيل المهمة تلقائياً من وقتٍ لآخر. التكرار الافتراضي هو مرة واحدة في الأسبوع.

إذا كنت قد أنشأت مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك جدولتها لتعمل بالتكرار نفسه الذي تعمل به مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة 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 بحث عن الثغرات الأمنية والتحديثات المطلوبة.

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 اعتماداً على حالة التحديث: غير محدد أو مقبول أو مرفوض. قد ترغب على سبيل المثال في إنشاء مخمة محددة للحوادم ووضع قاعدة لهذه المهمة من أجل السماح بتثبيت تحديثات Windows Update فقط والتحديثات التي بحالة مقبول. بعدها أنت تقوم يدوياً 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 تحديثات البرنامج (العمليات ← إدارة التصحيحات ← تحديثات البرنامج).

- وحدة تحكم الإدارة: [الموافقة على تحديثات البرامج ورفضها](#)

- Kaspersky Security Center 14 Web Console: [الموافقة على تحديثات برامج الأطراف الخارجية ورفضها](#)

6 تكوين خادم الإدارة للعمل كخادم (WSUS Windows Server Update Services) (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 14 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 14 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 معرف – 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 أولاً 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 فعالاً 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 معرف.

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 سابقاً. 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 سابقاً. ومع ذلك، لن يتم تثبيت هذه التحديثات أبداً 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 تُثبَّت بعد. ستظل التحديثات على الأجهزة التي تم تثبيتها عليها بالفعل. إذا كان يتعين عليك حذفها، فيمكنك حذفها يدوياً محلياً.

مزمنة التحديثات من Windows Update مع خادم الإدارة

إذا كنت قد حددت استخدام خادم الإدارة كخادم WSUS في النافذة إعدادات إدارة التحديثات الخاصة بمعالج البدء السريع، يتم إنشاء مهمة مزمنة Windows Update تلقائياً. يمكنك تشغيل المهمة في المجلد المهام. تتوفر وظائف تحديث برامج Microsoft فقط بعد اكتمال مهمة إجراء مزمنة Windows Update بنجاح.

تقوم المهمة إجراء مزمنة 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 لمزمنة 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 مزمنة Windows Update في القائمة المنسدلة.

يقوم المعالج بإنشاء المهمة إجراء مزمنة Windows Update التي يتم عرضها في المجلد المهام.

يبدأ معالج إنشاء مهمة استرداد بيانات مركز تحديث Windows. اتبع إرشادات المعالج.

يمكنك أيضاً إنشاء مهمة إجراء مزمنة 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 دائماً ما بين 200000 و300000. في Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 والإصدارات الأقدم، تم الاحتفاظ بكل التحديثات: لم يتم حذف أي تحديثات قديمة. كنتيجة لذلك، يزداد حجم قاعدة البيانات باستمرار. لتقليل استخدام مساحة القرص وحجم قاعدة البيانات في Kaspersky Security Center 10 Service Pack 3، تم تطبيق حذف التحديثات القديمة التي لم تعد موجودة على خوادم تحديث Microsoft.

عند تشغيل مهمة إجراء مزمنة 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 مزمنة Windows Update، يتم حذف كل التحديثات التي تحمل علامة للحذف منذ 30 يوماً. كما يتحقق Kaspersky Security Center من التحديثات القديمة التي تم وضع علامة عليها للحذف منذ أكثر من 180 يوماً، ثم يحذف هذه التحديثات الأقدم.

عند اكتمال المهمة إجراء مزمنة Windows Update وحذف التحديثات القديمة، قد تظل قاعدة البيانات تحتوي على رموز تجزئة متعلقة بملفات التحديثات المحذوفة، بالإضافة إلى الملفات المقابلة في ملفات AllUsersProfile%\Application% Data\KasperskyLab\adminikit\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 ولحد 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. تحديث 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 9

املاً حقل الحساب وكلمة المرور لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

• الحساب 9

الحساب الذي يتم تشغيل المهمة من خلاله.

• كلمة المرور 9

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: 9

حدد الجدول الذي تعمل المهمة وفقاً له، وقم بتكوين الجدول المحدد.

• كل N ساعة 9

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• كل N يوماً 9

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 أسبوعاً 9

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 9

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.

• يومياً (التوقيت الصيفي غير مدعوم) 9

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.

• أسبوعياً

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. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهرياً

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.

• يدوياً

لا يتم تشغيل المهمة تلقائياً. يمكنك بدء تشغيلها يدوياً فقط. يتم تمكين هذا الخيار افتراضياً.

• مرة

يتم تشغيل المهمة مرة واحدة في التاريخ والوقت المحددين.

• كل شهر في أيام معينة من الأسابيع المحددة

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد. بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• 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 المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى 9

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار تشغيل الجهاز وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• تشغيل المهام الفائتة 9

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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرةً وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط. يتم تمكين هذا الخيار افتراضيًا.

• استخدام التأخير العشوائي لبدء المهام تلقائيًا 9

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 تبدأ 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) 9

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 ("*\<?>|"). تكون القيمة الافتراضية هي إجراء مزامنة لـ Windows Update.

الخطوة 8. إكمال إنشاء المهمة

في النافذة إنهاء عملية إنشاء المهمة، انقر فوق الزر إنهاء لإنهاء المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار 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 مهمة 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 طلب 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، فسيتم تحديث التطبيق.

يبدأ معالج إنشاء مهمة "تثبيت التحديثات وإصلاح الثغرات الأمنية". انتقل عبر المعالج من خلال استخدام زر **التالي**.

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 نَقَم بإعادة تشغيل الجهاز ⑤

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 ⑤

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 ⑤

سيتم عرض تنكير 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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضيًا.

• تكرار المطالبة كل (بالدقائق) ⑤

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) ⑤

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 ⑤

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 المستخدمون 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 المعالج **تكوين جدول المهمة**، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

• البدء المُجدول: ٤

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

• كل N ساعة: ٤

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• كل N يومًا: ٤

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: ٤

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: ٤

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): ٤

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: ٤

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• حسب أيام الأسبوع: ٤

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهريًا: ٤

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** ⑤

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.
يتم تمكين هذا الخيار افتراضيًا.

• **كل شهر في أيام معينة من الأسابيع المحددة** ⑤

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.
بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• **عند انتشار الفيروس** ⑤

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوفر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع المحيط
- مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.
قد ترغب في تشغيل مهام مختلفة وفقًا لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• **عند إكمال مهمة أخرى** ⑤

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار تشغيل الجهاز وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• **تشغيل المهام الفائتة** ⑤

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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.
يتم تمكين هذا الخيار افتراضيًا.

• **استخدم التأخير العشوائي لبدء المهام تلقائيًا** ⑤

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) [5]

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 المعالج إنهاء عملية إنشاء المهمة، انقر على زر إنهاء لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار تشغيل المهمة بعد انتهاء المعالج.

بعد قيام المعالج باستكمال عملياته، تظهر تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية في المجلد 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.

انتقل عبر المعالج من خلال استخدام زر التالي.

4. في الصفحة البحث عن مهام تثبيت التحديثات الموجودة، حدد الإعدادات التالية:

• البحث عن مهام تثبيت هذا التحديث [5]

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 افتراضياً.

• الموافقة على تثبيت التحديث 9

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 افتراضياً.

5. إذا اخترت البحث عن مهام تثبيت التحديث الحالية وإذا قام البحث باسترداد بعض المهام، فيمكنك عرض خصائص تلك المهام أو بدئهم يدوياً. 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 تدريجياً في حالة طلب 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، فسي فشل تحديث التطبيق.

يبدأ معالج إنشاء مهمة "تثبيت التحديثات وإصلاح الثغرات الأمنية". انتقل عبر المعالج من خلال استخدام زر التالي.

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 9

لم تتم إعادة تشغيل أجهزة العميل تلقائياً بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدوياً 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 أمراً بالغ الأهمية.

• أعد تشغيل الجهاز 9

يتم إعادة تشغيل الأجهزة العميلة تلقائياً دائماً 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 9

سيتم عرض تنذير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدوياً. 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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضياً.

• تكرار المطالبة كل (بالدقائق) 9

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد. يتم تمكين هذا الخيار افتراضياً. 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) 9

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد. يتم تمكين هذا الخيار افتراضياً. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

• فرض إغلاق التطبيقات في الجلسات المحظورة 9

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 الموقوف على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدم 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 الموقوفة يدوياً وإعادة تشغيل هذه الأجهزة. يتم تعطيل هذا الخيار افتراضياً.

9. في صفحة المعالج حدد الأجهزة التي سيتم تعيين المهمة لها، حدد أحد الخيارات التالية:

• حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة 9

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 يدوياً أو استيراد العناوين من القائمة 9

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 الحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

• تعيين مهمة إلى تحديد الجهاز 9

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 9

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.

10. في صفحة المعالج تكوين جدول المهمة، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

• البدء المُجدول: ٤

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

• كل N ساعة: ٤

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• كل N يومًا: ٤

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: ٤

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: ٤

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): ٤

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: ٤

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• حسب أيام الأسبوع: ٤

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهريًا: ٤

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 تمكين هذا الخيار افتراضياً.

• **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.
بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• **عند انتشار الفيروس**

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوفر أنواع التطبيق التالية:

• مكافحة الفيروسات لمحطات العمل وخوادم الملفات

• مكافحة الفيروسات للدفاع المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• **عند إكمال مهمة أخرى**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• **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 فوراً، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.

إذا تم تعطيل هذا الخيار، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفوراً، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تمكين هذا الخيار افتراضياً.

• **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) [5]

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 المعالج إنهاء عملية إنشاء المهمة، انقر على زر إنهاء لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار تشغيل المهمة بعد انتهاء المعالج.

عند انتهاء المعالج، يتم إنشاء المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وعرضها في المجلد المهام.

بالإضافة إلى الإعدادات التي تقوم بتحديددها 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 حالة

لتثبيت تحديث من خلال إضافة قاعدة لمهمة تثبيت حالة:

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.

انتقل عبر المعالج من خلال استخدام زر التالي.

4. في الصفحة البحث عن مهام تثبيت التحديثات الموجودة، حدد الإعدادات التالية:

• البحث عن مهام تثبيت هذا التحديث [5]

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 افتراضياً.

• الموافقة على تثبيت التحديث 9

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 افتراضياً.

5. إذا اخترت البحث عن مهام تثبيت التحديث الحالية وإذا قام البحث باسترداد بعض المهام، فيمكنك عرض خصائص تلك المهام أو بدئهم يدوياً. 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**.

أيضاً، يمكنك عرض خصائص المهام الحالية، أو بدئهم يدوياً، 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 تدريجياً في حالة طلب 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، فسي فشل 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 انقضاءها 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 الخاصة بالسياسة، 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 بدلاً 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 أولاً 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 العمل.

عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلاً 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 مركزياً.

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](#) 9

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 افتراضياً.

• [سلبى](#) 9

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](#) 9

إذا كان هذا الخيار مجدداً، 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**.

- 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 المثبتة على الأجهزة المُدارة، قم بتشغيل المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. عند اكتمال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المكتشفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة.

تم إنشاء المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائيًا بواسطة معالج البدء السريع لـ Kaspersky Security Center. إذا لم تشغّل "المعالج"، فابدأ تشغيله الآن أو أنشئ المهمة يدويًا.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [فحص التطبيقات بحثًا عن الثغرات الأمنية](#)، [جدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة](#)

- Kaspersky Security Center 14 Web Console: [إنشاء بحث عن الثغرات الأمنية والتحديثات المطلوبة المهمة](#)، [والبحث عن الثغرات الأمنية وإعدادات مهمة التحديثات المطلوبة](#)

2 تحليل قائمة الثغرات الأمنية المكتشفة 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 14 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 المُدارة باستخدام المهمة [تنصيب التحديثات المطلوبة وإصلاح الثغرات الأمنية](#) أو المهمة [إصلاح الثغرات الأمنية](#).

تُستخدم المهمة تنصيب 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 تنصيب 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 المهمة تنصيب التحديثات المطلوبة وإصلاح الثغرات الأمنية تحديثات البرامج الموصى بها.

المهمة إصلاح الثغرات الأمنية لا تتطلب 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.

- وحدة تحكم الإدارة: [تحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية، إصلاح الثغرات الأمنية في التطبيقات](#)
- [Kaspersky Security Center 14 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 جدول المهام

للتأكد من أن قائمة الثغرات الأمنية مُحدّثة دائماً، قم بجدولة المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة لتشغيلها تلقائياً 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 غالباً. 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 14 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 14 Web Console: إنشاء تقرير وعرضه](#)

8 التحقق من تكوين البحث عن الثغرات الأمنية 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

إذا أنشأت المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وكوّنتها، 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 لإصلاح 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](#).

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 المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة للعثور على الثغرات الأمنية بالبرامج.

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 تُحدّد 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 إصلاح ثغرات البرامج التي يمكنك استخدامها 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 لفحص الملفات بشكل تلقائي، كما تتضمن فحصًا مضادًا للفيروسات، 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 الموثوقة في مثل هذه التحديثات، بجانب عدم إجراء أنواع أخرى من تحليل التحديثات بخلاف ما هو محدد 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 العملية.

في المجلد خيارات متقدمة ← إدارة التطبيق في شجرة وحدة التحكم، حدد المجلد الفرعي الثغرات الأمنية بالبرنامج.

تعرض الصفحة قائمة بالثغرات الأمنية في التطبيقات المكتشفة على الأجهزة المُدارة.

للتغور 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. تُمثل الإحصاءات كمخطط. يعرض المخطط عدد الأجهزة بالحالات التالية:

• تم تجاهله على: <عدد الأجهزة>. يتم تعيين الحالة إذا عيّن يدويًا، في خصائص الثغرة الأمنية، الخيار لتجاهل الثغرات الأمنية.

• مثبت على: <عدد الأجهزة>. يتم تعيين الحالة إذا تم إكمال مهمة إصلاح الثغرات الأمنية بنجاح.

• الإصلاح مقرر في: <عدد الأجهزة>. يتم تعيين الحالة إذا كنت قد أنشأت المهمة لإصلاح الثغرات الأمنية لكن لم يتم تنفيذ المهمة بعد.

- التصحيح المطبق على: <عدد الأجهزة>. يتم تعيين الحالة إذا حددت تحديث برنامج يدويًا لإصلاح الثغرات الأمنية لكن هذا البرنامج الذي تم تحديثه لم يحل الثغرات الأمنية.

الإصلاح مطلوب في: <عدد الأجهزة>. يتم تعيين الحالة إذا تم إصلاح الثغرات الأمنية فقط من جانب الأجهزة المُدارة، وإذا كان مطلوبًا إصلاحها في الجزء المتبقي من الأجهزة المُدارة.

لعرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة:

1. في المجلد **خيارات متقدمة** ← **إدارة التطبيق** في شجرة 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، يُعرض 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 المثبتة 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 إنشاء مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة. انتقل عبر المعالج من خلال استخدام زر **التالي**.
3. في النافذة **تحديد نوع المهمة**، حدد **البحث عن الثغرات الأمنية والتحديثات المطلوبة**.
4. في صفحة المعالج **إعدادات**، 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 جهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

- **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 وكيل تحديث Windows على جهاز مُدار يستخدم المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها من مصدر تحديثات Microsoft في وقت سابق والمُخزّنة في الذاكرة المؤقتة للجهاز.

يمكن أن يكون الاتصال بمصدر تحديثات Microsoft مستهلكاً 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 عشوائياً في غضون 360 دقيقة.

يتم تمكين هذا الخيار افتراضياً.

يحدد مزيج الخيارات التالية لإعدادات سياسة وكلاء الشبكة طريقة الحصول على التحديثات:

• لا يتصل وكيل تحديث Windows على جهاز مُدار بخادم التحديث للحصول على التحديثات إلا في حالة تمكين الخيار **الاتصال بخادم التحديث لتحديث البيانات وتحديد الخيار نشط**، في مجموعة الإعدادات **وضع بحث تحديث Windows**.

• يستخدم وكيل تحديث Windows على جهاز مُدار المعلومات المتعلقة بتحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها مسبقاً من مصدر تحديثات Microsoft وتم تخزينها في الذاكرة المؤقتة للجهاز، في حالة تمكين خيار **الاتصال بخادم التحديث لتحديث البيانات وتحديد خيار سلبي**، في مجموعة الإعدادات **وضع بحث تحديث Windows**، أو في حالة تعطيل خيار **الاتصال بخادم التحديث لتحديث البيانات وتحديد خيار نشط** في مجموعة الإعدادات **وضع بحث تحديث Windows**.

• بغض النظر عن حالة الخيار **الاتصال بخادم التحديث لتحديث البيانات** (ممكّن أو معطل)، إذا تم تحديد الخيار **معطل**، في مجموعة الإعدادات **وضع بحث تحديث Windows**، لا يطلب Kaspersky Security Center أي معلومات حول 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 افتراضياً.

• **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 عمليات التتبع حتى وإن كان التتبع معطلاً لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الآخر؛ 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 وفقاً 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 لاحقاً 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 افتراضياً.

• الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت 5

القيمة الافتراضية هي 100 ميجابايت، وتكون 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 المعالج تكوين جدول المهمة، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

• البدء المُجدول: 5

حدد الجدول الذي تعمل المهمة وفقاً له، وقم بتكوين الجدول المحدد.

• كل N ساعة 5

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• كل N يوماً 5

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 أسبوعاً 5

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 5

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.

• يومياً (التوقيت الصيفي غير مدعوم) 5

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. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 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 تمكين 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، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• [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 المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• 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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تمكين 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 المترامنة 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 المترامنة 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 المعالج **إنهاء عملية إنشاء المهمة**، انقر على زر **إنهاء لإغلاق المعالج**.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج**.

بعد إنهاء المعالج عملياته، تظهر مهمة العثور على الثغرات الأمنية والتحديثات المطلوبة في قائمة المهام في المجلد الأجهزة المُدارة على علامة التبويب المهام.

بالإضافة إلى الإعدادات التي تقوم بتحديددها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

عند اكتمال مهمة العثور على الثغرات الأمنية والتحديثات المطلوبة، يعرض خادم الإدارة قائمة بالثغرات الأمنية التي تم العثور عليها في التطبيقات المثبتة على الجهاز؛ كما يعرض جميع تحديثات البرامج المطلوبة لإصلاح الثغرات الأمنية التي تم اكتشافها.

إذا كانت نتائج المهمة تحتوي على خطأ 0x80240033 وكيل تحديث Windows 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 وهما مهمة إجراء مزامنة Windows Update التي تم بها تعطيل الخيار **تنزيل ملفات التثبيت السريع**، ومهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة. ومن أجل عرض 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 العثور على الثغرات الأمنية والتحديثات المطلوبة على الأجهزة العملية.

يمكنك العثور على تفاصيل البرامج التابعة لجهة خارجية التي يمكن تحديثها عن طريق Kaspersky Security Center من خلال زيارة موقع خدمة الدعم الفني على صفحة Kaspersky Security Center في قسم **إدارة الخادم**.

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 وإصلاح الثغرات الأمنية المماثلة.

لإصلاح ثغرات أمنية تتوافق مع قواعد محددة:

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 إضافة المهمة. انتقل عبر المعالج من خلال استخدام زر التالي.

4. في صفحة المعالج تحديد نوع المهمة، حدد تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.

5. في صفحة المعالج إعدادات، 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 وفقاً لجدول زمني. استخدم هذا الخيار في حال كان تنزيل التحديثات قد يؤثر على أداء الجهاز. يتم تعطيل هذا الخيار افتراضياً.

• **تثبيت مكونات النظام العام المطلوبة**

إذا تم تمكين هذا الخيار، قبل تثبيت التحديث، يقوم التطبيق تلقائياً 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 يدوياً. يتم تعطيل هذا الخيار افتراضياً.

• **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 يدوياً 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 افتراضياً.

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 تلقائياً. بعد ذلك يمكنك تثبيت التحديثات التي تم تنزيلها يدوياً. 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 **مجلد تحميل التحديثات**. إذا تم تعطيل هذا الخيار، فسيتم تثبيت التحديثات على الجهاز تلقائياً. يتم تعطيل هذا الخيار افتراضياً.

• **مجلد تحميل التحديثات**

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 عمليات التتبع حتى وإن كان التتبع معطلًا لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الآخر؛ 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 %Temp%\WINDIR%. 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، وتكون 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.

6. 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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة 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) 9

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد. يتم تمكين هذا الخيار افتراضياً. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

• فرض إغلاق التطبيقات في الجلسات المحظورة 9

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 المستخدم 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 المستخدمون بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدوياً وإعادة تشغيل هذه الأجهزة. يتم تعطيل هذا الخيار افتراضياً.

7. في صفحة المعالج تكوين جدول المهمة، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

• البدء المُجدول: 9

حدد الجدول الذي تعمل المهمة وفقاً له، وقم بتكوين الجدول المحدد.

• كل N ساعة: 9

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• كل N يوماً: 9

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 أسبوعاً: 9

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: 9

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) 9

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 ⑤

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• حسب أيام الأسبوع ⑤

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهريًا ⑤

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 ⑤

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط. يتم تمكين هذا الخيار افتراضيًا.

• كل شهر في أيام معينة من الأسابيع المحددة ⑤

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد. بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• عند انتشار الفيروس ⑤

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوفر أنواع التطبيق التالية:

• مكافحة الفيروسات لمحطات العمل وخوادم الملفات

• مكافحة الفيروسات للدفاع المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقًا لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى ⑤

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• 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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط. يتم تمكين هذا الخيار افتراضيًا.

• استخدام 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 المترامنة 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 المترامنة 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.

8. 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 ("*\?>:\|").

9. في صفحة المعالج **إنهاء عملية إنشاء المهمة**، انقر على زر **إنهاء لإغلاق المعالج**.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار **تشغيل المهمة بعد انتهاء المعالج**.

بعد إنهاء المعالج عملياته، يتم إنشاء المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وعرضها في المجلد **المهام**.

بالإضافة إلى الإعدادات التي تقوم بتحديددها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

إذا كانت نتائج المهمة تحتوي على خطأ 0x80240033 وكيلا 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.

انتقل عبر المعالج من خلال استخدام زر التالي.

4. في النافذة البحث عن المهام الموجودة لإصلاح الثغرات الأمنية، حدد المعلمات التالية:

• **إظهار المهام التي تصلح هذه الثغرة الأمنية فقط** ④

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 افتراضياً.

• **الموافقة على التحديثات التي تستهدف إصلاح هذه الثغرات الأمنية** ④

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 افتراضياً.

5. إذا اخترت البحث عن مهام إصلاح الثغرات الأمنية الحالية وإذا قام البحث باسترداد بعض المهام، فيمكنك عرض خصائص تلك المهام أو بدئهم يدوياً. 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 تدريجياً في حالة طلب 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، فسي فشل تحديث التطبيق.

يبدأ معالج إنشاء مهمة "تثبيت التحديثات وإصلاح الثغرات الأمنية". انتقل عبر المعالج من خلال استخدام زر التالي.

8. في صفحة المعالج تحديد خيار إعادة تشغيل نظام التشغيل، حدد الإجراء الذي سيتم اتخاذه عندما يلزم إعادة تشغيل نظام التشغيل على الأجهزة العملية بعد عملية التشغيل:

• **لا تقم بإعادة تشغيل الجهاز** ④

لم تتم إعادة تشغيل أجهزة العميل تلقائياً بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدوياً 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 أمراً بالغ الأهمية.

• **أعد تشغيل الجهاز** ④

يتم إعادة تشغيل الأجهزة العملية تلقائياً دائماً 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** ④

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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضيًا.

• **تكرار المطالبة كل (بالدقائق) 5**

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) 5**

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 5**

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 المقبول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدم 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، حدد أحد الخيارات التالية:

• **حدد الأجهزة المتصلة بالشبكة والتي تم اكتشافها بواسطة خادم الإدارة 5**

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 5**

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 الحاسبين أو لفحص أجهزة في شبكة فرعية من المحتمل إصابتها.

• **تعيين مهمة إلى تحديد الجهاز 5**

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 5**

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.

10. في صفحة المعالج تكوين جدول المهمة، يمكنك إنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

• **البدء المُجدول:** ④

حدد الجدول الذي تعمل المهمة وفقاً له، وقم بتكوين الجدول المحدد.

• **كل N ساعة:** ④

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• **كل N يوماً:** ④

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 أسبوعاً:** ④

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:** ④

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.

• **يوماً (التوقيت الصيفي غير مدعوم):** ④

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.

• **أسبوعياً:** ④

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• **حسب أيام الأسبوع:** ④

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.
بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهرياً ⑤

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.

• يدياً ⑤

لا يتم تشغيل المهمة تلقائياً. يمكنك بدء تشغيلها يدوياً فقط.
يتم تمكين هذا الخيار افتراضياً.

• كل شهر في أيام معينة من الأسابيع المحددة ⑤

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.
بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• عند انتشار الفيروس ⑤

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوفر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وحوادم الملفات
- مكافحة الفيروسات للدفاع المحيط
- مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.
قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى ⑤

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• تشغيل المهام الفائتة ⑤

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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط. يتم تمكين 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 المترامنة 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 المترامنة 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 المعالج إنهاء عملية إنشاء المهمة، انقر على زر إنهاء لإغلاق المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار تشغيل المهمة بعد انتهاء المعالج.

عند انتهاء المعالج، يتم إنشاء المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وعرضها في المجلد المهام.

بالإضافة إلى الإعدادات التي تقوم بتحديددها 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.

انتقل عبر المعالج من خلال استخدام زر التالي.

4. في النافذة البحث عن المهام الموجودة لإصلاح الثغرات الأمنية، حدد المعلمات التالية:

• **إظهار المهام التي تصلح هذه الثغرة الأمنية فقط** 5

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، فسيطلبك معالج إصلاح الثغرات الأمنية بإنشاء قاعدة أو مهمة لإصلاح الثغرات الأمنية. يتم تمكين هذا الخيار افتراضياً.

• **الموافقة على التحديثات التي تستهدف إصلاح هذه الثغرات الأمنية** 5

سنتم 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 افتراضياً.

5. إذا اخترت البحث عن مهام إصلاح الثغرات الأمنية الحالية وإذا قام البحث باسترداد بعض المهام، فيمكنك عرض خصائص تلك المهام أو بدئهم يدوياً. 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.

أيضاً، يمكنك عرض خصائص المهام الحالية، أو بدئهم يدوياً، 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 تدريجياً في حالة طلب 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، فسي فشل 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 المدارة 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.

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

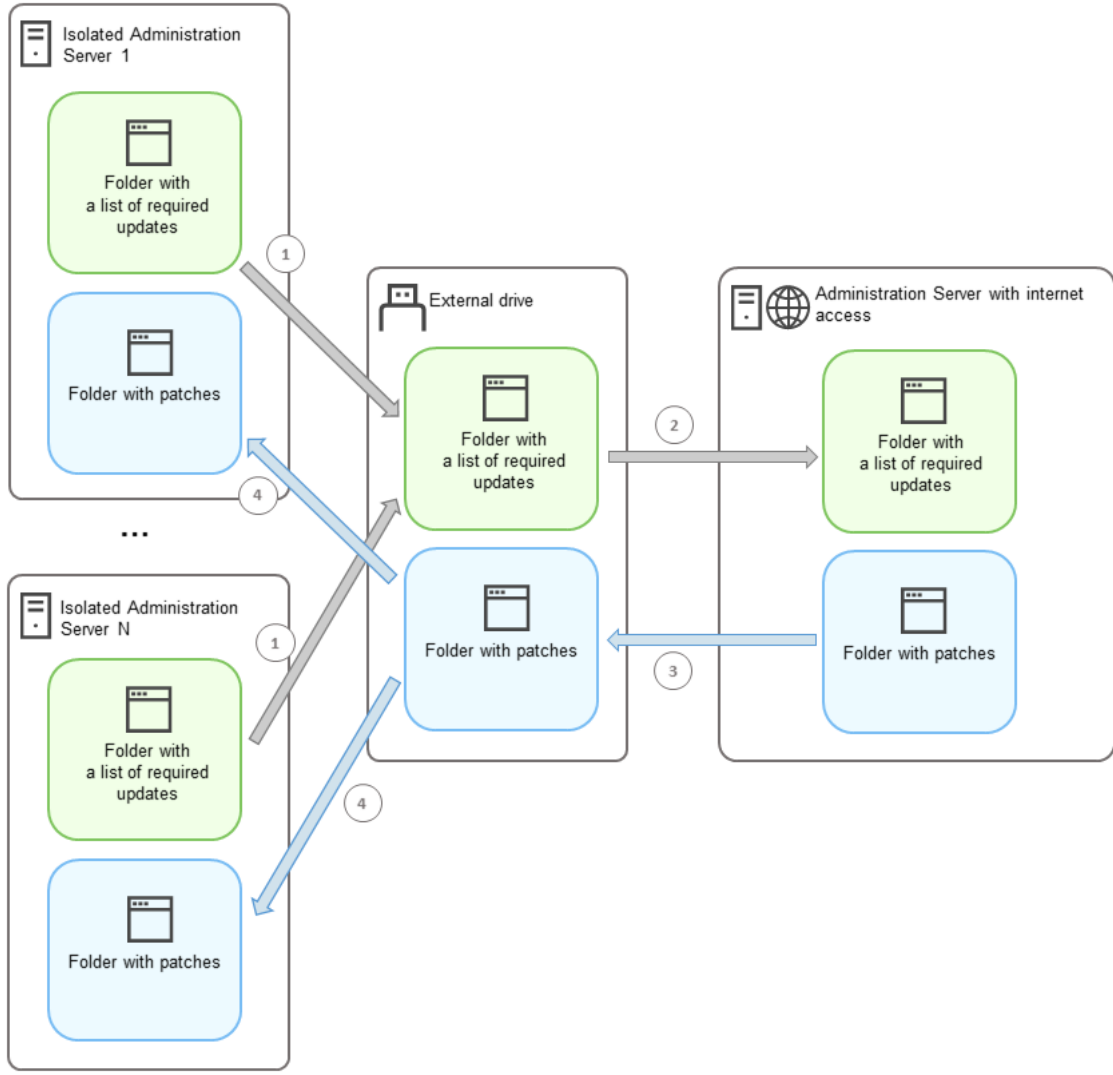
بعد الانتهاء من تكوين خوادم الإدارة، يمكنك إرسال قوائم التحديثات والتصحيحات المطلوبة بين خادم الإدارة مع الوصول إلى الإنترنت وخوادم الإدارة المعزولة. بعد ذلك، سيتم تثبيت التحديثات من التصحيحات على الأجهزة المدارة باستخدام مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.

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 المُدارة 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 klsccflag لكتابة المسارات إلى المجلدات في خصائص خادم الإدارة. أدخل الأمر التالي في موجه أوامر Windows، باستخدام حقوق المسؤول:

• لتعيين المسار إلى مجلد التصحيحات:

```
klsccflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v  
" >المسار الخاص  
بالمجلد <"
```

• لتعيين مسار المجلد للحصول على قائمة بالتحديثات المطلوبة:

```
klsccflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v  
" >المسار الخاص  
بالمجلد <"
```

مثال: "klsccflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\FolderForPatches

4. [اختياري] استخدم الأداة المساعدة klsccflag لتحديد عدد المرات التي يجب أن يتحقق فيها خادم الإدارة من طلبات التصحيح الجديدة:
klsccflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <القيمة بالثواني >
القيمة الافتراضية هي 120 ثانية.

مثال: klsccflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150

5. 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 klsccflag لكتابة المسارات إلى المجلدات في خصائص خادم الإدارة. أدخل الأمر التالي في موجه أوامر Windows، باستخدام حقوق المسؤول:

• لتعيين المسار إلى مجلد التصحيحات:

بالمجلد <" klschcflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v
المسار الخاص

• لتعيين مسار المجلد للحصول على قائمة بالتحديثات المطلوبة:

بالمجلد <" klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v
المسار الخاص

مثال: "klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\FolderForPatches

5. [اختياري] 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.

Example: klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150

6. [اختياري] استخدم الأداة المساعدة klscflag لحساب تجزئات SHA-256 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 وأنها قد تلتفت التصحيحات الصحيحة التي تحتوي على التحديثات المطلوبة.

افتراضياً، لا يحسب Kaspersky Security Center تجزئة SHA-256 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 وسيتم عليك استبدال التصحيحات غير الصحيحة.

7. قم بإنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة وتعيين جدول المهام. قم بتشغيل المهمة إذا كنت تريد تشغيلها في وقت أبكر مما هو محدد في جدول المهام.

8. قم بإعادة تشغيل خدمة خادم الإدارة.

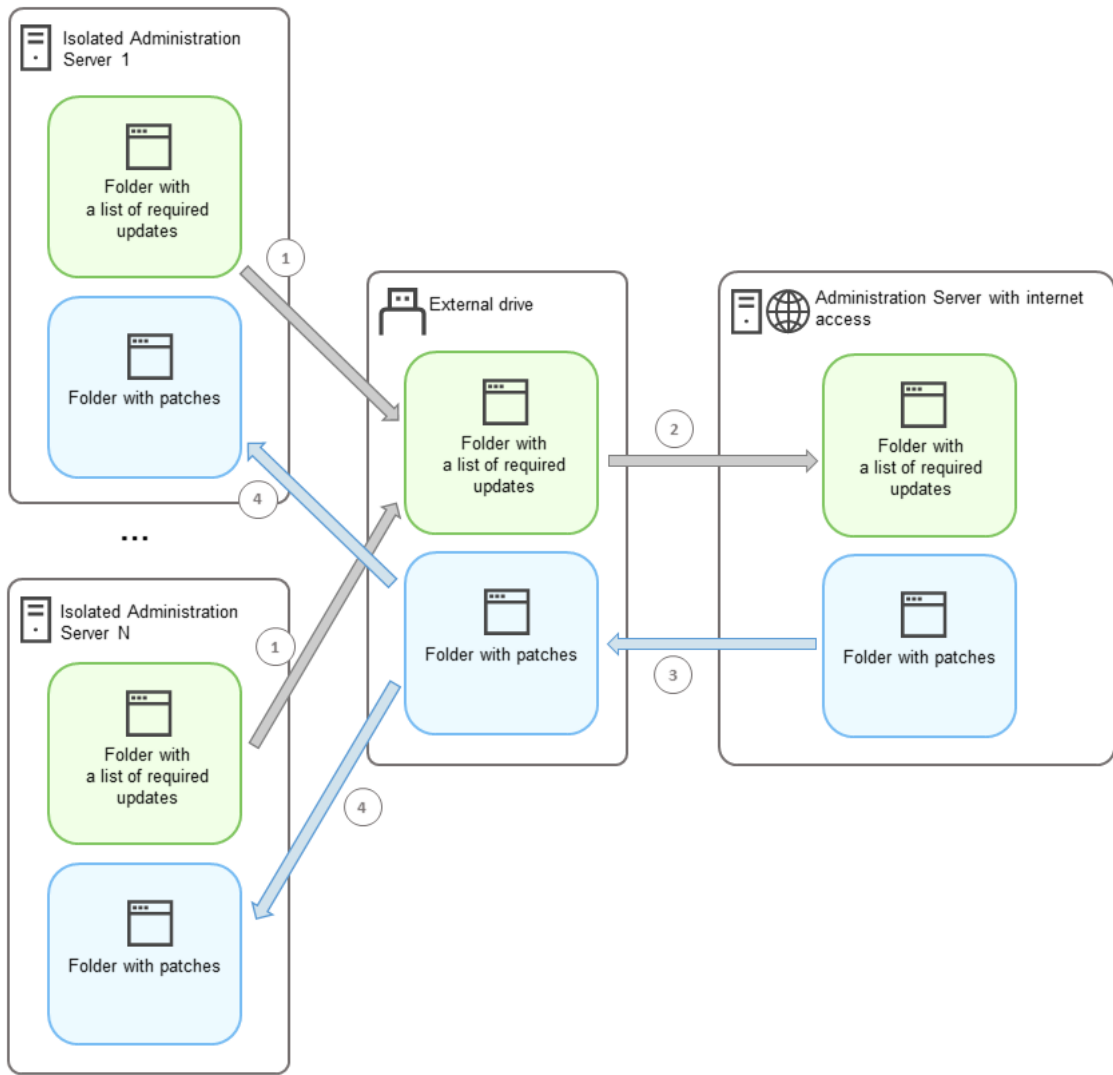
بعد تكوين جميع خوادم الإدارة، يمكنك نقل التصحيحات وقوائم التحديثات المطلوبة، وإصلاح الثغرات الأمنية بالبرامج الناجمة عن جهات خارجية على الأجهزة المدارة في الشبكة المعزولة.

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

لتنصيب 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. وصل 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 بحثاً 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.

أدخل الأمر التالي في موجه أوامر Windows، باستخدام حقوق المسؤول:

- لحذف المسار إلى مجلد التصحيحات:

```
"" klsclflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v
```

- لحذف مسار المجلد للحصول على قائمة بالتحديثات المطلوبة:

```
"" klsclflag -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:

```
"" klshclflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v
```

- لحذف مسار المجلد للحصول على قائمة بالتحديثات المطلوبة:

```
"" klsclflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v
```

4. أعد تشغيل خدمة كل خادم إدارة قمت بحذف المسارات إلى المجلدات عليه.

نتيجة 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 الثغرة الأمنية بالبرامج مشكلة حرجة بمؤسستك.
- 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 المُدارة المحددة فقط.

لتجاهل ثغرة أمنية في البرامج على جميع الأجهزة المُدارة:

1. في المجلد **خيارات متقدمة** ← **إدارة التطبيق** في شجرة 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 المُحدّد.

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 استبعاد الثغرات الأمنية بالبرامج التي تم تجاهلها من قائمة الثغرات الأمنية من خلال عامل التصفية.

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 لبرنامج Microsoft وإصلاحات المستخدم لبرامج الجهات الخارجية الأخرى. إصلاحات المستخدم هي تحديثات للبرامج لإصلاح الثغرات الأمنية التي يحددها المسؤول يدويًا للتنصيب.

لتحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية:

1. في المجلد **خيارات متقدمة** ← **إدارة التطبيق** في شجرة 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 قسم **إصلاحات المستخدم وإصلاحات أخرى**، انقر على زر **إضافة**.
يتم عرض قائمة حزم التنصيب المتاحة. تتوافق قائمة حزم التنصيب المعروضة مع القائمة **التنصيب عن بُعد** ← **حزم التنصيب**. إذا لم تقم بإنشاء حزمة تنصيب تحتوي على إصلاح مستخدم لثغرة أمنية محددة، فيمكنك إنشاء الحزمة الآن عن طريق بدء معالج حزمة جديدة.
5. حدد حزمة (أو حزم) تنصيب تحتوي على إصلاح مستخدم (أو إصلاحات مستخدم) لثغرة أمنية في برنامج تابع لجهة خارجية.
6. انقر على **موافق**.
يتم تحديد حزم التنصيب التي تحتوي على إصلاحات للمستخدم للثغرات الأمنية في البرامج. عند بدء المهمة إصلاح الثغرات الأمنية، سيتم تنصيب حزمة التنصيب وإصلاح الثغرات الأمنية في البرامج.

قواعد لتنصيب التحديثات

عند **إصلاح الثغرات الأمنية في التطبيقات**، يجب عليك تحديد القواعد لتنصيب التحديثات. تحدد هذه القواعد التحديثات المراد تنصيبها 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 Microsoft وKaspersky) أو لجميع التطبيقات. عند إنشاء قاعدة لتطبيقات Microsoft أو تطبيقات الجهات الخارجية، يمكنك تحديد تطبيقات وإصدارات تطبيق معينة ترغب في تنصيب التحديثات من أجلها. عند إنشاء قاعدة لجميع التطبيقات، يمكنك تحديد تحديثات معينة ترغب في تنصيبها وثغرات أمنية ترغب في إصلاحها عن طريق تنصيب التحديثات.

قم بما يلي لإنشاء قاعدة جديدة لتحديثات جميع التطبيقات:

1. في الصفحة **إعدادات الخاصة** بإضافة معالج المهمة، انقر فوق الزر **إضافة**.
يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.
2. في الصفحة **نوع القاعدة**، حدد **قاعدة لجميع التحديثات**.
3. في الصفحة **معايير عامة**، قم باستخدام القوائم المنسدلة لتحديد الإعدادات التالية:

- **مجموعة التحديثات المراد تنصيبها** 5

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 5**

قد تؤثر تحديثات البرامج في بعض الأحيان سلبًا 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 5**

تثبيت جميع تحديثات البرامج التي تتوافق مع المعايير المحددة في الصفحة معايير عامة بالمعالج. يتم تحديده بصورة افتراضية.

• **تثبيت التحديثات من القائمة فقط 5**

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 5**

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، فسيُفشل 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 5**

إصلاح جميع الثغرات الأمنية التي تتوافق مع المعايير المحددة في الصفحة معايير عامة بالمعالج. يتم تحديده بصورة افتراضية.

• إصلاح الثغرات الأمنية من القائمة فقط ⑤

قم بإصلاح الثغرات الأمنية التي تحددها بدويًا 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 قيام معالج إنشاء القاعدة باستكمال عملياته، يتم إنشاء القاعدة الجديدة وعرضها في الحقل **حدد قواعد لتثبيت التحديثات الخاص** بإضافة معالج المهمة.

قم بما يلي لإنشاء قاعدة جديدة لتحديثات تطبيقات Microsoft:

1. في الصفحة **إعدادات الخاصة** بإضافة معالج المهمة، انقر فوق 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 **معايير عامة**، حدد الإعدادات التالية:

• مجموعة التحديثات المراد تثبيتها ⑤

حدد التحديثات التي يجب تثبيتها على الأجهزة العملية:

• **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 ⑤

قد تؤثر تحديثات البرامج في بعض الأحيان سلبًا 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 ⑤

قد تؤثر تحديثات البرامج في بعض الأحيان سلبًا 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 افتراضياً.

5. في الصفحة **فئات التحديثات**، حدد فئات التحديثات المطلوب تثبيتها. هذه الفئات هي نفس الفئات الموجودة في Microsoft Update Catalog. يتم تحديد جميع الفئات افتراضياً.

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 قيام المعالج باستكمال عملياته، يتم إنشاء القاعدة الجديدة وعرضها في الحقل **حدد قواعد تثبيت التحديثات الخاص بإضافة معالج المهمة**.

قم بما يلي لإنشاء قاعدة جديدة لتحديثات تطبيقات الجهات الخارجية:

1. في الصفحة **إعدادات الخاصة بإضافة معالج المهمة**، انقر فوق 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 **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 سلباً 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 مساوياً 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 افتراضياً.

4. في الصفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضياً.

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 قيام المعالج باستكمال عملياته، يتم إنشاء القاعدة الجديدة وعرضها في الحقل **حدد قواعد تثبيت التحديثات الخاص بإضافة معالج المهمة**.

مجموعات التطبيقات

يوضح هذا القسم كيفية إدارة مجموعات التطبيقات المثبتة على الأجهزة.

يسمح لك Kaspersky Security Center بإنشاء فئات التطبيقات المثبتة على الأجهزة العملية.

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

يتيح لك Kaspersky Security Center القيام بإجراء جرد لمخزون البرامج على الأجهزة التي تعمل بنظام Windows. يقوم عميل الشبكة باستعادة معلومات حول 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 150000 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. تشمل 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 معلوماتي على خادم الإدارة.

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**.

السيناريو: إدارة التطبيق

يمكنك إدارة بدء التطبيقات على أجهزة المستخدم. يمكنك السماح للتطبيقات بالعمل على الأجهزة المُدارة أو حظرها من العمل عليها. يمكن تحقيق هذه الوظيفة من خلال مكون التحكم في التطبيقات. يمكنك إدارة التطبيقات المثبتة على أجهزة Windows فقط.

المتطلبات الأساسية

- يتم نشر Kaspersky Security Center في مؤسستك.
- من ضمن الأجهزة المُدارة في مؤسستك، يوجد أجهزة تعمل بنظام Windows.
- تم إنشاء سياسة Kaspersky Endpoint Security for Windows ونشطة.

المراحل

يسير سيناريو استخدام التحكم في التطبيقات في مراحل:

1 تشكيل قائمة بالتطبيقات على أجهزة العميل وعرضها

تساعدك هذه المرحلة في معرفة التطبيقات المثبتة على الأجهزة المُدارة. يمكنك عرض قائمة التطبيقات وتحديد التطبيقات التي ترغب في السماح لها والتطبيقات التي ترغب في حظرها وفق سياسات أمان مؤسستك. يمكن أن تكون القيود متعلقة بسياسات أمان المعلومات في مؤسستك. يمكنك تخطي هذه المرحلة إذا كنت تعرف تمامًا التطبيقات المثبتة على الأجهزة المُدارة.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [عرض سجل التطبيقات](#)

○ Kaspersky Security Center 14 Web Console: [الحصول على قائمة بالتطبيقات المثبتة على أجهزة العميل وعرضها](#)

2 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. يمكنك تخطي هذه المرحلة إذا كنت تعرف تمامًا الملفات التنفيذية المثبتة على الأجهزة المُدارة.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [مخزون الملفات التنفيذية](#)

○ Kaspersky Security Center 14 Web Console: [الحصول على قائمة الملفات التنفيذية المخزنة على أجهزة العميل وعرضها](#)

3 إنشاء فئات التطبيقات للتطبيقات المستخدمة في مؤسستك

قم بتحليل قوائم التطبيقات والملفات التنفيذية المخزنة على الأجهزة المُدارة. أنشئ فئات التطبيقات بناءً على التحليل. من الموصى به إنشاء فئة "تطبيقات العمل" تغطي المجموعة القياسية من التطبيقات المستخدمة في مؤسستك. في حال وجود مجموعات مستخدمين مختلفة تستخدم مجموعات مختلفة من التطبيقات في أعمالهم، يمكن إنشاء فئة تطبيق منفصلة لكل مجموعة مستخدم.

يمكنك إنشاء فئات التطبيقات من ثلاثة أنواع، ويعتمد ذلك على مجموعة المعايير لإنشاء فئة تطبيق.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: إنشاء فئات التطبيق من أجل سياسات [Kaspersky Endpoint Security for Windows](#)، إنشاء فئة تطبيق مضافاً إليها المحتوى يدويًا، إنشاء فئة تطبيق مضافاً إليها المحتوى تلقائيًا

○ [Kaspersky Security Center 14 Web Console](#): إنشاء فئة تطبيق مضافاً إليها المحتوى يدويًا، إنشاء فئة تطبيق تتضمن ملفات تنفيذية من أجهزة محددة، إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد

4 تكوين التحكم في التطبيقات في سياسة [Kaspersky Endpoint Security for Windows](#)

تكوين مكون التحكم في التطبيقات في سياسة [Kaspersky Endpoint Security for Windows](#) باستخدام فئات التطبيق التي قد أنشأتها في المرحلة السابقة.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [تكوين إدارة بدء تشغيل التطبيق على أجهزة العميل](#)

○ [Kaspersky Security Center 14 Web Console](#): [تكوين التحكم في التطبيقات في سياسة \[Kaspersky Endpoint Security for Windows\]\(#\)](#).

5 تشغيل مكون التحكم في التطبيقات في وضع الاختبار

لضمان أن قواعد التحكم في التطبيقات لا تحظر التطبيقات المطلوبة لعمل المستخدم، يُنصح بتفعيل اختبار قواعد التحكم في التطبيقات وتحليل عملها بعد إنشاء قواعد جديدة. عند تفعيل الاختبار، [Kaspersky Endpoint Security for Windows](#) لن يحظر التطبيقات الممنوع أن تبدأ بقواعد التحكم في التطبيقات، لكن بدلاً من ذلك سوف يرسل إخطارات عن بدئها 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 14 Web Console](#): [تكوين مكون التحكم في التطبيقات في سياسة \[Kaspersky Endpoint Security\]\(#\)](#). اتبع هذه التعليمات وقم بتفعيل خيار وضع الاختبار في عملية التكوين.

6 تغيير إعدادات فئات التطبيق لمكون التحكم في التطبيقات

أجر تغييرات في إعدادات التحكم في التطبيقات عند الضرورة بناءً على نتائج الاختبار، يمكنك إضافة ملفات تنفيذية متعلقة بأحداث مكون التحكم في التطبيقات إلى فئة تطبيق مضاف إليها المحتوى يدويًا.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق](#)

○ [Kaspersky Security Center 14 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 فئات التطبيق، يمكنك تطبيق قواعد التحكم في التطبيقات في وضع التشغيل.

تعليمات إرشادات [Kaspersky Security Center 14 Web Console](#): [تكوين مكون التحكم في التطبيقات في سياسة \[Kaspersky Endpoint Security\]\(#\)](#). 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 التطبيقات.

○ قم بتكوين التحكم في التطبيقات باستخدام فئات التطبيقات.

○ قد طبقت قواعد التحكم في التطبيقات في وضع التشغيل.

عند اكتمال السيناريو، يتم التحكم في بدء تشغيل التطبيقات على الأجهزة المُدارة. لا يمكن للمستخدمين تشغيل إلا تلك التطبيقات المسموح بتشغيلها في مؤسستك ولا يمكنهم تشغيل التطبيقات المحظورة في مؤسستك.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى [التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows](#) و [Kaspersky Security for Virtualization Light Agent](#).

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 المجلد **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 و COM و DLL و SYS و BAT و PS1 و CMD و JS و VBS و REG و MSI و MSC و CPL و HTML و HTM و DRV و OXC و SCR.

- **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**.

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 **المجلد 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 والإجراء**، 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 وCPL 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

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 فئة المعالج الجديدة.

3. في صفحة المعالج، حدد الفئة المضاف إليها المحتوى يدويًا كنوع فئة المستخدم.

4. في الصفحة تهيئة الشروط لإدراج التطبيقات في الفئات، انقر فوق الزر **إضافة**.

5. 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.

• **البيانات الوصفية لملفات مُثَبَّت MSI**

إذا تم تحديد هذا الخيار ، يمكنك تحديد ملف مُثَبَّت MSI كشرط لإضافة تطبيقات إلى فئة المستخدم. وسيتم إرسال البيانات الوصفية لمُثَبَّت التطبيق إلى خادم الإدارة. تتم إضافة التطبيقات التي تشبه فيها البيانات الوصفية للمُثَبَّت MSI المحدد إلى فئة تطبيقات المستخدم.

• **المجاميع الاختبارية لملفات من مُثَبَّت MSI الخاص بالتطبيق**

إذا تم تحديد هذا الخيار ، يمكنك تحديد ملف مُثَبَّت MSI كشرط لإضافة تطبيقات إلى فئة المستخدم. سيتم إرسال تجزئة ملفات مُثَبَّت 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.

• **مجلد التطبيق**

إذا تم تحديد هذا الخيار ، فيمكنك تحديد المسار المؤدي إلى المجلد الموجود على الجهاز العميل الذي يحتوي على الملفات التنفيذية المراد إضافتها إلى فئة تطبيقات المستخدم.

• **تحديد شهادة من المستودع**

إذا تم تحديد هذا الخيار ، فيمكنك تحديد الشهادات من وحدة التخزين. ستتم إضافة الملفات التنفيذية التي تم توقيعها وفقًا للشهادات المحددة إلى فئة المستخدم.

• **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.

6. اتبع إرشادات المعالج.

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، مضافاً إليها المحتوى يدوياً. يمكنك عرض الفئة التي تم إنشاؤها حديثاً باستخدام قائمة الفئات الموجودة في مساحة عمل المجلد فئات التطبيق.

إنشاء فئة تطبيق مضافاً إليها المحتوى تلقائياً

لإنشاء فئة تطبيق مضافاً إليها المحتوى تلقائياً:

1. من شجرة وحدة التحكم، في المجلد خيارات متقدمة ← إدارة التطبيق حدد المجلد الفرعي فئات التطبيق.
2. انقر فوق الزر فئة جديدة لتشغيل معالج الفئة الجديدة.
في نافذة المعالج، حدد الفئة المضاف إليها المحتوى تلقائياً كنوع فئة المستخدم.
3. في النافذة مجلد المستودع حدد الإعدادات ذات الصلة:

• مسار للمجلد للإضافة التلقائية لمحتوى الفئة

حدد، في هذا الحقل، مساراً إلى المجلد حيث سيبحث خادم الإدارة فيه عن الملفات التنفيذية بشكل منتظم. يتم تحديد المسار إلى هذا المجلد عند إنشاء الفئة. لا يمكن تغيير المسار إلى هذا المجلد.

• تضمين مكتبات الروابط الديناميكية (DLL) في هذه الفئة

تشمل فئة التطبيق مكتبات الروابط الديناميكية (ملفات بتنسيق DLL)، ويسجل مكون التحكم في التطبيقات الإجراءات التي تقوم هذه المكتبات بتنفيذها في النظام. قد يؤدي تضمين ملفات DLL في الفئة إلى خفض أداء Kaspersky Security Center.
تكون خانة الاختيار غير محددة بشكل افتراضي.

• تضمين بيانات البرنامج النصي في هذه الفئة

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 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 حفظ المعلومات حول قيم التجزئة المحسوبة في قاعدة بيانات خادم الإدارة. لا يؤدي تخزين قيم التجزئة إلى زيادة حجم قاعدة البيانات بقدر كبير.

SHA-256 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 SHA-256. 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 إصدارات Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو إصدارات أحدث، فحدد خانة الاختيار حساب SHA-256 للملفات في هذه الفئة (مدعوم بواسطة Kaspersky Endpoint Security 10 Service Pack 2 for Windows وأي إصدارات أحدث). لا ننصحك بإضافة أي فئات تم إنشاؤها وفقاً لمعيار مجموع تجزئة SHA-256 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 للملفات الفئة.

- إذا تم تثبيت أي إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows في شبكتك، فحدد حساب MD5 للملفات في هذه الفئة (مدعوم بواسطة إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows). 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 SHA-256 للملفات الفئة.

في حالة استخدام الأجهزة المختلفة في شبكتك لكل من الإصدارات الأقدم والأحدث من Kaspersky Endpoint Security 10، فقم بتحديد خانة الاختيار حساب SHA-256 للملفات في هذه الفئة وخانة الاختيار حساب MD5 للملفات في هذه الفئة.

يتم تحديد خانة الاختيار حساب SHA-256 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.

• فرض فحص المجلد للتغييرات ④

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 تحقيقات من المجلد. يحاول الخادم الوصول إلى الملفات إذا تم تعديلها أو إضافتها أو حذفها. يتم تعطيل هذا الخيار افتراضياً.

• فرض فحص المجلد للتغييرات ④

في هذا الحقل، يمكنك تحديد الفاصل الزمني (بالساعات) والذي سيبدأ التطبيق بعده بالتحقق الإجباري من التغييرات بالمجلد الخاصة بالإضافة التلقائية لمحتوى الفئة. وبشكل افتراضي، يكون الفاصل الزمني بين الفحوصات الإجبارية هو 24 ساعة. يتوفر هذا الحقل إذا تم تحديد خانة الاختيار فرض فحص المجلد للتغييرات. تكون خانة الاختيار غير محددة بشكل افتراضي.

4. اتبع إرشادات المعالج.

عند اكتمال المعالج، يتم إنشاء فئة التطبيق المضاف إليها المحتوى تلقائياً. يمكنك عرض الفئة التي تم إنشاؤها حديثاً باستخدام قائمة الفئات الموجودة في مساحة عمل المجلد فئات التطبيق.

إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق

يمكنك إضافة الملفات التنفيذية المتعلقة بأحداث تم حظر بدء تشغيل التطبيق وتم 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 إنشاء فئة مستخدم. 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 SHA-256 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 SHA-256 فريدة خاصة به. عندما تحديد وظيفة تجزئة SHA-256، 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 SHA-256 للملفات بدون شهادة).
يتم تحديد هذا الخيار افتراضيًا.

• تفاصيل الشهادة (سيتم تخطي الملفات التي لا يوجد لديها شهادة) ⑤

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.

• SHA-256 فقط (سيتم تخطي الملفات التي يوجد لديها SHA-256) ⑤

كل ملف لديه وظيفة تجزئة SHA-256 فريدة خاصة به. عندما تحديد وظيفة تجزئة SHA-256، ينتهي ملف مقابل واحد على سبيل المثال، إصدار التطبيق المحدد، إلى الفئة. حدد هذا الخيار إذا كنت ترغب بإضافة فقط تفاصيل وظيفة تجزئة SHA-256 الخاصة بالملف التنفيذي.

• MD5 فقط (وضع الإيقاف، فقط لإصدار Kaspersky Endpoint Security 10 Service Pack 1) ⑤

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 العملية

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 وفقاً إلى قاعدة التحكم في التطبيقات. يمكنك إنشاء فئة ذات محتوى مضاف تلقائياً بناءً على معايير مختلفة من مجلد محدد. في هذه الحالة، يتم إضافة الملفات تلقائياً إلى الفئة من المجلد المحدد. يتم نسخ الملفات التنفيذية للتطبيقات إلى المجلد المحدد ومعالجتها تلقائياً؛ كما يتم إضافة مقابليها إلى الفئة.

لتكوين إدارة بدء التطبيقات على الأجهزة العملية:

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 زر سياسة جديدة لإنشاء سياسة جديدة لـ 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 حديثاً 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 نصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار تجزئة SHA-256 الخاص بالملف التنفيذي لإصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2. 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 المضمنة في الفئة المحددة طبقًا للقاعدة التي قمت بإنشائها. 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.

ستفتح 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 المضمنة في فئة التطبيق.

عرض سجل التطبيقات

يقوم Kaspersky Security Center بتخزين جميع البرامج المثبتة على الأجهزة المدارة.

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.

لعرض سجل التطبيقات المثبتة على الأجهزة العملية،

في المجلد خيارات متقدمة ← إدارة التطبيق بشجرة وحدة التحكم، حدد المجلد الفرعي سجل التطبيقات.

تعرض مساحة عمل مجلد سجل التطبيقات قائمة بالتطبيقات المثبتة على الأجهزة العملية و خادم 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 التبويب 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 وافترضية.

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:

• لنظام 64 بت:

/_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags

• لنظام 32 بت:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags

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 بمتابعة 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 انتهاء القيود التالية وتعبئها:

• 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 حقيقياً أم لا. يمكنك فقط تتبع القيود التي تحددها. في حالة انتهاك أحد القيود التي تفرضها على مفتاح الترخيص، وخدام 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 والبيانات 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 والتصحیحات في نافذة **تكوين الواجهة**.

إنشاء مجموعات التطبيقات المرخصة

لإنشاء مجموعة تطبيقات مرخصة:

1. في المجلد **خيارات متقدمة – إدارة التطبيق** في شجرة 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**:

- حدث إعلامي: سيتم تجاوز حد عمليات التثبيت قريباً (تم استهلاك أكثر من 95%) لأحدى مجموعات التطبيقات المرخصة
 - حدث تحذيري: سيتم تجاوز حد عمليات التثبيت لإحدى مجموعات التطبيقات المرخصة قريباً
 - 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 المجلد خيارات متقدمة ← إدارة التطبيق في شجرة وحدة التحكم، حدد المجلد الفرعي استخدام تراخيص الجهات الخارجية.

2. في مساحة عمل مجلد استخدام تراخيص الجهات الخارجية، انقر على زر إدارة المفاتيح المتعلقة بالتطبيقات المرخصة. ستفتح نافذة إدارة المفتاح في التطبيقات المرخصة.

3. في النافذة إدارة المفتاح في التطبيقات المرخصة، انقر فوق الزر إضافة. ستفتح 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 المجلد خيارات متقدمة ← إدارة التطبيق في شجرة 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 استخدام مهمة المخزون لتنفيذ مخزون الملفات التنفيذية على الأجهزة العميلة. يوفر Kaspersky Endpoint Security 10 for Windows والإصدارات الأحدث ميزة جرد الملفات التنفيذية.

لا يمكن أن يتجاوز عدد الملفات التنفيذية التي تم استلامها من جهاز مفرد 150000 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 وكيل 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 وكيل الشبكة وقم بما يلي:

1. انتقل إلى إعدادات التطبيق ← 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. بالنقر فوق الزر مهمة جديدة في مساحة عمل المجلد المهام.

يبدأ تشغيل معالج إضافة مهمة.

3. في النافذة تحديد نوع المهمة الخاصة بالمعالج، حدد Kaspersky Endpoint Security كنوع المهمة، ثم حدد Inventory كنوع فرعي للمهمة وانقر فوق التالي.

4. اتبع بقية إرشادات المعالج.

بعد انتهاء المعالج، يتم إنشاء مهمة مخزون لـ Kaspersky Endpoint Security. يتم عرض المهمة التي تم إنشاؤها حديثاً 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 لـ 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 لتناسب 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 عرضاً على الشاشة يتضمن مجموعات الأحداث المُسمَّاة المحددة من قاعدة بيانات خادم الإدارة. يتم تجميع مجموعات الأحداث هذه وفقاً للفئات التالية:

- حسب مستوى الأهمية—أحداث حرجة، وحالات الخلل الوظيفي، وتحذيرات، ومعلومات عن الأحداث

• حسب الوقت—الأحداث الأخيرة

• حسب النوع—طلبات المستخدم وأحداث التدقيق

يمكنك إنشاء أقسام الأحداث المحددة من قبل المستخدم بناءً على الإعدادات المتوفرة بغرض تكوينها في واجهة Kaspersky Security Center 14 Web Console.

السيناريو: المراقبة وإعداد التقارير

يعرض هذا القسم سيناريو لتكوين ميزة المراقبة وإعداد التقارير في Kaspersky Security Center.

المتطلبات الأساسية

بعد أن تنتشر 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

تعرف على الإعدادات التي تحدد تخصيص حالات الجهاز اعتماداً 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. وأنتك 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.

إشارات حركة المرور 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 أجزاء معلومات تحتوي على إشارات حركة مرور. 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	وظيفة تطبيق الأمان: حالة الحماية والفحص للكشف عن الفيروسات
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.

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 لأنواع التالية من الكائنات:

- لتحديدات الأجهزة التي تم إنشاؤها وفقاً 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 التبويب **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 حديثاً 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.

• عام القسم

• اسم قالب التقرير

• أقصى عدد من الإدخالات المراد عرضها ⑤

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 وفقاً 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 جداً من الإدخالات. إذا كانت هذه هي الحالة، فقد تجد صعوبة في قراءتها وتحليلها جميعاً. وقد تنفذ مساحة الذاكرة في جهازك أيضاً أثناء إنشاء مثل هذا التقرير، وبالتالي لن تتمكن من عرض التقرير. يتم تمكين هذا الخيار افتراضياً. القيمة الافتراضية هي 1000.

• طباعة الإصدار ⑤

يتم تحسين التقرير الناتج من أجل طباعته: تتم إضافة أحرف المسافة بين بعض القيم لتحسين الرؤية.

يتم تمكين هذا الخيار افتراضياً.

• 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

• مجموعة تحديد الجهاز، أو قسماً الأجهزة

قم بتغيير مجموعة الأجهزة العملية التي يتم إنشاء التقرير من أجلها. قد يكون واحد فقط من هذه الأقسام موجوداً، وفقاً 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 ⑤

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 أدونات لمستخدم أو مجموعة من المستخدمين، كما هو مطبق على التقرير.
يتم تمكين هذا الخيار افتراضياً.

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 ④

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 افتراضياً.

- أعلى إلى مستوى التداخل ④

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) ④

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 بيانات ذاكرة التخزين المؤقت من خوادم الإدارة الثانوية)، أو لا يوجد (غير متوفر) بخلاف ذلك.
القيمة الافتراضية هي 5 (ثوان).

- بيانات ذاكرة التخزين المؤقت من خوادم الإدارة الثانوية ④

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 أيضاً 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 افتراضياً.

- تكرار تحديث التخزين المؤقت (بالساعات) ④

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 9

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 افتراضياً.

تنسيق عامل التصفية الموسع في قوالب التقرير

في Kaspersky Security Center 14، يمكنك تطبيق تنسيق عامل التصفية الموسع في قوالب التقرير. يوفر تنسيق عامل التصفية الموسع مزيداً من المرونة مقارنة 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 مدعوماً 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 التبويب **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 حديثاً. 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 التبويب **التقارير**.

3. في قائمة قوالب التقرير، حدد قالب التقرير الذي تم [تحويله مسبقاً إلى تنسيق عامل التصفية الموسع](#).

4. من قائمة سياق قالب التقرير المحدد، حدد **خصائص**.

5. في نافذة الخصائص التي تفتح، حدد القسم **عوامل تصفية**.

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 اسماً فريداً 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 التبويب **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 تمثيلاً.
- 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 التبويب **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.

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 التبويب **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 التقارير. 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**.
- يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.

يتم عرض المهمة تسليم التقرير التي تم إنشاؤها حديثاً في المجلد **المهام** في شجرة وحدة التحكم.

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 هذه فقط إذا تم تحديد حفظ تقرير 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 لأي 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.

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 افتراضياً.

• **تحديد حساب**

املاً حقل الحساب وكلمة 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 وفقاً 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 ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• **كل N يوماً**

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 أسبوعاً**

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 9

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.

• يومياً (التوقيت الصيفي غير مدعوم) 9

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.

• أسبوعياً 9

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• حسب أيام الأسبوع 9

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهرياً 9

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.

• يدوياً 9

لا يتم تشغيل المهمة تلقائياً. يمكنك بدء تشغيلها يدوياً فقط. يتم تمكين هذا الخيار افتراضياً.

• كل شهر في أيام معينة من الأسابيع المحددة 9

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد. بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• عند انتشار الفيروس 9

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 المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكلٍ افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى 9

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار تشغيل الجهاز وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• تشغيل المهام الفائتة 9

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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العملية الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط. يتم تمكين هذا الخيار افتراضيًا.

• استخدم التأخير العشوائي لبدء المهام تلقائيًا 9

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 تبدأ المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المترامنة 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) 9

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 المترامنة 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، انقر فوق الزر إنهاء لإنهاء المعالج.

إذا كنت ترغب في بدء المهمة بمجرد انتهاء المعالج، حدد خانة الاختيار 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 مبنية 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 مبنية 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 زر 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 معلومات 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 التيوبيد 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 افتراضياً.

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 إعلانات 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 والتحقق 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 للاتصال 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.

■ حاوية 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 معلومات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة من خلال إضافة معلومات بديلة أخرى مع تفاصيل ذات صلة أكثر بالحدث. تتوفر قائمة بالمعلومات 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 9

تتيح لك علامة التبويب رسالة SMS تكوين إرسال إخطارات بمختلف الأحداث عبر رسالة SMS إلى هاتف محمول. سيتم إرسال رسائل SMS عبر بوابة البريد.

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، يمكنك 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، يمكنك 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 لفتح 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 لتحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مدار الفاصل الزمني المحدد.

يتيح لك النقر فوق الزر إرسال رسالة اختبار للتحقق 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 وقت 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 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. ستفتح 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 المحددة باستمرار في مساحة العمل، فانقر على زر ☆ بجانب المجموعة المحددة.
- 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 بتحديدته 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 التكميلية 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 الاستثناءات. اتبع تعليماته.

سيتم استثناء التطبيقات المحددة من القائمة **تشغيل القواعد 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. من شجرة وحدة التحكم، حدد المجلد **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 زر **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

إذا تم تمكين هذا الخيار، فسيتم عكس حالة التحديد المحددة. سيضمن التحديد جميع الأجهزة التي لا تتوافق مع الحالة. يتم تعطيل هذا الخيار افتراضياً.

الشبكة

في القسم الشبكة، يمكنك تحديد المعايير التي ستستخدم لتضمين الأجهزة في التحديد وفقاً لبيانات الشبكة الخاصة بهم:

• اسم الجهاز أو عنوان IP

اسم الجهاز الموجود في شبكة Windows (اسم NetBIOS)

• 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 وظاهري، 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 موجوداً في النص.

مثال:

للبحث عن عبارة تحتوي على الكلمة المركبة الخادم التابع، أدخل "الخادم التابع" في الاستعلام.

• نطاق IP ٩

إذا تم تمكين هذا الخيار، فيمكنك إدخال عناوين IP الأولية والنهائية لنطاق IP الذي يجب تضمين الأجهزة ذات الصلة فيه.
يتم تعطيل هذا الخيار افتراضياً.

العلامات

في القسم العلامات، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على الكلمات المفتاحية (العلامات) التي تمت إضافتها سابقاً إلى أوصاف الأجهزة المدارة:

• تطبيق في حالة مطابقة علامة محددة واحدة على الأقل ٩

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 افتراضياً.

• **يجب تضمين العلامة** ④

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 افتراضياً.

• **يجب استثناء العلامة** ④

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** ④

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من وحدة Active Directory المحددة في حقل الإدخال.
يتم تعطيل هذا الخيار افتراضياً.

• **تضمين وحدات تنظيمية تابعة** ④

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من الوحدات التنظيمية التابعة للوحدة التنظيمية المحددة Active Directory.
يتم تعطيل هذا الخيار افتراضياً.

• **هذا الجهاز عضو في مجموعة Active Directory** ④

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من مجموعة Active Directory المحددة في حقل الإدخال.
يتم تعطيل هذا الخيار افتراضياً.

نشاط الشبكة

في القسم **نشاط الشبكة** يمكنك تحديد المعايير التي ستستخدم لتضمين الأجهزة في التحديد وفقاً لنشاط الشبكة الخاص بهم:

• **هذا الجهاز هو عبارة عن نقطة توزيع** ④

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:

• مُمكن. 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 اختبار عند إجراء البحث:
- نعم. يشمل التطبيق في الاختيار الأجهزة المرئية في الوقت الحالي على الشبكة.
- لا. يشمل التطبيق في الاختيار 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 ④

- 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 ④

- 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 ④

- في حقل الإدخال، يمكنك تحديد معيار للأجهزة المشمولة في التحديث عند إجراء بحث باسم التطبيق أو برقم حزمة التحديث. إذا تم ترك الحقل فارغاً، لن يتم تطبيق المعيار.

آخر تحديث للوحدات ④

- 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 14 ④

- 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 9

- 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 ستستخدم لتضمين الأجهزة في التحديد وفقاً لنوع نظام التشغيل الخاص بهم.

• إصدار نظام التشغيل 9

إذا تم تحديد خانة الاختبار، فيمكنك تحديد نظام تشغيل من القائمة. يتم تضمين الأجهزة المثبت عليها أنظمة التشغيل المحددة في نتائج البحث.

• حجم نظام التشغيل بالبت 9

في القائمة المنسدلة، يمكنك تحديد بنية نظام التشغيل والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز (غير معروف، AMD64، x86 أو IA64). وبشكل افتراضي، لا يتم تحديد أي خيار في القائمة ومن ثم لا يتم تحديد بنية نظام التشغيل.

• إصدار حزمة خدمة نظام التشغيل 9

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 9

لا يكون هذا الإعداد قابلاً 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 أيضاً تكوين البحث عن جميع أرقام النسخة باستثناء الرقم المحدد.

• معرف تحرير نظام التشغيل 9

لا يكون هذا الإعداد قابلاً 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 أيضاً 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 ⑤

القائمة المنسدلة التي يمكنك فيها تحديد إحدى حالات الجهاز: موافق، أو حرج، أو تحذير.

• وصف حالة الجهاز ⑤

يمكنك في هذا الحقل، تحديد خانة الاختيار بجانب الشروط التي تحدد، إن تم استيفائها، إحدى الحالات التالية لجهاز الكمبيوتر: موافق أو حرج أو تحذير.

• حالة الجهاز المحددة بواسطة التطبيق ⑤

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 ⑤

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 افتراضياً.

• عملية الفحص الأخيرة ⑤

إذا تم تمكين هذا الخيار، فيمكنك البحث عن أجهزة العميل حسب وقت آخر فحص للفيروسات. في حقول الإدخال، يمكنك تحديد الفترة الزمنية التي تم فيها آخر فحص للفيروسات. يتم تعطيل هذا الخيار افتراضياً.

• إجمالي عدد التهديدات المكتشفة ⑤

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 افتراضياً.

سجل التطبيقات

في القسم سجل التطبيقات، يمكنك إعداد معايير البحث عن الأجهزة وفقاً للتطبيقات المثبتة عليها:

• اسم التطبيق ⑤

القائمة المنسدلة التي يمكنك فيها تحديد أي تطبيق. يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

• إصدار التطبيق ⑤

يمكنك في حقل الإدخال تحديد إصدار التطبيق المحدد.

• [المورد](#) ④

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة لأي تطبيق مثبت على الجهاز.

• [حالة التطبيق](#) ④

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](#) ④

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 وإصدار التطبيق وحالة التطبيق إلى اسم التحديث وإصدار التحديث والحالة على التوالي. يتم تعطيل هذا الخيار افتراضياً.

• [اسم تطبيق الأمان غير المتوافق](#) ④

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](#) ④

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](#) ④

إذا تم تمكين هذا الخيار، فسيتم تضمين تحديد أجهزة أوصافها لا تحتوي على أي من العلامات المحددة. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق المعيار. يتم تعطيل هذا الخيار افتراضياً.

سجل الأجهزة

في القسم **سجل الأجهزة**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على الأجهزة المثبتة:

• [الجهاز](#) ④

يمكنك في القائمة المنسدلة تحديد نوع الوحدة. يتم تضمين جميع الأجهزة الموجودة بها هذه الوحدة في نتائج البحث. يدعم الحقل البحث بالنص الكامل.

• [المورد](#) ④

يمكنك في القائمة المنسدلة تحديد اسم الشركة المصنعة للوحدة. يتم تضمين جميع الأجهزة الموجودة 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) (بالمجاهرتز)**

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 ⑤

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 ⑤

نطاق القيم لحجم ذاكرة الوصول العشوائي للجهاز. سيتم تضمين الأجهزة التي تحتوي على ذاكرة الوصول العشوائي، والتي تطابق النطاق في حقوق 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 جزءاً من البنية الأساسية لسطح المكتب الافتراضي (VDI):

• هذا جهاز ظاهري ⑤

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- ليس هاماً.
- لا. البحث عن الأجهزة التي لا تعد أجهزة ظاهرية.
- نعم. البحث عن الأجهزة التي تعد أجهزة ظاهرية.

• نوع الجهاز الظاهري ⑤

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة للجهاز الظاهري. هذه القائمة المنسدلة متاحة إذا تم تحديد القيمة نعم أو ليس هاماً تم تحديد القيمة هذا جهاز ظاهري في القائمة المنسدلة.

• جزء من البنية الأساسية لسطح المكتب الافتراضي ⑤

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- ليس هاماً.
- لا. البحث عن الأجهزة التي لا تعد جزءاً من البنية الأساسية لسطح المكتب الافتراضي.
- نعم. البحث عن الأجهزة التي تعد جزءاً من البنية الأساسية لسطح المكتب الافتراضي (VDI).

الثغرات الأمنية والتحديثات

في القسم الثغرات الأمنية والتحديثات، يمكنك تحديد المعايير التي ستستخدم لتضمين الأجهزة في التحديد وفقاً لمصدر Windows Update الخاص بها:

• تم تبديل WUA إلى خادم الإدارة ⑤

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، فستشتمل النتائج على 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. ستضمن 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 ستستخدم 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 خانة 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 تسريب البيانات (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

• [حالة الحماية الخاصة بتعاون الخوادم](#)

البحث عن الأجهزة حسب حالة حماية تعاون الخادم (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

• [حالة الحماية ضد الفيروسات الخاصة بخوادم البريد](#)

البحث عن الأجهزة حسب حالة حماية خادم البريد (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

• [حالة أداة استشعار نقطة النهاية](#)

البحث عن الأجهزة حسب حالة المكون أداة استشعار نقطة النهاية (لا توجد بيانات من الجهاز، 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: AES56 وAES128 وAES192 وAES256.

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 يمكن اكتشاف الجهاز باستخدام AWS API أو Azure API أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة ولكن لا يمكن اكتشافه باستخدام API لسبب ما.
- دون قيمة. يتعذر تطبيق هذا المعيار.

مكونات التطبيق

يحتوي هذا القسم على قائمة المكونات لهذه التطبيقات التي لديها مكونات إدارة إضافية مطابقة مثبتة في وحدة تحكم الإدارة.

في القسم مكونات التطبيق، يمكنك تحديد معايير لتضمين الأجهزة في تحديد وفقاً للحالات ولأرقام الإصدار المكونات التي تشير للتطبيق الذي حددته:

• الحالة ⑤

البحث عن الأجهزة وفقاً لحالة المكون المرسله بواسطة تطبيق إلى خادم الإدارة. يمكنك تحديد أحد الحالات التالية: لا بيانات من الجهاز، أو متوقف، أو بدء التشغيل، أو تم إيقاف مؤقتاً، أو قيد التشغيل، أو اختلال تشغيل أو غير مثبت. إذا كان للمكون المحدد للتطبيق المثبت على جهاز مُدار حالة محددة، فإنه يتم تضمين الجهاز في تحديد الجهاز.

الحالات المرسله بواسطة التطبيقات:

- بدء تشغيل—يكون المكون في عملية التهيئة في الوقت الحالي.
- قيد التشغيل—يكون المكون ممكناً ويعمل على النحو الصحيح.
- تم إيقاف مؤقتاً—تم تعليق المكون، على سبيل المثال، بعد إيقاف المستخدم للحماية مؤقتاً في التطبيق المُدار.
- اختلال التشغيل—حدث خطأ أثناء تشغيل المكون.
- متوقف—تم تعطيل المكون وهو لا يعمل في الوقت الحالي.
- غير مثبت—لم يتم 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 ⑤

البحث عن الأجهزة وفقاً لرقم الإصدار للمكون الذي حددته في القائمة. يمكنك كتابة رقم الإصدار، على سبيل المثال 0، 1، 4، 3، ثم تحديد ما إذا كان المكون المحدد يجب أن يمتلك إصداراً مماثلاً أو إصداراً سابقاً أو إصداراً أحدث. يمكنك أيضاً تكوين البحث عن جميع الإصدارات عدا الإصدار المحدد.

تصدير إعدادات تحديد جهاز إلى ملف

لتصدير إعدادات تحديد جهاز إلى ملف نصي:

1. من شجرة وحدة التحكم، حدد المجلد **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 اسماً لملف تصدير إعدادات التحديد، وحدد مجلداً لحفظه فيه، وانقر فوق الزر **حفظ**. وسوف يتم حفظ إعدادات تحديد الجهاز على الملف المحدد.

إنشاء تحديد جهاز

لإنشاء تحديد جهاز:

1. من شجرة وحدة التحكم، حدد المجلد **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 وفقاً لإعدادات مستوردة

لإنشاء تحديد جهاز وفقاً لإعدادات مستوردة:

1. من شجرة وحدة التحكم، حدد المجلد **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 بتحديدته.

إذا كان التحديد الذي يحمل اسم **تحديد جديد** موجوداً 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:
 - **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 إزالة تثبيتها على الأجهزة المُدارة، (على سبيل المثال، مستعرض مُعيّن). لاستخدام هذه الوظيفة، يمكنك إضافة تطبيقات من سجل التطبيقات إلى قائمة التطبيقات المُراقبة. عند تثبيت تطبيق مُراقَب أو إزالة تثبيته، ينشر عميل الشبكة الأحداث المعنية: تم تثبيت التطبيق المراقَب أو تم إلغاء تثبيت التطبيق المراقَب. 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 المُراقبة:

1. في المجلد **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.

أنواع الأحداث

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 الأجهزة المحمولة التي تعمل بنظام iOS MDM، وخادم الأجهزة المحمولة Exchange. أنواع الأحداث التي تظهر في تطبيقات Kaspersky غير مدرجة في هذا القسم.

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 المواقع 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 مدة التخزين للأحداث:

• وحدة تحكم الإدارة: تعيين مدة التخزين لحدث

• Kaspersky Security Center 14 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**: معرف 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.

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	<p>يقوم Kaspersky Security Center بالتحقق مما إذا تم تجاوز قيود الترخيص أم لا بمعدل مرة يوميًا.</p> <p>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 <u>وحدات الترخيص</u> المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد لنسبة 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص.</p> <p>حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none">• استعراض قائمة الأجهزة المُدارة.حذف الأجهزة غير المُستخدمة حاليًا.	180 يومًا

	<ul style="list-style-type: none"> تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخدام الإدارة). <p>يحدد Kaspersky Security Center القواعد المُستخدمة لإنشاء أحداث عند تجاوز تقييد الترخيص.</p>			
180 يومًا	<p>تحدث الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة زمنية قصيرة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> يمكنك تكوين الحد في خصائص خادم الإدارة. قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة التي سيتم تشغيلها عند وقوع هذا الحدث. 	GNRL_EV_VIRUS_OUTBREAK	26 (للحماية من تهديدات الملفات)	انتشار الفيروسات
180 يومًا	<p>تحدث الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة زمنية قصيرة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> يمكنك تكوين الحد في خصائص خادم الإدارة. قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة التي سيتم تشغيلها عند وقوع هذا الحدث. 	GNRL_EV_VIRUS_OUTBREAK	27 (للحماية من تهديدات البريد)	انتشار الفيروسات
180 يومًا	<p>تحدث الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة زمنية قصيرة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> يمكنك تكوين الحد في خصائص خادم الإدارة. قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة التي سيتم تشغيلها عند وقوع هذا الحدث. 	GNRL_EV_VIRUS_OUTBREAK	28 (لجدار الحماية)	انتشار الفيروسات
180 يومًا	<p>تحدث الأحداث من هذا النوع في حالة وجود أي جهاز مُدار مرئيًا على الشبكة، ولكنه غير متصل بخادم الإدارة لفترة زمنية محددة.</p>	KLSRV_HOST_OUT_CONTROL	4111	أصبح الجهاز غير مُدار

	تعرف على ما يمنع التشغيل السليم لعميل الشبكة على الجهاز. تتضمن الأسباب المحتملة حدوث مشكلات في الشبكة وإزالة عميل الشبكة من الجهاز.			
180 يوماً	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.	KLSRV_HOST_STATUS_CRITICAL	4113	حالة الجهاز حرج
180 يوماً	تقع الأحداث من هذا النوع عندما يضيف برنامج Kaspersky رمز التنشيط أو ملف المفتاح الذي تستخدمه في قائمة الرفض. تواصل مع الدعم الفني للحصول على المزيد من التفاصيل.	KLSRV_LICENSE_BLACKLISTED	4124	تمت إضافة ملف المفتاح إلى قائمة الرفض
180 يوماً	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 لخدم 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).	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	4130	وضع الوظائف المحدودة
180 يوماً	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 و15 يوم 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 .	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	4129	ستنتهي فترة صلاحية الترخيص قريباً

	<p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • تأكد من إضافة <u>مفتاح ترخيص احتياطي</u> إلى خادم الإدارة. • إذا كنت تستخدم <u>اشترًا</u>، فتأكد من تجديده. يتم تجديد الاشتراك غير المحدود تلقائيًا في حالة الدفع المسبق لموفر الخدمة في المواعيد المحددة. 			
180 يومًا	<p>تحدث الأحداث من هذا النوع عند انتهاء صلاحية شهادة خادم الإدارة لإدارة الجهاز المحمول.</p> <p>تحتاج إلى <u>تحديث الشهادة المنتهية الصلاحية</u>.</p> <p>يمكنك تكوين التحديثات التلقائية للشهادات بتحديد <u>إعادة إصدار الشهادة تلقائيًا</u> إن أمكن خانة الاختيار في <u>إعدادات إصدار الشهادة</u>.</p>	KLSRV_CERTIFICATE_EXPIRED	4132	انتهت صلاحية الشهادة
180 يومًا	<p>تحدث الأحداث من هذا النوع في حالة إبطال <u>التحديثات المستمرة</u> (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.</p>	KLSRV_SEAMLESS_UPDATE_REVOKED	4142	تم إبطال تحديثات الوحدات النمطية لبرامج Kaspersky

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

يوضح الجدول أدناه أنواع أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية خلل وظيفي.

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

مدة التخزين الافتراضية.	الوصف	نوع الحدث	معرف نوع الحدث	اسم العرض لنوع الحدث
180 يومًا	<p>تحدث الأحداث من هذا النوع بسبب حدوث مشكلات غير معروفة.</p> <p>وفي الغالب ما تكون عبارة عن مشكلات DBMS، ومشكلات في الشبكة، ومشكلات أخرى في البرامج والأجهزة.</p> <p>يمكن العثور على تفاصيل الحدث في وصف الحدث.</p>	KLSRV_RUNTIME_ERROR	4125	حدث خطأ وقت التشغيل
180 يومًا	<p>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</p>	KLSRV_INVLICPROD_EXCEDED	4126	تم تجاوز حد عمليات تثبيت إحدى مجموعات

التطبيقات المرخصة			<p>في Kaspersky Security Center وكذلك إذا تجاوز عدد عمليات التثبيت الحد الذي تم تعيينه بواسطة مفتاح الترخيص التابع لجهة خارجية.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • 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. <p>يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المرخصة. تشمل مجموعة التطبيقات المرخصة على التطبيقات التي تفي بالمعايير المحددة بواسطة.</p>
فشل استقصاء قطاع السحابة	4143	KLSRV_KL_CLOUD_SCAN_ERROR	<p>تحدث الأحداث من هذا النوع عندما يفشل خادم الإدارة في استقصاء مقطع شبكة في بيئة سحابية. اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقاً لذلك.</p>
فشل نسخ التحديثات إلى المجلد المحدد	4123	KLSRV_UPD_REPL_FAIL	<p>تحدث الأحداث من هذا النوع عند القيام بنسخ تحديثات البرنامج إلى مجلد (مجلدات) إضافية مشتركة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • 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 (المجلدات) أم لا. • تحقق من الاتصال بالإنترنت لأنه قد يكون السبب في حدوث هذا الحدث. اتبع التعليمات للقيام بتحديث قواعد البيانات والوحدات النمطية للبرامج.
لا توجد مساحة فارغة على القرص	4107	KLSRV_DISK_FULL	<p>تحدث الأحداث من هذا النوع عند نفاذ مساحة القرص في الجهاز المثبت عليه خادم الإدارة.</p> <p>قم بتحرير مساحة القرص على الجهاز.</p>
المجلد المشترك غير متاح	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	<p>تحدث الأحداث من هذا النوع في حال عدم توافر <u>المجلد المشترك لخادم الإدارة</u>.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • تحقق مما إذا تم تشغيل خادم الإدارة وتوافره (حيث يوجد المجلد المشترك) أم لا.

	<ul style="list-style-type: none"> تحقق مما إذا تم تغيير اسم المستخدم و / أو كلمة المرور الخاصة بالمجلد أم لا. تحقق من الاتصال بالشبكة. 			
180 يومًا	<p>تحدث الأحداث من هذا النوع في حال أصبحت قاعدة بيانات خادم الإدارة غير متاحة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> 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. 	KLSRV_DATABASE_UNAVAILABLE	4109	قاعدة بيانات خادم الإدارة غير متوفرة
180 يومًا	<p>تحدث الأحداث من هذا النوع في حالة عدم توافر مساحة فارغة في قاعدة بيانات خادم الإدارة.</p> <p>لا يقوم خادم الإدارة بإداء وظيفته عند وصول قاعدة البيانات الخاصة به إلى سعته وكذلك عند استحالة إجراء المزيد من التسجيلات في قاعدة البيانات.</p> <p>فيما يلي الأسباب التي أدت إلى هذا الحدث، وفقًا لـ DBMS التي تستخدمها، والاستجابات المناسبة للحدث:</p> <ul style="list-style-type: none"> 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. <p><u>يمكنك تقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.</u> 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 بتخزين حدث التحكم في التطبيقات في قاعدة بيانات خادم الإدارة.</p> <ul style="list-style-type: none"> إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition: <u>لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.</u> <u>يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.</u> 	KLSRV_DATABASE_FULL	4110	لا توجد مساحة فارغة في قاعدة بيانات خادم الإدارة

أحداث التحذير لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center التي تدرج ضمن مستوى أهمية تحذير.

أحداث التحذير لخادم الإدارة

مدة التخزين الافتراضية.	الوصف	نوع الحدث	معرف نوع الحدث	اسم العرض لنوع الحدث
90 يومًا	<p>يقوم Kaspersky Security Center بالتحقق مما إذا تم تجاوز قيود الترخيص أم لا بمعدل مرة يوميًا.</p> <p>تحدث الأحداث من هذا النوع عند اكتشاف خادم الإدارة حدوث تجاوز لبعض قيود الترخيص بواسطة تطبيقات Kaspersky المثبتة على الأجهزة العملية وكذلك في حال كان عدد <u>وحدات الترخيص</u> المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد يشكل من 100% إلى 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص.</p> <p>حتى عند حدوث هذا الحدث، تكون الأجهزة العملية محمية.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا. • تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). <p>يحدد Kaspersky Security Center <u>القواعد المُستخدمة لإنشاء أحداث</u> عند تجاوز تقييد الترخيص.</p>	KLSRV_EV_LICENSE_CHECK_100_110	4098	تم تجاوز حد الترخيص
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يظهر الجهاز المُدار عدم النشاط لبعض الوقت.</p> <p>يحدث هذا غالبًا عند إيقاف تشغيل الجهاز المُدار.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • إزالة الجهاز من قائمة الأجهزة المُدارة تلقائيًا. 	KLSRV_EVENT_HOSTS_NOT_VISIBLE	4103	ظل الجهاز غير نشط على الشبكة لوقت طويل

	<ul style="list-style-type: none"> • 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 14 Web Console • حدد الفاصل الزمني الذي يتم بعده إزالة الجهاز تلقائيًا من المجموعة باستخدام وحدة تحكم الإدارة أو باستخدام Kaspersky Security Center 14 Web Console 			
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يعتبر خادم الإدارة جهازين مُدارين أو أكثر كجهاز واحد.</p> <p>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.</p> <p>لتجنب هذه المشكلة، قم بتبديل عميل الشبكة إلى وضع استنساخ القرص على جهاز مرجعي قبل استنساخ محرك الأقراص الثابتة لهذا الجهاز.</p>	KLSRV_EVENT_HOSTS_CONFLICT	4102	تعارض في أسماء الجهاز
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يتم تعيين الحالة تحذير للجهاز المُدار. يمكنك تكوين الشروط التي يتم من خلالها تغيير حالة الجهاز إلى تحذير.</p>	KLSRV_HOST_STATUS_WARNING	4114	حالة الجهاز 'تحذير'
90 يومًا	<p>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.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • 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. 	KLSRV_INVLICPROD_FILLED	4127	سيتم تجاوز حد عمليات التثبيت لإحدى مجموعات التطبيقات المرخصة قريبًا

	<p>يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المرخصة.</p>			
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما تفشل إعادة إصدار شهادة إدارة الأجهزة المحمولة تلقائيًا.</p> <p>قد تكون الأسباب والردود المناسبة على الحدث فيما يلي:</p> <ul style="list-style-type: none"> 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 وإصدار الشهادة. راجع خصائص الحساب. 	KLSRV_CERTIFICATE_REQUESTED	4133	تم طلب شهادة
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يزيل المسؤول أي نوع من الشهادات (عام، بريد، VPN) لإدارة الجهاز المحمول.</p> <p>بعد إزالة الشهادة، ستنقل الأجهزة المحمولة المتصلة عبر هذه الشهادة في الاتصال بخادم الإدارة.</p> <p>قد يكون هذا الحدث مفيدًا عند التحقيق في الأعطال المرتبطة بإدارة الأجهزة المحمولة.</p>	KLSRV_CERTIFICATE_REMOVED	4134	تمت إزالة الشهادة
غير مخزنة	<p>تحدث الأحداث من هذا النوع عند انتهاء صلاحية شهادة APN.</p> <p>تحتاج إلى تجديد شهادة APN يدويًا وتثبيتها على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.</p>	KLSRV_APN_CERTIFICATE_EXPIRED	4135	انتهت صلاحية شهادة أسماء نقاط الوصول
غير مخزنة	<p>تحدث الأحداث من هذا النوع عندما يتبقى أقل من 14 يومًا قبل انتهاء صلاحية شهادة APN.</p> <p>عند انتهاء صلاحية شهادة APN، تحتاج إلى تجديد شهادة APN يدويًا وتثبيتها على خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM.</p> <p>نوصيك بجدولة تجديد شهادة أسماء نقاط الوصول (APNs) قبل تاريخ انتهاء الصلاحية.</p>	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	4136	ستنتهي صلاحية شهادة أسماء نقاط الوصول قريبًا
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Google Firebase (Cloud Messaging) (FCM).</p>	KLSRV_GCM_DEVICE_ERROR	4138	فشل إرسال رسالة FCM إلى الجهاز المحمول

	<p>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.</p> <p>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 Google Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات").</p>			
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Google Firebase (FCM Cloud Messaging) 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:</p> <ul style="list-style-type: none"> • 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 Google Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات"). • مشاكل من جانب الخادم الوكيل (إذا كنت تستخدم خادمًا وكيلًا). اقرأ كود HTTP في تفاصيل الحدث واستجب وفقًا لذلك. 	KLSRV_GCM_HTTP_ERROR	4139	حدث خطأ في HTTP أثناء إرسال رسالة FCM إلى خادم FCM
90 يومًا	<p>تحدث الأحداث من هذا النوع بسبب أخطاء غير متوقعة من جانب خادم الإدارة عند العمل مع بروتوكول Google Firebase Cloud Messaging HTTP.</p> <p>اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقًا لذلك.</p> <p>إذا لم تتمكن من إيجاد حل لمشكلة ما بنفسك، فنوصيك بالاتصال بالدعم الفني لـ Kaspersky.</p>	KLSRV_GCM_GENERAL_ERROR	4140	فشل إرسال رسالة FCM إلى خادم FCM
90 يومًا	<p>تحدث الأحداث من هذا النوع عند نفاد مساحة القرص في الجهاز المثبت عليه خادم الإدارة.</p>	KLSRV_NO_SPACE_ON_VOLUMES	4105	توجد مساحة فارغة قليلة على القرص الصلب

	قم بتحرير مساحة القرص على الجهاز.			
90 يومًا	<p>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.</p> <p>فيما يلي الأسباب التي أدت إلى هذا الحدث، وفقًا لـ DBMS التي تستخدمها، والاستجابات المناسبة للحدث.</p> <p>إنك تستخدم خادم SQL Server Express Edition DBMS:</p> <ul style="list-style-type: none"> • 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. <p>إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition:</p> <ul style="list-style-type: none"> • لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. <p>استعرض المعلومات عند تحديد DBMS.</p>	KLSRV_NO_SPACE_IN_DATABASE	4106	توجد مساحة فارغة قليلة في قاعدة بيانات خادم الإدارة
90 يومًا	<p>تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي.</p> <p>اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الثانوي واستجب وفقًا لذلك.</p>	KLSRV_EV_SLAVE_SRV_DISCONNECTED	4116	تمت مقاطعة الاتصال بخادم الإدارة الثانوي

90 يومًا	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.	KLSRV_EV_MASTER_SRV_DISCONNECTED	4118	تم قطع الاتصال بخادم الإدارة الأساسي
90 يومًا	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 Kaspersky Security Center Web Console .	KLSRV_SEAMLESS_UPDATE_REGISTERED	4141	تم تسجيل تحديثات جديدة للوحدات النمطية لبرنامج Kaspersky
غير مخزنة	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 المخزنة في قاعدة بيانات خادم الإدارة . • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة .	KLSRV_EVP_DB_TRUNCATING	4145	تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وبدأت عملية حذف الأحداث
غير مخزنة	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 المخزنة في قاعدة بيانات خادم الإدارة . • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة .	KLSRV_EVP_DB_TRUNCATED	4146	تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وتم حذف الأحداث

الأحداث المعلوماتية لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية معلومات.

الأحداث المعلوماتية لخادم الإدارة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.

30 يومًا	KLSRV_EV_LICENSE_CHECK_90	4097	تم استنفاد أكثر من 90% من هذا المفتاح
30 يومًا	KLSRV_EVENT_HOSTS_NEW_DETECTED	4100	تم اكتشاف جهاز جديد
30 يومًا	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	4101	تمت إضافة جهاز إلى المجموعة تلقائيًا
30 يومًا	KLSRV_INVISIBLE_HOSTS_REMOVED	4104	تمت إزالة الجهاز من المجموعة: غير نشط على الشبكة لمدة طويلة
30 يومًا	KLSRV_INVLICPROD_EXPIRED_SOON	4128	سيتم تجاوز حد عمليات التثبيت قريبًا (تم استهلاك أكثر من 95%) لأحدى مجموعات التطبيقات المرخصة
30 يومًا	KLSRV_APS_FILE_APPEARED	4131	تم العثور على ملفات سترسل إلى Kaspersky للتحليل
30 يومًا	KLSRV_GCM_DEVICE_REGID_CHANGED	4137	تم تغيير معرف ميثيل FCM على هذا الجهاز المحمول
30 يومًا	KLSRV_UPD_REPL_OK	4122	تم نسخ التحديثات بنجاح إلى المجلد المحدد
30 يومًا	KLSRV_EV_SLAVE_SRV_CONNECTED	4115	تم إنشاء الاتصال بخادم الإدارة الثانوي
30 يومًا	KLSRV_EV_MASTER_SRV_CONNECTED	4117	تم إنشاء الاتصال بخادم الإدارة الأساسي
30 يومًا	KLSRV_UPD_BASES_UPDATED	4144	تم تحديث قواعد البيانات
30 يومًا	KLAUD_EV_SERVERCONNECT	4147	تدقيق: تم إنشاء اتصال بخادم الإدارة
30 يومًا	KLAUD_EV_OBJECTMODIFY	4148	تدقيق: تم تعديل الكائن
30 يومًا	KLAUD_EV_TASK_STATE_CHANGED	4150	تدقيق: تم تغيير حالة الكائن
30 يومًا	KLAUD_EV_ADMGROUP_CHANGED	4149	تدقيق: تم تعديل إعدادات المجموعة
30 يومًا	KLAUD_EV_SERVERDISCONNECT	4151	التدقيق: تم إنهاء الاتصال بخادم الإدارة
30 يومًا	KLAUD_EV_OBJECTPROPMODIFIED	4152	التدقيق: تم تعديل خصائص الكائن
30 يومًا	KLAUD_EV_OBJECTACLMODIFIED	4153	التدقيق: تم تعديل أذونات المستخدم

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 تدرج ضمن مستوى خطورة خلل وظيفي.

أحداث الخلل الوظيفي لعميل الشبكة

اسم العرض لنوع الحدث	معرف نوع	نوع الحدث	الوصف	مدة التخزين
-------------------------	-------------	-----------	-------	----------------

الافتراضية	الحدث	الحدث	خطأ في تثبيت التحديث
30 يومًا	KLNAG_EV_PATCH_INSTALL_ERROR	770	خطأ في تثبيت التحديث
30 يومًا	KLNAG_EV_3P_PATCH_INSTALL_ERROR	7697	فشل تثبيت تحديث برامج الجهة الخارجية
30 يومًا	KLNAG_EV_WUA_INSTALL_ERROR	7717	فشل تثبيت تحديثات Windows

أحداث تحذير عميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center التي تدرج ضمن مستوى الخطورة تحذير.

أحداث تحذير عميل الشبكة

مدة التخزين الافتراضية	نوع الحدث	معرف نوع الحدث	اسم العرض لنوع الحدث
30 يومًا	KLNAG_EV_PATCH_INSTALL_WARNING	7701	ظهر تحذير أثناء تثبيت تحديث الوحدة النمطية للبرامج
30 يومًا	KLNAG_EV_3P_PATCH_INSTALL_WARNING	7696	اكتمل تثبيت تحديث برامج الجهة الخارجية مع وجود تحذير
30 يومًا	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	7698	تم تأجيل تثبيت تحديث برامج الجهة الخارجية
30 يومًا	GNRL_EV_APP_INCIDENT_OCCURED	549	وقع حادث
30 يومًا	KSNPROXY_STARTED_CON_CHK_FAILED	7718	بدأ وكيل KSN. فشل فحص مدى توفر KSN

الأحداث المعلوماتية لعميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center التي تدرج ضمن مستوى الخطورة معلومات.

مدة التخزين الافتراضية.	نوع الحدث	معرف نوع الحدث	اسم العرض لنوع الحدث
30 يومًا	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	7699	تم تثبيت تحديث الوحدات النمطية للبرامج بنجاح
30 يومًا	KLNAG_EV_PATCH_INSTALL_STARTING	7700	بدأ تثبيت تحديث الوحدة النمطية للبرامج
30 يومًا	KLNAG_EV_INV_APP_INSTALLED	7703	تم تثبيت التطبيق
30 يومًا	KLNAG_EV_INV_APP_UNINSTALLED	7704	تم إلغاء تثبيت التطبيق
30 يومًا	KLNAG_EV_INV_OBS_APP_INSTALLED	7705	تم تثبيت التطبيق المراقب
30 يومًا	KLNAG_EV_INV_OBS_APP_UNINSTALLED	7706	تم إلغاء تثبيت التطبيق المراقب
30 يومًا	KLNAG_EV_INV_CMPTR_APP_INSTALLED	7707	تم تثبيت التطبيق التابع لجهة خارجية
30 يومًا	KLNAG_EV_DEVICE_ARRIVAL	7708	تمت إضافة جهاز جديد
30 يومًا	KLNAG_EV_DEVICE_REMOVE	7709	تمت إزالة الجهاز
30 يومًا	KLNAG_EV_NAC_DEVICE_DISCOVERED	7710	تم اكتشاف جهاز جديد
30 يومًا	KLNAG_EV_NAC_HOST_AUTHORIZED	7711	تم اعتماد الجهاز
30 يومًا	KLUSRLOG_EV_FILE_READ	7712	مشاركة سطح المكتب لـ Windows: تمت قراءة الملف
30 يومًا	KLUSRLOG_EV_FILE_MODIFIED	7713	مشاركة سطح المكتب لـ Windows: تم تعديل الملف
30 يومًا	KLUSRLOG_EV_PROCESS_LAUNCHED	7714	مشاركة سطح المكتب لـ Windows: تم بدء التطبيق
30 يومًا	KLUSRLOG_EV_WDS_BEGIN	7715	مشاركة سطح المكتب لـ Windows: تم البدء
30 يومًا	KLUSRLOG_EV_WDS_END	7716	مشاركة سطح المكتب لـ Windows: تم الإيقاف
30 يومًا	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	7694	تم تثبيت تحديث برامج الجهات الخارجية بنجاح
30 يومًا	KLNAG_EV_3P_PATCH_INSTALL_STARTING	7695	تم بدء تثبيت تحديث برامج الجهة الخارجية
30 يومًا	KSNPROXY_STARTED_CON_CHK_OK	7719	بدأ وكيل KSN. اكتمل فحص مدى توفر KSN بنجاح
30 يومًا	KSNPROXY_STOPPED	7720	توقف وكيل شبكة KSN

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**.

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 الخطورة **تحذير**.

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم اكتشاف محاولة توصيل جهاز محمول مقفل	INACTICE_DEVICE_TRY_CONNECTED	30 يوماً
تم إزالة ملف التعريف	MDM_PROFILE_WAS_REMOVED	30 يوماً
تم اكتشاف محاولة إعادة استخدام شهادة عميل.	CLIENT_CERT_ALREADY_IN_USE	30 يوماً
تم اكتشاف جهاز غير مقفل.	FOUND_INACTIVE_DEVICE	30 يوماً
رمز الاسترداد مطلوب.	NEED_REDEMPTION_CODE	30 يوماً
تم تضمين ملف التعريف في سياسة تمت إزالتها من الجهاز.	UMDM_PROFILE_WAS_REMOVED	30 يوماً

الأحداث المعلوماتية لخدمات 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 معلومات.

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم توصيل جهاز محمول جديد.	NEW_DEVICE_CONNECTED	30 يوماً
تم طلب قائمة بملفات التعريف بنجاح.	PROFILELIST_COMMAND_SUCCESSFULL	30 يوماً
تم تثبيت ملف التعريف بنجاح.	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 يوماً
تمت إزالة ملف التعريف بنجاح.	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 يوماً
تم طلب قائمة بملفات تعريف التزويد بنجاح.	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 يوماً
تم تثبيت ملف تعريف التزويد بنجاح.	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 يوماً
تم إزالة ملف تعريف التزويد بنجاح.	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 يوماً
تم طلب قائمة بالشهادات الرقمية بنجاح.	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 يوماً
تم طلب قائمة بالتطبيقات المثبتة بنجاح.	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 يوماً
تم طلب المعلومات العامة بشأن الجهاز المحمول بنجاح.	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 يوماً
تم طلب معلومات الأمان بنجاح.	SECURITYINFO_COMMAND_SUCCESSFULL	30 يوماً
تم قفل الجهاز المحمول بنجاح.	DEVICELOCK_COMMAND_SUCCESSFULL	30 يوماً
تمت إعادة تعيين كلمة المرور بنجاح.	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 يوماً
تم مسح البيانات من الجهاز المحمول.	ERASEDEVICE_COMMAND_SUCCESSFULL	30 يوماً
تم تثبيت التطبيق بنجاح.	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 يوماً
تم تعيين رمز الاسترداد الخاص بالتطبيق بنجاح.	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 يوماً
تم طلب قائمة التطبيقات المُدارة بنجاح.	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 يوماً
تمت إزالة التطبيق المدار بنجاح.	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 يوماً
تم تطبيق إعدادات التجوال بنجاح.	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 يوماً

أحداث خادم الأجهزة المحمولة Exchange

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بخادم الأجهزة المحمولة Exchange.

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة Exchange

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة Exchange في Kaspersky Security Center التي تشمل مستوى الخطورة **خلل وظيفي**.

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة Exchange

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
فشل في مسح البيانات من الجهاز المحمول	WIPE_FAILED	30 يوماً
يتعذر حذف معلومات حول اتصال الجهاز المحمول بصندوق البريد.	DEVICE_REMOVE_FAILED	30 يوماً
فشل تطبيق سياسة ActiveSync على صندوق البريد.	POLICY_APPLY_FAILED	30 يوماً
خطأ في تشغيل التطبيق.	PRODUCT_FAILURE	30 يوماً
فشل تعديل حالة وظائف ActiveSync.	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 يوماً

الأحداث المعلوماتية الخاصة بخادم الأجهزة المحمولة Exchange

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة Exchange في Kaspersky Security Center التي تشمل مستوى الخطورة **معلومات**.

الأحداث المعلوماتية الخاصة بخادم الأجهزة المحمولة Exchange

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم توصيل جهاز محمول جديد.	NEW_DEVICE_CONNECTED	30 يوماً
تم مسح البيانات من الجهاز المحمول.	WIPE_SUCCESSFULL	30 يوماً

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. تلقى 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 **الإستمرار 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 فوق الزر **حذف**.

بهذا تم حذف الحدث المتكرر من قائمة الأحداث المتكررة. سيستلم خادم الإدارة أحداثاً 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 المُدارة. إذا كان جهاز ظاهري يعمل كجهاز مُدار، فيمكن للمستخدم استعادة حالته في أي وقت باستخدام لقطة الجهاز الظاهري التي تم إنشائها مسبقاً. 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 12:00 مساءً، والتي ستبدأ على الجهاز الافتراضي VM_1 في تمام الساعة 12:01 مساءً. وفي تمام الساعة 12:30 مساءً، قام مستخدم الجهاز الافتراضي VM_1 بتغيير حالته باستعادتها من لقطة تم إجراؤها في تمام الساعة 11:00 صباحاً. 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، محلياً، باستخدام الأمر **regedit** من القائمة **بدء > تشغيل**).

2. انتقل إلى الخلية التالية:

- أنظمة 32 بت:

Y_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

- أنظمة 64 بت:

INE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

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

الوصف	القيمة	المفتاح (نوع البيانات)
التاريخ والوقت (بتنسيق UTC) لآخر اتصال بخادم الإدارة	DD-MM-YYYY HH-MM-SS	Protection_LastConnected ((REG_SZ
اسم خادم الإدارة الذي يُدير الجهاز	IP أو اسم DNS أو اسم NetBIOS	Protection_AdmServer ((REG_SZ
بناء رقم عميل الشبكة المثبت على الجهاز	a.b.c.d	Protection_NagentVersion ((REG_SZ
العدد الكامل لإصدار عميل الشبكة (مع تصحيحات) المثبتة على الجهاز	؛a.b.c.d (patch1 (patchN ؛...؛ patch2	Protection_NagentFullVersion ((REG_SZ
معرف الجهاز	مُعرّف الجهاز	(Protection_HostId (REG_SZ
يتم تثبيت عميل الشبكة في الوضع الديناميكي للبنية الأساسية لسطح المكتب الافتراضي (VDI)	0 - لا 1 - نعم	Protection_DynamicVM ((REG_DWORD
يوجد تطبيق أمن مثبت على الجهاز	0 - لا 1 - نعم	Protection_AvInstalled ((REG_DWORD
تم تمكين الحماية في الوقت الحقيقي على الجهاز	0 - لا 1 - نعم	Protection_AvRunning ((REG_DWORD
يتم تثبيت مكون الحماية في الوقت الحقيقي	0 - لا 1 - نعم	Protection_HasRtp ((REG_DWORD
حالة الحماية في الوقت الحقيقي:		Protection_RtpState ((REG_DWORD
غير معروف	0	
معطل	1	
متوقف مؤقتاً	2	
يجري البدء	3	

ممكن	4	
ممكّن مع مستوى مرتفع من الحماية (حماية القسوى)	5	
ممكّن مع انخفاض مستوى الحماية (السرعة القسوى)	6	
ممكّن مع الإعدادات الافتراضية (مستحسن)	7	
ممكّن مع الإعدادات المخصصة	8	
فشلت العملية	9	
التاريخ والوقت (بتنسيق UTC) لآخر فحص كامل	DD-MM-YYYY HH-MM-SS	Protection_LastFscan ((REG_SZ
التاريخ والوقت (بتنسيق UTC) لإصدار قواعد بيانات التطبيق	DD-MM-YYYY HH-MM-SS	Protection_BasesDate ((REG_SZ

عرض وتكوين الإجراءات عندما تكون حالة الأجهزة غير نشطة

إذا كانت الأجهزة العملية 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.

سيتم توزيع قيم الإعداد إلى المجموعات الفرعية ولكن في خصائص المجموعات الفرعية يتم قفل هذه الإعدادات. يتم تعطيل هذا الخيار افتراضياً.

5. انقر على موافق.

تم حفظ وتطبيق التغييرات الخاصة بك.

تعطيل أخبار Kaspersky

في Kaspersky Security Center 14 Web Console، قسم [أخبار Kaspersky](#) (المراقبة والإبلاغ — أخبار Kaspersky) يبيّنك 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 14 Web Console**.

4. انقر فوق موافق.

بهذا تم تعطيل أخبار Kaspersky.

يتم تعطيل الأخبار التسويقية افتراضياً. أنت لا تتلقى أخبار تسويقية إلا إذا قمت بتمكين (KSN Kaspersky Security Network). 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:

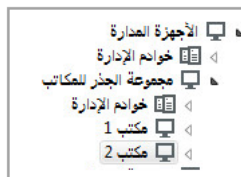
• بناء بنية مجموعات الإدارة مع الأخذ في الاعتبار مخطط الشبكة. قد لا تعكس بنية مجموعات الإدارة مخطط الشبكة بالدقة المطلقة. قد يكون التطابق بين الأجزاء المنفصلة للشبكة ومجموعات الإدارة المحددة كافيًا. يمكنك استخدام التعيين التلقائي لنقاط التوزيع أو تعيينها يدويًا.

• 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 عميل من عملاء الشبكة في الإصدار Service Pack 110 أو الإصدارات الأحدث بنقطة التوزيع التي لديها المسار الأقصر. 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 والمكتب 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 زر إضافة.
- 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.

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 شريحة شبكة جديدة باستخدام أجهزة Linux

يمكنك توصيل شريحة شبكة جديدة على جهاز Linux. أنت بحاجة إلى جهازين مختلفين على الأقل. يمكنك تكوين جهاز واحد كبوابة اتصال في منطقة الأجهزة الموصولة مباشرة بالإنترنت؛ والجهاز الآخر كنقطة توزيع.

اتبع الإجراءات الموضح في هذا القسم فقط بعد الانتهاء من [سيناريو التثبيت الرئيسي](#).

لتوصيل شريحة شبكة جديدة على جهاز Linux:

1. قم بتوصيل جهاز Linux للعمل كبوابة في منطقة الأجهزة الموصولة مباشرة بالإنترنت.

2. قم بتوصيل جهاز Linux بخادم الإدارة عبر أحد بوابات الاتصال.

تم تكوين توصيل شريحة شبكة جديدة على جهاز Linux.

توصيل جهاز Linux للعمل كبوابة في منطقة الأجهزة الموصولة مباشرة بالإنترنت

لتوصيل جهاز Linux للعمل كبوابة في منطقة الأجهزة الموصولة مباشرة بالإنترنت (DMZ):

1. يقوم المسؤول بـتثبيت عميل الشبكة على الجهاز العميل.

2. قم بتشغيل البرنامج النصي بعد التثبيت واتبع المعالج من أجل إعداد تكوين البيئة المحلية. من موجه 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 نافذة خصائص خادم الإدارة التي يتم فتحها، حدد قسم **نقاط التوزيع**.

5. في نافذة **نقاط التوزيع** التي تفتح، في الجزء الأيمن من النافذة:

a. حدد خيار **تعيين نقاط التوزيع يدويًا**.

b. انقر على زر **إضافة**.

يؤدي ذلك إلى فتح النافذة **إضافة نقطة توزيع**.

6. في النافذة **إضافة نقطة توزيع**، قم بتنفيذ الإجراءات التالية:

a. في ظل **عمل الجهاز كنقطة توزيع**، انقر على السهم لأسفل ▼ من قائمة الزر المنقسم **تحديد**، وحدد الاختيار **إضافة بوابة اتصال في DMZ حسب العنوان**.

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**.

7. سيتم عرض نقطة التوزيع التي أضفتها في قائمة نقاط التوزيع، في القسم **نقاط التوزيع**.

8. 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 $
```

9. في نافذة التطبيق الرئيسية، انتقل إلى Kaspersky Security Center و**اكتشف الجهاز**.

10. في النافذة التي تفتح، انقر فوق **اسم الجهاز**.

11. في القائمة المنسدلة، اختر **الانتقال إلى رابط المجموعة**.

12. في نافذة **تحديد المجموعة** التي تفتح، انقر على رابط **نقاط التوزيع**.

14. أعد تشغيل خدمة عميل الشبكة على عميل Linux عن طريق تنفيذ الأمر التالي في موجه الأوامر:
`sudo /opt/kaspersky/klnagent64/bin/klnagchk $` - إعادة التشغيل

اكتمل توصيل جهاز Linux للعمل كبوابة في منطقة الأجهزة الموصولة مباشرة بالإنترنت.

اتصال جهاز Linux بخادم الإدارة عبر أحد بوابات الاتصال

لتوصيل جهاز Linux بخادم الإدارة عبر أحد بوابات الاتصال، قم بتنفيذ الإجراءات التالية على هذا الجهاز:

1. يقوم المسؤول بتهيئة 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 موجه 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 الموصولة مباشرة بالإنترنت للعمل كنقطة توزيع

تتطلب [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 الموصولة 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 زر إضافة.

يؤدي ذلك إلى فتح النافذة إضافة نقطة توزيع.

6. في النافذة إضافة نقطة توزيع، قم بتنفيذ الإجراءات التالية:

a. في ظل عمل الجهاز كنقطة توزيع، انقر على السهم الأسفل  من قائمة الزر المنقسم تحديد، وحدد الاختيار 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 لتحديد.

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.

تعيين نقاط التوزيع تلقائيًا

نوصي بقيامك بتعيين نقاط التوزيع تلقائيًا. حينئذٍ، سيحدد Kaspersky Security Center نفسه 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 الموصولة 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 معين خصيصاً كبوابة اتصال، وتغطية 10000 جهاز عميل (بما في ذلك الأجهزة المحمولة) كحد أقصى باستخدام بوابة الاتصال هذه.

إضافة نطاقات IP لقائمة النطاقات التي تم فحصها الخاصة بنقطة توزيع

يمكنك إضافة نطاقات IP لقائمة النطاقات التي تم فحصها الخاصة بنقطة التوزيع.

لإضافة نطاق IP لقائمة النطاقات التي تم فحصها:

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 خانة الاختيار تمكين استقصاء النطاق.
7. انقر على زر إضافة.
8. في النافذة نطاق IP، أدخل اسم نطاق IP الجديد (يكون النطاق الجديد هو الاسم الافتراضي).
9. انقر على زر إضافة.

- 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 فحصها.

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 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.

يدعم خادم الدفع تحميل ما يصل إلى 50000 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 [عديك قطع الاتصال بخادم الإدارة](#) على الأجهزة المدارة أو إرسال الحزم إلى منفذ UDP الخاص بوكيل 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 قسم عام من الجزء الأيسر الأقسام، حدد خيار [استخدام نقطة التوزيع هذه كخادم دفع](#).
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 قسم [الاتصال](#)، انتقل إلى القسم الفرعي [الشبكة](#).
10. في القسم الفرعي [الشبكة](#)، حدد خيار [استخدام 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 بتشغيل 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 مثبت عليه وحدة تحكم إدارة والتي من خلالها يمكن الوصول إلى منافذ TCP رقم 13291 على كل 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 المزعم 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 العقدة خوادم الإدارة الخاصة بالمجموعة المحددة، انقر فوق الرابط [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". [سيتم تلقي خادم الإدارة الثانوي اتصال من خادم الإدارة الرئيسي](#).

إن لم يكن لديك جهازاً مثبتاً 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 المنافذ 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 المنافذ 13000 الخاص بخادم الإدارة الرئيسي المزعم 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 لمطابته 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 العقدة خوادم الإدارة، انقر فوق الرابط **إضافة خادم إدارة ثانوي**.

يبدأ تشغيل معالج إضافة خادم إدارة ثانوي

7. في الخطوة الأولى من المعالج (إدخال العنوان)، اترك الحقل **عنوان خادم الإدارة الثانوي (اختياري)** فارغاً.

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 مختلفاً لوحدت تحكم الإدارة للاتصال بخادم الإدارة الثانوي المفترض. إذا كان خادم الإدارة موجود في مكتب بعيد، اتصل بمسؤول النظام الخاص بهذا المكتب لمطابته 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 خانة 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 المزعم.

14. حدد الملف الذي تم حفظه سابقاً 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. سيُتلقى خادم الإدارة الثانوي اتصالاً 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 المنافذ 13000. يُنصح بذلك إذا، على سبيل المثال، قمت بوضع خادم إدارة تابع في DMZ.

ستحتاج لجهاز مثبت عليه وحدة تحكم إدارة والتي من خلالها يمكن الوصول إلى منافذ TCP رقم 13291 على كل من خادمي الإدارة: خادم الإدارة الرئيسي المفترض وخادم الإدارة الثانوي المفترض.

إضافة 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 العقدة خوادم الإدارة الخاصة بمجموعة الإدارة ذات الصلة، انقر فوق الرابط **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 الوكيل** وحدد إعدادات الاتصال.

7. اتبع إرشادات المعالج.

يتم إنشاء التسلسل الهرمي لخوادم الإدارة. سيُتلقى 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>.

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 تخصص 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 المستخدمين الأخرى والمستخدمين الفرديين المسجلين 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** بِنفاذة 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 موجوداً 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 مفتوحاً (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 يدوياً 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 مقاييس 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 محلياً.

وإذا قمت بتثبيت عميل الشبكة على جهاز محلياً، فيمكنك تحديد شهادة خادم الإدارة يدوياً.

تستخدم النسخة المنزلة 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 محلياً في محطة عمل المسؤول. وبعدها، في كل مرة تحاول فيها وحدة تحكم الإدارة الاتصال بخادم الإدارة، يتم تحديد الخادم بناءً على نسخة الشهادة.

إذا كانت شهادة خادم الإدارة غير مطابقة للنسخة المخزنة 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 14 Web Console (المشار إليها فيما يلي باسم Web Console) أو حيث يتم تثبيت وحدة التحكم الإدارية 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 مدرجاً 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:

- خدمة وحدة تحكم الويب

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

- تفاعل 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 و IPv6. 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\Program Files (x86)\Kaspersky Security Center (Lab)\Kaspersky Security Center).

3. أدخل الأمر التالي، باستخدام حقوق المسؤول:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v  
IP>" -t s
```

حدد عناوين IP التي تفي بالمطلوبات المذكورة أعلاه. يجب فصل عدة عناوين IP بفاصلة منقوطة.

مثال على كيفية السماح لجهاز واحد فقط بالاتصال بخادم الإدارة:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -  
ts
```

مثال على كيفية السماح لأجهزة متعددة بالاتصال بخادم الإدارة:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0  
ts- "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:

```
IP>" klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v  
-t 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:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0  
ts- "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:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s
```

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 klakout، 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 بتنفيذ الأمر التالي في سطر الأوامر:

```
klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -  
";"\svt BOOL_T -ss "|ss_type = \"SS_SETTINGS
```

2. 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 "|ss_type = \"SS_SETTINGS
```

يُرجع هذا الأمر النتيجة التالية:

```
(PARAMS_T) ---+  
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T>false---+
```

تعني القيمة الخاطئة أن المنفذ مغلق. خلاف ذلك، يتم عرض القيمة الحقيقية .

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 14 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 يمكنك 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 أضف 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.

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. يؤدي هذا الإجراء أيضاً 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. يؤدي هذا الإجراء أيضاً 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 وتأكد كلمة المرور فارغاً. إذا قمت بتحديد المستخدمين، أدخل كلمة مرور جديدة للمستخدم وقم بتأكيدهما.

سيتم تغيير حساب خدمة خادم إدارة إلى الحساب الذي قمت بتحديدته.

عند استخدام خادم Microsoft SQL Server في وضع يفترض مسبقاً 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 أحياناً إلى تغيير بيانات اعتماد DBMS، مثلاً 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.

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:

- 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.

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 %MMC%\Microsoft\Roaming\USERPROFILE%\AppData\Roaming\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 المعلومات 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 [بإستبدال 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 14 في Kaspersky Security Center في %MMC%\Microsoft\Roaming\USERPROFILE%\AppData\Roaming\MMC%.

3. قم بتشغيل وحدة تحكم إدارة Kaspersky Security Center.

سنتم 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 والتصحیحات
- 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 خانة 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 حول الأحداث 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).

في القسم **مستودع الأحداث** في نافذة 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.

إذا وصل عدد الأحداث في قاعدة البيانات إلى الحد الأقصى المحدد من قبل المسؤول، فيقوم التطبيق بحذف الأحداث الأقدم ويعيد أحداث جديدة عليها. عند قيام خادم الإدارة بحذف الأحداث القديمة، فلا يمكن حفظ الأحداث الجديدة في قاعدة البيانات. وأثناء هذه الفترة الزمنية، تتم كتابة معلومات حول الأحداث المرغوبة في سجل أحداث Kaspersky. يتم وضع الأحداث الجديدة في قائمة الانتظار ثم حفظها في قاعدة البيانات بعد اكتمال عملية الحذف.

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.

قم بما يلي 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 القسم **إعدادات اتصال خادم الإدارة**، حدد 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 الملف
ProgramData%\KasperskyLab\adminikit\logs\sc.syslog%

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 بنافذة 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 حدوث 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 زر **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 ونطاق 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 والنهاية. 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 فعالاً 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 و عميل 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 kbackup. تتضمن النسخة الاحتياطية جميع الإعدادات والكانتات 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 لعمل الشبكة على شبكة الشركة مرة أخرى. كما ستفقد أيضًا كل المفاتيح الرئيسية لتشفير محركات الأقراص الموجودة على الأجهزة المُدارة، 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 لتشتغل يوميًا في الساعة 4:00 صباحًا. ويتم حفظ النسخ الاحتياطية افتراضيًا في المجلد %Application Data\KasperskySC%\ALLUSERSPROFILE%.

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 الغير واضح مستنبط 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 kbackup يعملان على حماية النسخ الاحتياطية 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 المُدارة 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 وتحديثاته.

لتقليل حجم النسخ الاحتياطية لأدنى حد، قم بتمكين خيار **ضغط النسخ الاحتياطية** في إعدادات خادم SQL Server.

تتم الاستعادة من نسخة احتياطية باستخدام الأداة المساعدة kbackup 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 ستم عملية الاستعادة عليه باستخدام نظام إدارة قواعد بيانات من النوع نفسه (خادم SQL Server أو MySQL أو MariaDB) والإصدار نفسه (أو الأحدث). يمكن أن يكون إصدار خادم الإدارة هو نفسه (بتصحيح مشابه أو أحدث) أو إصدار أحدث.

يوضح هذا القسم السيناريو هات القياسية لإعدادات الاستعادة و كانتات خادم الإدارة.

استخدام لقطة نظام الملفات لتقليل مدة النسخ الاحتياطي

في Kaspersky Security Center 14، تم تقليل وقت حمول 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. وتقدم هذه الميزة خفضًا إضافيًا لوقت الحمول عن طريق استخدام الأداة المساعدة kbackup، 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 kbackup 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%KasperskyLab%\ALLUSERSPROFILE% على القرص المنطقي ذاته وأن يكونا محليين بالرجوع إلى خادم الإدارة.

- أن لا يحتوي المجلد %KasperskyLab%\ALLUSERSPROFILE% 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 يخزن مجلد %ALLUSERSPROFILE%. لاحظ أن حساب خدمة خادم الإدارة ليس لديها مثل هذا الإذن.

لاستخدام ميزة التقاط لقطه 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 لقطه لنظام الملفات للنسخ الاحتياطي للبيانات.
5. في الحقول اسم المستخدم وكلمة المرور، قم بإدخال اسم وكلمة مرور حساب لديه إذن إنشاء لقطات للقرص المنطقي الذي يخزن 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 القائمة بدء، قم بتشغيل الأداة المساعدة klbackup وإجراء الاستعادة.

إعدادات خادم الإدارة أو قاعدة البيانات تالفة

إذا تعذر تشغيل خادم الإدارة نتيجة لتلف الإعدادات أو قاعدة البيانات (على سبيل المثال، بعد حدوث تغيير 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.

أي محاولات لاستعادة خادم الإدارة من خلال برنامج تابع لجهة خارجية ستؤدي حتمًا إلى عدم مزامنة البيانات على عُقد تطبيق Kaspersky Security Center الموزع، وبالتالي عمل التطبيق بطريقة غير صحيحة.

النسخ الاحتياطي والاستعادة لبيانات خادم الإدارة

النسخ الاحتياطي للبيانات يسمح بنقل خادم الإدارة من جهاز إلى آخر دون فقدان للبيانات. باستخدام النسخ الاحتياطي، يمكنك استعادة البيانات عند نقل قاعدة بيانات خادم الإدارة إلى جهاز آخر، أو عند الترقية إلى إصدار أحدث من Kaspersky Security Center.

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 kbackup** 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 العملية.
- تخزين حزم توزيع التطبيقات للتثبيت عن بُعد.
- شهادة خادم الإدارة.

ولا يمكن استعادة بيانات خادم الإدارة إلا باستخدام أداة kbackup المساعدة.

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 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.

يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج. في نافذة **تحديد نوع المهمة** الخاصة بالمعالج، حدد نوع المهمة الذي يحمل الاسم **النسخ الاحتياطي لبيانات خادم الإدارة**.

يمكن إنشاء مهمة **النسخ الاحتياطي لبيانات خادم الإدارة** في نسخة مفردة فقط. إذا تم إنشاء مهمة نسخ احتياطي لبيانات خادم الإدارة بالفعل على خادم الإدارة، فلن تُعرض في نافذة اختيار نوع المهمة في "معالج إنشاء مهمة النسخ الاحتياطي".

الأداة المساعدة لنسخ البيانات احتياطيًا واستعادتها (kbackup)

يمكنك نسخ بيانات خادم الإدارة للنسخ الاحتياطي واسترجاعها في المستقبل باستخدام أداة kbackup المساعدة التي تعد جزءًا من حزمة توزيع Kaspersky Security Center.

ويمكن تشغيل أداة kbackup المساعدة في وضع من الوضعين التاليين:

- [التفاعلي](#)

- [غير التفاعلي](#)

النسخ الاحتياطي للبيانات واستعادتها في الوضع التفاعلي

لإنشاء نسخة احتياطية من بيانات خادم الإدارة في الوضع التفاعلي:

1. قم بتشغيل الأداة المساعدة kbackup الموجودة في مجلد تثبيت Kaspersky Security Center. يبدأ معالج الاستعادة والنسخ الاحتياطي.

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 فقط. انقر فوق التالي.

3. في النافذة التالية من المعالج، حدد الخيارات التالية:

- مجلد وجهة النسخ الاحتياطي

- [التحويل إلى تنسيق MySQL/MariaDB](#)

قم بتمكين هذا الخيار إذا كنت تستخدم خادم SQL حاليًا باعتباره DBMS لخادم الإدارة وتريد تحويل 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.

- [التحويل إلى تنسيق Azure](#)

قم بتمكين هذا الخيار إذا كنت تستخدم خادم SQL حاليًا باعتباره DBMS لخادم الإدارة وتريد [تحويل 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 ⑤

لقد تلقيت معرف المفتاح (عبارة عن تسلسل من الحروف الأبجدية الرقمية) عند إنشاء حساب مستخدم IAM للتعامل مع مثيل تخزين مستودع S3.
يكون الحقل متاحًا في حالة تحديد قاعدة بيانات RDS على مستودع S3.

• المفتاح السري ⑤

المفتاح السري الذي تلقينته مع معرف مفتاح الوصول عند إنشاء 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 للتحويل بدلاً من دور IAM.

• بالنسبة لـ Microsoft Azure:

• اسم حساب تخزين Azure ⑤

لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

• معرف اشتراك Azure ⑤

لقد قمت بإنشاء الاشتراك على مدخل Azure.

• كلمة مرور Azure ⑤

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 ⑤

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 أولاً بحذف اتصال Azure الموجود.

• اسم خادم Azure SQL Server ⑤

يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

• مجموعة مورد خادم Azure SQL Server ⑤

يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

يكون متاحًا في خصائص [حساب التخزين](#) الخاص بك، في قسم مفاتيح الوصول. يمكنك استخدام أي من المفاتيح (المفتاح 1 أو المفتاح 2).

لاستعادة بيانات خادم الإدارة في الوضع التفاعلي:

1. قم بتشغيل الأداة المساعدة k1backup الموجودة في مجلد تثبيت Kaspersky Security Center. يجب بدء الأداة المساعدة تحت نفس الحساب الذي استخدمته لتثبيت خادم الإدارة.
يبدأ معالج الاستعادة والنسخ الاحتياطي.

2. في النافذة الأولى من المعالج، حدد استعادة بيانات خادم الإدارة.
إذا قمت بتحديد خيار استعادة شهادة خادم الإدارة أو نسخها احتياطيًا فقط، فستتم استعادة شهادة خادم الإدارة فقط.
انقر فوق التالي.

3. في النافذة استعادة الإعدادات الخاصة بالمعالج:

- حدد المجلد الذي يحتوي على نسخة احتياطية من بيانات خادم الإدارة. يجب عليك التأكد أن الملف باسم backup.zip. إذا كنت تستخدم بيئة سحابة كـ AWS، أو Azure، حدد عنوان المخزن.

- 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 غير التفاعلي

لإنشاء نسخة احتياطية من بيانات خادم الإدارة أو استعادتها في الوضع غير التفاعلي:

قم بتشغيل الأداة k1backup التي تحتوي على مجموعة المفاتيح المطلوبة من سطر الأوامر بالجهاز المثبت عليه خادم الإدارة.

بناء جملة سطر الأوامر للأداة المساعدة:

```
k1backup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts][[-restore] [-password PASSWORD]
[[-online
```

إذا لم يتم تحديد كلمة مرور في سطر الأوامر بأداة k1backup المساعدة، فستطالبك الأداة بإدخال كلمة مرور بشكل تفاعلي.

مواصفات المفاتيح:

- path BACKUP_PATH - حفظ المعلومات في المجلد BACKUP_PATH أو استخدام بيانات من المجلد BACKUP_PATH لإجراء الاستعادة (معلمة إجباري).

- logfile LOGFILE - حفظ تقرير حول النسخ الاحتياطي لبيانات خادم الإدارة واستعادتها.

يجب منح حساب خادم قاعدة البيانات وأداة k1backup المساعدة الأذن الخاصة بتغيير البيانات في المجلد BACKUP_PATH.

- `use_ts` - عند حفظ البيانات، نسخ إلى المجلد `BACKUP_PATH`، إلى المجلد الفرعي الذي يحتوي اسمه على تاريخ النظام الحالي ووقت التشغيل بتنسيق `klbackup YYYY-MM-DD # HH-MM-SS`. إذا لم يتم تحديد مفتاح، يتم حفظ المعلومات في جذر المجلد `BACKUP_PATH`. 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 بأرشفيف بيانات خادم الإدارة. على سبيل المثال، إذا كان مفتاح المسار - يشير إلى المجلد `C:\KLBackups`، فسيقوم المجلد `klbackup 19/06/2022 # 11-30-18` بتخزين معلومات عن حالة خادم الإدارة اعتبارًا من 19 يونيو 2022 في تمام الساعة 11:30:18 ص.
- `restore` - استعادة بيانات خادم الإدارة. يتم إجراء استعادة البيانات بناءً على المعلومات الموجودة في المجلد `BACKUP_PATH`. وفي حالة عدم توفر مفتاح، يتم نسخ البيانات احتياطيًا في المجلد `BACKUP_PATH`.
- `savecert PASSWORD-PASSWORD` - حفظ شهادة خادم الإدارة أو استعادتها؛ لتشفير الشهادة أو فك تشفيرها، استخدم كلمة المرور المحددة حسب المعلمة `PASSWORD`.

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.

- `online-Backup` - 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.

نقل خادم إدارة إلى جهاز آخر

لنقل خادم إدارة إلى جهاز آخر:

1. قم بإنشاء نسخة احتياطية من بيانات خادم الإدارة.
2. قم بتثبيت خادم الإدارة على الجهاز المحدد.
3. لتبسيط عملية الحفاظ على هيكل مجموعات الإدارة، نوصيك بالتأكد من أن عنوان خادم الإدارة الجديد هو نفس عنوان خادم الإدارة القديم. يتم تحديد العنوان (أي اسم الجهاز في شبكة Windows أو عنوان IP) في إعدادات عميل الشبكة بخادم الإدارة في مجموعة إعدادات الاتصال بخادم الإدارة.
4. على خادم الإدارة الجديد، قم باستعادة بيانات خادم الإدارة من النسخة الاحتياطية.
5. إذا كان عنوان (أي اسم الجهاز في شبكة Windows أو عنوان IP) خادم الإدارة الجديد ليس هو نفسه عنوان خادم الإدارة القديم، فقم بتوصيل أجهزة العميل بخادم الإدارة الجديد عن طريق إنشاء مهمة تغيير خادم الإدارة لمجموعة الأجهزة المُدارة على خادم الإدارة القديم.
6. إذا كان العنوان هو نفسه، فلن تضطر إلى إنشاء هذه المهمة. سيتم الاتصال بالعنوان المحدد في الإعدادات.
7. احذف خادم الإدارة القديم.

إذا كنت تريد ذلك، فيمكنك أيضًا استخدام جهاز جديد لنظام إدارة قاعدة البيانات (DBMS). لنقل المعلومات بشكل صحيح، تأكد من أن نظام إدارة قاعدة البيانات الجديد (DBMS) لديه نفس مخططات الترتيب مثل القديم.

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 يتسبب ذلك، على سبيل المثال، في التثبيت عن بُعد للتطبيق نفسه على الجهاز نفسه من أكثر من خادم واحد وتضاربات أخرى. لتجنب حدوث مثل هذا الموقف، يتيح لك Kaspersky Security Center 14 [منع تثبيت تطبيق على جهاز مُدار بواسطة خادم إدارة آخر](#).

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](#)

يستخدم Kaspersky Security Center 14 الأساليب التجريبية لتحديد ما إذا كانت تتم إدارة الجهاز العميل بواسطة خادم الإدارة الذي تعمل به أو بواسطة خادم إدارة مختلف.

المصادقة الثنائية

هذا القسم يصف يمكنك استخدام المصادقة الثنائية لتقليل مخاطر الوصول غير المصرح به إلى وحدة تحكم الإدارة أو Kaspersky Security Center 14 Web Console.

السيناريو: تكوين المصادقة الثنائية 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 أيضاً 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 تبدأ:

- 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 قيام المستخدمين الآخرين لخادم الإدارة بتثبيت تطبيق مصدق على أجهزتهم.

المراحل

تمكين المصادقة الثنائية لجميع المستخدمين يتم في مراحل:

1 تثبيت تطبيق مصادقة على جهاز

يمكنك تثبيت Google Authenticator أو Microsoft Authenticator أو أي تطبيق مصادقة آخر يدعم خوارزمية كلمة المرور لمرة واحدة المستندة إلى الوقت.

2 مزامنة وقت تطبيق المصادقة مع وقت الجهاز المثبت عليه خادم الإدارة.

تأكد من أن الوقت المحدد في تطبيق المصادقة متزامن مع وقت خادم الإدارة.

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 14 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 لـ Kaspersky Security Center 14 Web Console: [تمكين المصادقة الثنائية لجميع المستخدمين](#)

5 تحرير اسم مُصدر 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 مُصدر رمز الأمان](#)

○ بالنسبة لـ Kaspersky Security Center 14 Web Console: [تحرير اسم مُصدر 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 لـ Kaspersky Security Center 14 Web Console: [استثناء الحسابات من المصادقة الثنائية](#)

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

يوفر Kaspersky Security Center 14 Web وحدة التحكم الإدارية أو Kaspersky Security Center Console. عند تمكين المصادقة الثنائية لحسابك الخاص، في كل مرة تقوم فيها بتسجيل الدخول إلى وحدة تحكم الإدارة أو Kaspersky Security Center 14 Web Console، 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 يكون لديك تطبيق مصادقة على جهاز الكمبيوتر لديك أو على جهازك المحمول.

رمز الحماية له معرّف يشار إليه باسم اسم المصدر. اسم مصدر رمز الأمان يُستخدم كمعرّف لخدمات الإدارة في تطبيق المصادقة. يمكنك تغيير اسم مصدر رمز الأمان. اسم مصدر رمز الأمان له قيمة افتراضية مماثلة لاسم خادم الإدارة. اسم المصدر يُستخدم كمعرّف لخدمات الإدارة في تطبيق المصادقة. إذا قمت بتغيير اسم مصدر رمز الأمان، يجب عليك إصدار مفتاح سري جديد وتمريضه إلى تطبيق المصادقة. رمز الحماية يُستخدم مرة واحدة وصالح لمدة تصل إلى 90 ثانية (قد يختلف الوقت المحدد).

يمكن لأي مستخدم تم تمكين المصادقة الثنائية له إعادة إصدار مفتاحه السري. عندما يقوم مستخدم بالمصادقة باستخدام المفتاح السري المعاد إصداره ويستخدمه لتسجيل الدخول، يحفظ خادم الإدارة المفتاح السري الجديد لحساب المستخدم. إذا أدخل المستخدم المفتاح السري الجديد بشكل غير صحيح، خادم الإدارة لن يحفظ المفتاح السري الجديد وسيترك المفتاح السري الحالي صالحًا للتصديق المستقبلي.

أي برنامج للمصادقة يدعم خوارزمية كلمة المرور لمرة واحدة المستندة إلى الوقت (TOTP) يمكن استخدامه كتطبيق للمصادقة، مثل Google Authenticator. لإنشاء رمز الأمان، يجب عليك مزمنة الوقت المحدد في تطبيق المصادقة مع الوقت المحدد لخادم الإدارة.

تطبيق المصادقة يُنشئ رمز الأمان على النحو التالي:

1. يقوم خادم الإدارة بإنشاء مفتاح سري خاص ورمز استجابة سريعة.
2. أنت تمرر المفتاح السري الذي تم إنشاؤه أو رمز الاستجابة السريعة إلى تطبيق المصادقة.
3. تطبيق المصادقة يُنشئ رمز أمان للاستخدام مرة واحدة تقوم بتمريره إلى نافذة المصادقة لخادم الإدارة.

نوصي بشدة بتثبيت تطبيق المصادقة على أكثر من جهاز محمول. احفظ المفتاح السري (أو رمز الاستجابة السريعة)، واحتفظ به في مكان آمن. سيساعدك هذا في استعادة الوصول إلى وحدة تحكم الإدارة أو Kaspersky Security Center 14 Web Console في حالة فقدان الوصول إلى جهازك 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.

المصادقة الثنائية تعمل وفق القواعد التالية:

- فقط حساب المستخدم الذي يملك حق [تعديل قوائم التحكم في الوصول للكائن](#) مباشرةً في المجال الوظيفي [الميزات العامة: أذونات المستخدم](#) تمكين المصادقة الثنائية لجميع المستخدمين.
- يمكن فقط للمستخدم الذي قام بتمكين المصادقة الثنائية لحسابه الخاص أن يقوم بتمكين خيار المصادقة الثنائية لجميع المستخدمين.
- يمكن فقط للمستخدم الذي قام بتمكين المصادقة الثنائية لحسابه الخاص أن يقوم باستثناء حسابات مستخدمين آخرين من قائمة المصادقة الثنائية التي تم تمكينها لجميع المستخدمين.
- يمكن للمستخدم تمكين المصادقة الثنائية لحسابه فقط.
- يمكن لحساب المستخدم الذي لديه حق [تعديل قوائم التحكم في الوصول للكائن](#) مباشرةً في المجال الوظيفي [الميزات العامة: أذونات المستخدم](#) ومسجل الدخول إلى وحدة تحكم الإدارة أو Kaspersky Security Center 14 Web Console باستخدام المصادقة الثنائية أن يقوم بتعطيل المصادقة الثنائية لأي مستخدم آخر فقط إذا تم تعطيل المصادقة الثنائية لجميع المستخدمين، ولمستخدم مستثنى من قائمة المصادقة الثنائية التي تم تمكينها لجميع المستخدمين.
- يمكن لأي مستخدم قام بتسجيل الدخول إلى وحدة تحكم أو Kaspersky Security Center 14 Web Console الإدارة باستخدام المصادقة الثنائية إعادة إصدار مفتاحه السري.

- يمكنك تمكين خيار المصادقة الثنائية لجميع المستخدمين لخادم الإدارة الذي تعمل معه حالياً. إذا قمت بتمكين هذا الخيار على خادم الإدارة، أنت تقوم كذلك بتمكين هذا الخيار لحسابات المستخدمين لخوادم الإدارة الافتراضية الخاصة بها، ولا تقوم بتمكين المصادقة الثنائية لحسابات المستخدمين لخوادم الإدارة الثانوية.

إذا كانت المصادقة الثنائية مفعلة لحساب مستخدم على خادم إدارة Kaspersky Security Center الإصدار 13 أو أعلى، لن يقدر المستخدم على تسجيل الدخول إلى Kaspersky Security Center Web Console 12 أو 12.1 أو 12.2.

تمكين المصادقة الثنائية لحسابك الخاص

قبل أن تقوم بتمكين المصادقة الثنائية لحسابك، تأكد من تثبيت تطبيق مصادقة على جهازك 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**.
في نافذة خصائص المصادقة الثنائية التي تفتح، يتم عرض المفتاح السري.
 4. أدخل المفتاح السري في تطبيق المصادقة لتلقي رمز الحماية لمرة واحدة. يمكنك تحديد المفتاح السري في تطبيق المصادقة يدوياً أو مسح رمز الاستجابة السريعة ضوئياً باستخدام جهازك المحمول.
 5. حدد رمز الحماية الذي تم إنشاؤه عبر تطبيق المصادقة ثم انقر على زر **موافق** للخروج من نافذة خصائص المصادقة الثنائية.
 6. انقر على زر **تطبيق**.
 7. انقر على زر **موافق**.
- بهذا تم تمكين المصادقة الثنائية لحسابك الخاص.

تمكين المصادقة الثنائية لجميع المستخدمين

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 مصرحاً لك استخدام المصادقة الثنائية. إذا لم تقم بتمكين المصادقة الثنائية لحسابك قبل تمكينها لجميع المستخدمين، فإن التطبيق يفتح نافذة **لتمكين المصادقة الثنائية لحسابك الخاص أولاً**.

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. 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 المصادقة الثنائية لحساب مستخدم

لتعطيل المصادقة الثنائية لحسابك الشخصي:

1. في شجرة وحدة التحكم - 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 المصادقة الثنائية لحساب مستخدم آخر فقط إذا كان لديك حق **تعديل قوائم التحكم في الوصول للكائن** مباشرةً في المجال الوظيفي **الميزات العامة: أدونات المستخدم**. 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.

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.

تعطيل المصادقة الثنائية لجميع المستخدمين

يمكنك تعطيل المصادقة الثنائية لجميع مستخدمي خادم الإدارة إذا كان لديك حق [تعديل قوائم التحكم في الوصول للكائن](#) مباشرة في المجال الوظيفي الميزات العامة: **أدوات المستخدم** وإذا كان مصرحًا لك باستخدام المصادقة الثنائية.

لتعطيل المصادقة الثنائية لجميع المستخدمين:

1. في شجرة وحدة التحكم - 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.

استثناء الحسابات من عملية المصادقة الثنائية

يمكنك استثناء حساب من المصادقة الثنائية إذا كان حسابك له حق [تعديل قوائم التحكم في الوصول للكائن](#) مباشرة في المجال الوظيفي الميزات العامة: **أدوات المستخدم**.

إذا تم استثناء حساب مستخدم من المصادقة الثنائية، يمكن لهذا المستخدم تسجيل الدخول إلى وحدة تحكم الإدارة أو Kaspersky Security Center 14 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**.
3. في مساحة العمل، انقر نقرًا مزدوجًا على حساب المستخدم الذي ترغب في استثناءه 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 المستثناءة في [قائمة حسابات المستخدمين](#).

تحرير اسم مُصدر رمز الأمان

يمكن أن يكون لديك العديد من المعارف (يطلق عليها المصدرون) لخوادم الإدارة المختلفة. يمكنك تغيير اسم مُصدر رمز الأمان إذا كان مثلاً خادم الإدارة يستخدم بالفعل اسماً مشابهاً 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 وتمريه إلى تطبيق المصادقة.

لتحديد اسم جديد لمُصدر 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 **مصدر 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.

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 هيكلية 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 تلقائياً على الأجهزة المضمنة في مجموعة.
- لا يمكنك القيام بهذه الإجراءات إلا في حالة امتلاكك **إذن التعديل** في 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 المُدارة. 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 ستضمن 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.

بدء 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 وخواصم 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 تنتقل إليه مجموعة الإدارة، فينبغي عليك تغيير اسم المجموعة التي يتم نقلها. إذا لم يتم نقلها. إذا تم تغيير 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 المُدارة 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 خواصم 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 خواصم الإدارة الثانوية والمجموعات المتداخلة والأجهزة العميلة من هذه المجموعة.

لحذف مجموعة:

1. حدد مجموعة إدارة في شجرة وحدة التحكم.

- 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 المعالج 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 المحدد 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 يؤثر 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 مضمناً في المجموعة **الأجهزة غير المخصصة** لأي سبب كان (تم إيقاف تشغيله أو قطع اتصاله بالشبكة)، فلن يتم نقل الجهاز تلقائياً إلى مجموعة الإدارة. يمكنك إضافة أجهزة إلى مجموعات الإدارة يدوياً 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**.
- بدء 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 التي تم إضافتها مؤخراً إلى مجموعة.

لتكوين تثبيت تلقائي للتطبيقات على الأجهزة الجديدة في مجموعة الإدارة:

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 الجديدة.
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 محدثة 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 وفقاً لإعدادات عميل الشبكة (كل 15 دقيقة على سبيل المثال). ويمكنك تحديد الفاصل الزمني للاتصال يدوياً.

يتم تسليم معلومات حول الحدث إلى خادم الإدارة حال حدوثها.

إذا كان خادم الإدارة موجوداً 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 مفتوحاً (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 يدوياً 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 نشطاً 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 يدوياً، يستخدم النظام طريقة اتصال بديلة، تسمح ببدء الاتصال بواسطة خادم الإدارة. قبل إنشاء اتصال على جهاز عميل، يجب عليك فتح منفذ UDP. إذ يرسل 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 يدوياً. 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 تلقائياً إلى مجلد تثبيت عميل الشبكة.

لتوصيل جهاز عميل بخادم الإدارة يدوياً 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.

بناء جملة سطر الأوامر للأداة المساعدة:

```
klmover [-logfile <file name>] [-address <server address>] [-pn <port number>] [-ps  
[<SSL port number>] [-nossll] [-cert <path to certificate file>] [-silent] [-dupfix
```

حقوق المسؤول مطلوبة لتشغيل الأداة.

مواصفات المفاتيح:

- `-logfile <file name>` – تسجيل نتائج تشغيل الأداة المساعدة في ملف سجل. يتم حفظ المعلومات افتراضياً في دفق الإخراج القياسي (stdout). إذا لم يكن المفتاح مستخدماً، فسيتم عرض النتائج ورسائل الخطأ على الشاشة.
- `-address <server address>` – عنوان خادم الإدارة للاتصال. يمكنك تحديد عنوان IP أو اسم NetBIOS أو اسم DNS الخاص بالجهاز كعنوانه.
- `-pn <port number>` – 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.
- `-nossll` – استخدام اتصال غير مشفر بخادم الإدارة. إذا لم يكن المفتاح مستخدماً، 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 مستخدماً، فسيتم تلقي عميل الشبكة شهادة في الاتصال الأول بخادم الإدارة.
- `-silent` – تشغيل الأداة المساعدة في وضع السكون. ربما يكون استخدام المفتاح مفيداً، إذا تم بدء تشغيل الأداة المساعدة مثلاً من برنامج تسجيل الدخول عند تسجيل المستخدم.
- `-dupfix-ISO` – المفتاح مستخدم إذا تم تثبيت عميل الشبكة باستخدام طريقة تختلف عن الطريقة المعتادة (مع حزمة التوزيع) – مثل استعادته من صورة قرص.

نفق اتصال أحد الأجهزة العملية 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 مثبت 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 أيضاً تمكين الأنفاق عن طريق استخدام أدوات خارجية. على سبيل المثال، يمكن للمسؤول تشغيل الأداة المساعدة putty و عميل VNC والأدوات الأخرى بهذه الطريقة.

نقذ اتصال بين جهاز عميل بعيد وخدام 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 و UDP بالجهاز العميل.

عند إنشاء اتصال مع الجهاز، يكون للمسؤول حق الوصول الكامل للمعلومات المخزنة على هذا الجهاز ليتمكن من إدارة التطبيقات المثبتة عليه.

يمكن إنشاء اتصال عن بُعد بجهاز بإحدى الطرق التالية:

- عن طريق استخدام مكون Microsoft Windows القياسي المسمى Remote Desktop Connection. يتم إنشاء اتصال سطح المكتب عن بُعد عبر أداة Windows القياسية mstsc.exe وفقًا لإعدادات الأداة.
- تم إنشاء اتصال بجلسة سطح المكتب البعيد للحالية للمستخدم دون علم المستخدم. بمجرد اتصال المسؤول بالجلسة، يتم قطع اتصال مستخدم الجهاز من الجلسة دون إخطار مسبق.
- عن طريق استخدام تقنية 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 نتائجها 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:

- يتم تثبيت Microsoft Windows Vista أو إصدار نظام تشغيل أحدث من Windows على الجهاز.
- يتطلب 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.
- يستخدم Kaspersky Security Center ترخيصًا لإدارة الثغرات الأمنية والتصحيات.

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.

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، فسيُوفر 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**.

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**.

سنتفتح نافذة **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 خانة الاختيار المقابلة وإعدادات الوقت في مربعات الزيادة والنقصان.

6. انقر فوق موافق لحفظ التغييرات وعلق 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 خانة الاختيار تمكين التدقيق.

6. في القوائم أقنعة الملفات التي ينبغي مراقبتها عند قراءتها وأقنعة 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 odt و pdf افتراضياً.

7. انقر فوق موافق لحفظ التغييرات وعلق 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 (مثل 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 أداة klnagchk المساعدة.

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

يمكن للأداة المساعدة klnagchk عند بدء تشغيلها من سطر الأوامر القيام بالإجراءات التالية (بناءً على المفاتيح المستخدمة):

- عرض، على الشاشة أو تسجيلها، قيم الإعدادات المستخدمة لاتصال عميل الشبكة المثبت على الجهاز بخادم الإدارة.
 - تسجيل إحصائيات عميل الشبكة في ملف سجل الأحداث (منذ آخر مرة بدأ تشغيلها) ونتائج تشغيل الأداة المساعدة، أو عرض المعلومات على الشاشة.
 - إجراء محاولة لإنشاء 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 أداة klnagchk المساعدة،

على الجهاز، ابدأ تشغيل أداة klnagchk المساعدة من سطر الأوامر.

بناءً جملة سطر الأوامر للأداة المساعدة:

```
[restart-] [ <المسار إلى ملف الشهادة> ] klnagchk [-logfile <file name>] [-sp] [-savecert
```

مواصفات المفاتيح:

- `-logfile <file name>` - تسجيل 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 الإعداد قيد الاستخدام في حالة إنشاء اتصال بخادم الإدارة من خلال خادم وكيل.

• -savecert <file name> - حفظ الشهادة المستخدمة للوصول إلى خادم الإدارة في الملف المحدد.

• - إعادة التشغيل -إعادة تشغيل عميل الشبكة بعد اكتمال الأداة المساعدة.

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 العملية على خادم الإدارة

يتم تحديد الأجهزة العملية بناءً على أسمائها. ويكون اسم الجهاز فريداً بين جميع أسماء الأجهزة المتصلة بخادم الإدارة.

ويتم نقل اسم الجهاز إلى خادم الإدارة عند استقضاء شبكة Windows واكتشاف جهاز جديد بها أو عند أول اتصال لعميل الشبكة المثبت على الجهاز بخادم الإدارة. افتراضياً، يكون الاسم مطابقاً 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: **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 التعديل** في نطاق إدارة مجموعات الإدارة لكلاً 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 العملية 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 يدوياً، 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 وتُعرض 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. اتصل بخادم الإدارة الذي يتولى إدارة الأجهزة.

2. أنشئ مهمة تغيير خادم الإدارة عن طريق إحدى الطرق التالية:

• إذا كنت بحاجة لتغيير خادم الإدارة للأجهزة التي تم تضمينها في مجموعة الإدارة المحددة، فقم بإنشاء مهمة لمجموعة محددة.

• إذا كنت بحاجة لتغيير خادم الإدارة للأجهزة التي تم تضمينها في مجموعات إدارة مختلفة أو في مجموعة بخلاف المجموعات الحالية، فقم بإنشاء مهمة لأجهزة خاصة.


يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج. في نافذة تحديد نوع المهمة الخاصة بمعالج مهمة جديدة، حدد عقدة **Kaspersky Security Center** وافتح المجلد **خيارات متقدمة** وحدد مهمة **تغيير خادم الإدارة**.

3. 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.

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 المستخدم من الوصول إلى البيانات المشفرة فقط التي عملوا عليها مسبقاً. 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](#) عبر الإنترنت.

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 جزءاً من مصفوفة خادم، فيصبح هذا الجهاز العميل عقدة نظام المجموعة. سيتم إضافة المجموعة بوصفها كائن فردي في مجلد **الأجهزة المُدارة** الخاص بشجرة وحدة التحكم مع رمز .

يمكن تمييز بعض الميزات النموذجية لنظام المجموعة:

- يكون نظام الإدارة والعقد الخاصة به دائماً 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.

يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج. في نافذة **تحديد نوع المهمة** الخاصة بمعالج مهمة جديدة، حدد العقدة **Kaspersky Security Center** وافتح المجلد **خيارات متقدمة** وحدد مهمة **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 (لفرض تطبيق نهج ما مثلاً)، سيرسل خادم الإدارة حزمة شبكة موقعة إلى عميل الشبكة على المنفذ UDP 15000 (يمكن لخادم الإدارة إرسال هذه الحزمة عبر شبكة IPv4 أو IPv6). إذا لم يكن الاتصال عبر UDP ممكنًا بين خادم الإدارة وجهاز مُدار لأي سببٍ من الأسباب، سيتم تشغيل المزامنة عند الاتصال الروتيني التالي بين عميل الشبكة وخادم الإدارة خلال 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 اختبار 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 تم إجراء المزامنة بالفعل أم لا لجهاز محدد في الوقت الحالي.

في قائمة السياق الخاصة بالأجهزة المدارة في وحدة تحكم الإدارة، يحتوي عنصر القائمة **جميع المهام على الأمر فرض المزامنة**. عندما ينفذ Kaspersky Security Center 14 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.

يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.

3. في نافذة نوع المهمة الخاصة بمعالج مهمة جديدة، حدد العقدة خادم إدارة **Kaspersky Security Center 14**، وافتح المجلد خيارات متقدمة، وحدد مهمة إرسال رسالة إلى المستخدم. 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 المجلد حسابات المستخدمين.

إدارة Kaspersky Security for Virtualization

يدعم Kaspersky Security Center خيار اتصال الأجهزة الظاهرية بخادم الإدارة. تتم إدارة الأجهزة الظاهرية من خلال 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 لجهاز 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 النافذة خصائص التي تفتح في الجزء 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 المقفل في السياسة الأصلية.

4. حدد القيمة المطلوبة للحالة المحددة.

يمكنك تعيين قيم لبعض الشروط، ولكن ليس جميعها.

5. انقر على موافق.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار على 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. من النافذة خصائص المهمة التي تفتح، في الجزء 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. حدد القيمة المطلوبة للحالة المحددة.

يمكنك تعيين قيم لبعض الشروط، ولكن ليس جميعها.

5. انقر على موافق.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار على تحذير .

وضع العلامات على الأجهزة وعرض العلامات المعينة

يتيح Kaspersky Security Center وضع العلامات للأجهزة. 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 كشرط 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 ساع في مجموعة إدارة المستخدمين وإذا تم تمكين تفعيل ملف تعريف السياسة المقابلة بواسطة علامة ساع، 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** بدلاً 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 زر **إضافة**.
يتم فتح النافذة **قاعدة قاعدة جديدة**.
5. في النافذة **قاعدة 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 خانة الاختيار **تمكين القاعدة** بشكل افتراضي.

- في الحقل **علامة**، أدخل اسم علامة.

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** لتحديد شرط موجود.

سنتفتح نافذة معالج شرط قاعدة وضع العلامة تلقائيًا الجديد.

7. في النافذة **معالج شرط تعيين العلامة**، حدد خانة 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، وتضمنين الجهاز في مجال أو شبكة IP فرعية.
- **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**—تضمنين الجهاز في نوع محدد من الأجهزة الظاهرية.
- **تم تثبيت تطبيق من سجل التطبيقات**—وجود تطبيقات لبايعين مختلفين على الجهاز.

9. بعد إعداد الشرط، أدخل اسمًا له، ثم أغلق 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 إنشاؤها 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. سيُسري 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 التنبع، تغيير مستوى التنبع، تنزيل ملف التنبع.

• تنزيل معلومات النظام وإعدادات التطبيق.

• تنزيل سجلات الأحداث.

• إنشاء ملف تفرغ 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 التفرغ 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 بُعد.
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 وكلمة 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.

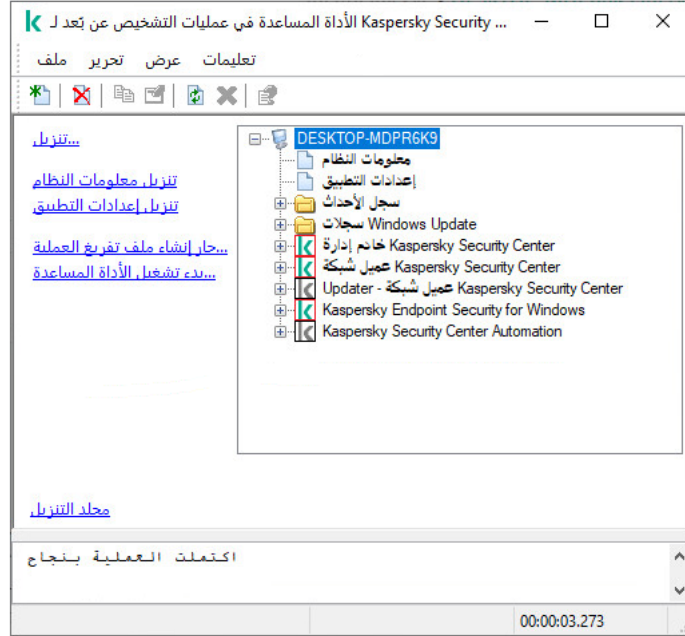
القيمة الافتراضية هي عنوان خادم الإدارة الذي يتم منه تشغيل الأداة المساعدة.

• إذا لزم الأمر، حدد خانة الاختيار استخدام SSL، وضغط حركة المرور، وينتمي 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.

يجب عليك أخذ التصريح باستخدام [التحقق المزدوج](#) إذا تم تمكين التحقق المزدوج 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.

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 لعمل الشبكة، يمكنك أيضاً القيام بذلك أثناء إنشاء مهمة [تنصيب التحديثات المطلوبة وإصلاح الثغرات الأمنية](#). في هذه الحالة، سيقوم عميل الشبكة بكتابة معلومات التتبع وذلك حتى في حالة تعطيل التتبع لعمل 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 9**

يحدد مستوى التتبع مقدار التفاصيل التي يحتويها ملف التتبع.

• **التتبع القائم على التدوير 9** (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 9**

يحتوي ملف التتبع من هذا النوع على الحد الأدنى لمقدار المعلومات حول النظام. يتم تحديد هذا الخيار افتراضيًا.

• **مستوى عميق 9**

يحتوي ملف التتبع من هذا النوع على معلومات مفصلة مقارنة بملفات التتبع من النوع البسيط، وقد يطالبك أخصائي الدعم الفني بتحديدده 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 9**

يتم استقبال معلومات التتبع أثناء تشغيل تطبيق Kaspersky Endpoint Security. يتم تحديد هذا الخيار افتراضيًا.

• **النوع القائم على إعادة التشغيل 9**

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

• جار إنشاء ملف تفرغ العملية

في النافذة التي تفتح بعد أن تنقر فوق هذا الرابط، حدد الملف التنفيذي للتطبيق الذي تريد إنشاء ملف تفرغ 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 **سجل الأحداث** 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 التفرغ.

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 خانة الاختيار الموجودة بجوار العناصر التي تريد تنزيلها.
 4. انقر **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 حديثاً 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 خادِم 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 Kaspersky Anti-Virus for UEFI متكامل 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 خادِم الإدارة المطلوب.

2. في قائمة السياق لخادِم الإدارة، حدد خصائص.

3. في نافذة خصائص خادِم الإدارة، حدد إعدادات الاتصال بالخادِم < 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 بخادِم 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 مدار:

1. في شجرة وحدة التحكم، حدد 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

تحديد تاريخ آخر تحديث لقواعد البيانات أو التطبيقات على الجهاز.

• آخر وقت مرئي ⑤

التاريخ والوقت اللذين كان فيهما الجهاز مرئيًا على الشبكة.

• تم الاتصال بخادم الإدارة ⑤

تاريخ ووقت تثبيت عميل الشبكة على آخر جهاز عميل تم توصيله بخادم الإدارة.

• عدم قطع الاتصال عن خادم الإدارة ⑤

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، فسيتم فصل 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 ممكنًا حتى إذا حاولت تعطيله.

الحماية

يقدم القسم الحماية معلومات حول الحالة الحالية للحماية ضد الفيروسات على الجهاز العميل:

• حالة الجهاز ⑤

يتم تعيين حالة الجهاز بناء على المعايير التي حددها المسؤول عن حالة الحماية ضد الفيروسات على الجهاز وعن نشاط الجهاز على الشبكة.

• كل المشكلات ⑤

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 ⑤

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 ⑤

تاريخ ووقت آخر فحص للفيروسات أُجري على الجهاز العميل.

• إجمالي عدد التهديدات المكتشفة ⑤

العدد الإجمالي للتهديدات المكتشفة على الجهاز العميل منذ تثبيت تطبيق مكافحة الفيروسات (الفحص الأول) أو منذ آخر إعادة تعيين لعداد الفيروسات.

• [تهديدات نشطة](#) 9

عدد الملفات التي لم تتم معالجتها على الجهاز العميل.
يتجاهل هذا الحقل عدد الملفات التي لم تتم معالجتها على الأجهزة المحمولة.

• [حالة تشفير القرص](#) 9

الحالة الحالية لتشفير الملفات على محركات أقراص الجهاز المحلية.

التطبيقات

يقوم قسم **التطبيقات** بإدراج جميع تطبيقات Kaspersky المثبتة على الجهاز العميل:

• [الأحداث](#) 9

انقر على زر لعرض قائمة بالأحداث التي وقعت على الأجهزة العميلة عندما تم تشغيل التطبيق، ولعرض نتائج المهمة لهذا التطبيق.

• [إحصائيات](#) 9

انقر فوق هذا الزر لعرض المعلومات الإحصائية الحالية حول التطبيق.

• [خصائص](#) 9

انقر على الزر لتلقي معلومات حول التطبيق وكذلك لتكوين التطبيق.

المهام

في القسم **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. إذا لم يتم إنشاء الاتصال، فلا يتم عرض الحالة.

أحداث

يعرض القسم **الأحداث** الأحداث المسجلة على خادم الإدارة للجهاز العميل المحدد.

العلامات

في القسم **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**. يتم توفير معلومات حول التطبيقات المثبتة للأجهزة التي تعمل بنظام تشغيل Windows فقط.

يوفر عميل الشبكة معلومات حول التطبيقات اعتمادًا على البيانات التي يتم استلامها من سجل النظام.

• 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، فسيتم 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.

الجلسات

يعرض القسم الجلسات معلومات حول مالك الجهاز العميل، بالإضافة إلى حسابات المستخدمين الذين استخدموا الجهاز 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 وخصائص 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.

الحوادث

في القسم **الحوادث**، يمكنك عرض الحوادث وتحريرها وإنشاؤها للجهاز العميل. يمكن إنشاء الحوادث 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 حادث. يمكن للمسؤول توفير وصف مختصر للحالة والإجراءات الموصى بها (مثل الإجراءات التأديبية التي سيتم اتخاذها ضد المستخدم) في نص الحادث، ويمكنه إضافة رابط للمستخدم أو المستخدمين.

يُطلق على حادث تم اتخاذ جميع الإجراءات المطلوبة بشأنه اسم تمت المعالجة. قد يتم اختيار وجود حوادث غير معالجة كشرط لتغيير حالة الجهاز إلى حرج أو تحذير.

يحتوي هذا القسم على قائمة بالحوادث التي تم إنشاؤها للجهاز. يتم تصنيف الحوادث بحسب مستوى الخطورة وبحسب النوع. يتم تحديد نوع الحادث بواسطة تطبيق Kaspersky، الذي يقوم بإنشاء الحادث. يمكنك تمييز الحوادث 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 المُحدّد 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 وحدة تحكم الويب الخاصة بـ [Kaspersky Security Center 14](#)).

• عرض قائمة الإصلاحات الموصى بها للثغرة الأمنية.

• حدد تحديثات البرامج يدويًا لإصلاح الثغرات الأمنية (في وحدة تحكم الإدارة أو في [Kaspersky Security Center 14 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.

• [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 افتراضياً.

سياسات نشطة

يعرض هذا القسم قائمة بسياسات تطبيق Kaspersky المفعلة حالياً 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 العملية. 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 ⑤

إذا تم تحديد هذا الخيار، تصبح السياسة نشطة.
يتم تحديد هذا الخيار افتراضياً.

• سياسة الوجود خارج المكتب ⑤

إذا تم تحديد هذا الخيار، تصبح السياسة نشطة عندما يغادر الجهاز شبكة الشركة.

• سياسة غير نشطة ⑤

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 ⑤

إذا تم تمكين هذا الخيار، يتم توريث قيم إعدادات السياسة من سياسة المجموعة ذات المستوى الأعلى؛ ولهذا يتم إلغاء تأمينها.
يتم تمكين هذا الخيار افتراضياً.

• فرض توريث الإعدادات في السياسات الفرعية ⑤

إذا تم تمكين هذا الخيار، يتم تنفيذ الإجراءات التالية بعد تطبيق تغييرات السياسة:

- سيتم توزيع قيم إعدادات السياسة على سياسات مجموعات الإدارة المتداخلة أي على السياسات الفرعية.
- في كتلة توريث الإعدادات الخاصة بالقسم عام في نافذة الخصائص لكل سياسة فرعية، سيتم تمكين الخيار توريث الإعدادات من السياسة الأصلية تلقائياً.

إذا تم تمكين هذا الخيار، فسيتم تأمين إعدادات السياسة الفرعية.
يتم تعطيل هذا الخيار افتراضياً.

تكوين الحدث

يتيح لك القسم تكوين الحدث 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 ومدة 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 **تخصيص**، يمكنك تكوين نوع حدث **وقوع حادث**. 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 **وقوع حادث**، حدده وانقر على زر **خصائص**. بعد ذلك، يمكنك تحديد مكان تخزين الأحداث التي وقعت وكيفية الإبلاغ عنها.

إذا اكتشف عميل الشبكة حادثًا، فيمكنك إدارة هذا الحادث 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.

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 على سياسات مجموعات الإدارة المتداخلة أي على السياسات الفرعية.
 - في كثة 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 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 ومدة 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 **وقوع حادث**. 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 **وقوع حادث**، حدده وانقر على زر **خصائص**. بعد ذلك، يمكنك تحديد مكان تخزين الأحداث التي وقعت وكيفية الإبلاغ عنها.

إذا اكتشف عميل الشبكة حادثًا، فيمكنك إدارة هذا الحادث 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 المدارة **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 ⑤

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 الذي تتم إدارته
- اسم السياسة المفعلة أو خارج المكتب في لحظة تسليم السياسة إلى الجهاز الذي تتم إدارته
- الاسم والمسار الكامل لمجموعة الإدارة التي كانت تحتوي على الجهاز الذي تتم إدارته في لحظة تسليم السياسة إلى الجهاز الذي تتم إدارته
- قائمة ملفات تعريف السياسة المفعلة
- يمكنك استخدام المعلومات لضمان تطبيق السياسة الصحيحة على الجهاز ولأغراض استكشاف الأخطاء وإصلاحها. يتم تعطيل هذا الخيار افتراضياً.

• حماية خدمة عميل الشبكة من عمليات الإزالة أو الإنهاء غير المصرح بها، ومنع إجراء تغييرات في الإعدادات ⑤

بعد تثبيت عميل الشبكة على جهاز مُدار، يتعذر إزالة المكون أو إعادة تكوينه دون الامتيازات المطلوبة. يتعذر إيقاف خدمة عميل الشبكة.
يتم تعطيل هذا الخيار افتراضياً.

• استخدام كلمة مرور إلغاء التثبيت ⑤

إذا تم تمكين هذا الخيار، فيمكنك تحديد كلمة المرور لإزالة تثبيت عميل الشبكة عن بُعد بالنقر فوق زر **تعديل**.
يتم تعطيل هذا الخيار افتراضياً.

المستودعات

في القسم **المستودعات**، يمكنك تحديد أنواع الكائنات التي سيتم إرسال تفاصيلها من عميل الشبكة إلى خادم الإدارة. إذا كان تعديل بعض الإعدادات في هذا القسم ممنوعاً في سياسة عميل الشبكة، فلا يمكنك تعديلها. تتوفر الإعدادات الموجودة في القسم **المستودعات** فقط على الأجهزة التي تعمل بنظام التشغيل Windows:

• تفاصيل تحديثات Windows Update ⑤

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 افتراضياً. إنه متاح فقط لنظام التشغيل Windows.

• تفاصيل الثغرات الأمنية بالبرنامج والتحديثات المطابقة لها ⑤

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 وكيل الشبكة. يتم تمكين هذا الخيار افتراضياً. 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.

• [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 افتراضياً.

• [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 افتراضياً. إنه متاح فقط لنظام التشغيل Windows.

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. الإعدادات الموجودة في قسم تحديثات البرنامج والثغرات الأمنية متوفرة فقط على الأجهزة التي تعمل بنظام Windows:

• [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 افتراضياً.

• **ضمن السماح للمستخدمين بإدارة تثبيت تحديثات Windows Update، يمكنك تقييد تحديثات Windows التي يمكن للمستخدمين تثبيتها يدوياً 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 بدلاً 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 أولاً 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 العمل.

عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلاً 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.

• **سليبي**

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 مجدداً، 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 9

إذا تم تمكين هذا الخيار، فيستمر مسح الملفات التنفيذية ضوئياً للعثور على الثغرات الأمنية عند تشغيلها.
يتم تمكين هذا الخيار افتراضياً.

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. لا تتوفر الإعدادات الموجودة إلا في قسم إدارة إعادة التشغيل على الأجهزة التي تعمل بنظام التشغيل Windows:

• عدم إعادة تشغيل نظام التشغيل 9

لن يتم إعادة تشغيل نظام التشغيل

• إعادة تشغيل نظام التشغيل تلقائياً عند الحاجة 9

إذا لزم الأمر، يتم إعادة تشغيل نظام التشغيل تلقائياً.

• مطالبة المستخدم باتخاذ إجراء 9

يقوم التطبيق بمطالبة المستخدم بالسماح بإعادة تشغيل نظام التشغيل.
يتم تحديد هذا الخيار افتراضياً.

• تكرار المطالبة كل (بالدقائق) 9

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بمطالبة المستخدم 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 افتراضياً.

• فرض إعادة التشغيل بعد (دقيقة) 9

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 افتراضياً.

• فترة الانتظار قبل فرض إغلاق التطبيقات في الجلسات المحجوبة (بالدقائق) 9

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. لا تتوفر الإعدادات الموجودة إلا في قسم **مشاركة سطح المكتب لـ Windows** على الأجهزة التي تعمل بنظام التشغيل Windows:

• **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. يتوفر التثبيت التلقائي للتصحيحات ذات الحالة غير المحددة للإصدار Kaspersky Security Center 10 Service Pack 2 والإصدارات اللاحقة.

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) 9

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 بشكل 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 و macOS 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 للزمنية للمزامنة بين أجهزة العميل وخادم الإدارة:

• ضغط حركة مرور الشبكة 9

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 9

إذا تم تمكين هذا الخيار، فستتم إضافة منفذ UDP، اللازم لعمل عميل الشبكة، إلى قائمة استثناء جدار حماية Microsoft Windows. يتم تمكين هذا الخيار افتراضياً.

• استخدام SSL

في حال تمكين هذا الخيار، يتم إجراء الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL. يتم تمكين هذا الخيار افتراضياً.

• استخدام 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 افتراضياً.

• استخدام منفذ UDP

إذا احتجت أن تكون الأجهزة المُدارة متصلة بخادم وكيل KSN عبر منفذ UDP، فقم بتمكين خيار استخدام منفذ UDP وحدد رقم منفذ UDP. يتم تمكين هذا الخيار افتراضياً. والمنفذ الافتراضي لـ UDP للاتصال بخادم وكيل KSN هو 15111.

• 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 يدوياً.

• استخدام نقطة التوزيع لفرض الاتصال بخادم الإدارة

حدد هذا الخيار إذا كنت قد حددت خيار استخدام 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 متاحاً. لا تتوفر الإعدادات الموجودة في القسم ملفات تعريف الاتصال إلا على الأجهزة التي تعمل بنظام التشغيل Windows وmacOS:

• 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 افتراضياً.

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 افتراضياً.

• **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 وتعيين جدول استقصاء كامل.

إذا تم تعطيل هذا الخيار، فلن يجري خادم الإدارة استقصاء الشبكة.

يمكن تكوين الفاصل الزمني لاكتشاف الجهاز لإصدارات عميل الشبكة السابقة لـ 10.2 في الحقول معدل الاستقصاءات من مجالات Windows (دقيقة) ومعدل استقصاءات الشبكة (بالدقائق). تتوفر الحقول إذا تم تمكين الخيار.

يتم تعطيل هذا الخيار افتراضيًا.

• [تمكين استقصاء نطاق IP](#) ⑤

إذا تم تمكين الخيار، فإن خادم الإدارة يجري استقصاء نطاقات IP تلقائيًا وفقًا للجدول المُكوّن عن طريق النقر فوق الرابط تعيين جدول الاستقصاء.

إذا تم تعطيل هذا الخيار، فلن يجري خادم الإدارة 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 استخدام استقصاء شبكة لا تتطلب تكوينًا \(على النظام الأساسي Linux فقط\): نطاقات IP المحددة يدويًا](#) ⑤

إذا تم تمكين هذا الخيار، فستقوم نقطة التوزيع تلقائيًا باستقصاء الشبكة باستخدام أجهزة IPv6 عن طريق [شيكات 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](#) ⑤

إذا تم تمكين الخيار، فإن خادم الإدارة يجري 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.

في القسم الفرعي إعدادات اتصال الإنترنت، يمكنك تحديد إعدادات الوصول إلى الإنترنت:

• [استخدام الخادم الوكيل](#) ⑤

في حالة تحديد خانة الاختيار هذه، يمكنك تكوين اتصال الخادم الوكيل في حقول الإدخال.

تكون خانة الاختيار غير محددة بشكل افتراضي.

• [عنوان الخادم الوكيل](#) ⑤

عنوان الخادم الوكيل.

• رقم المنفذ ④

رقم المنفذ المستخدم في الاتصال.

• تجاوز الخادم الوكيل للعناوين المحلية ④

إذا تم تمكين هذا الخيار، فلن يتم استخدام خادم الوكيل للاتصال بالأجهزة على الشبكة المحلية. يتم تعطيل هذا الخيار افتراضياً.

• مصادقة الخادم الوكيل ④

إذا تم تحديد خانة الاختيار تلك، فيمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال. يتم تعطيل خانة الاختيار هذه بشكل افتراضي.

• اسم المستخدم ④

حساب المستخدم الذي من خلاله تم إنشاء اتصال بخادم الوكيل.

• كلمة المرور ④

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 من جانب نقطة التوزيع ④

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. يوجد بيان KSN افتراضياً في `ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula%`. يتم تعطيل هذا الخيار افتراضياً. يسري تمكين هذا الخيار فقط في حالة **تمكين** الخيارين استخدام خادم الإدارة كخادم وكيل وأوافق على استخدام Kaspersky Security Network في نافذة خصائص خادم الإدارة. يمكنك تعيين عقدة مجموعة نشط-خامل إلى نقطة توزيع، وتمكين وكيل KSN على هذه العقدة.

• توجيه طلبات KSN إلى خادم الإدارة ④

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المُدارة إلى خادم الإدارة. يتم تمكين هذا الخيار افتراضياً.

• الوصول إلى KSN Cloud / شبكة KSN الخاصة مباشرة عبر الإنترنت ④

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المُدارة إلى KSN Cloud أو شبكة KSN الخاصة. يتم أيضًا إرسال طلبات KSN – التي تم إنشاؤها على نقطة التوزيع نفسها – مباشرةً إلى KSN Cloud أو Private KSN.

لا يمكن لنقاط التوزيع التي لديها الإصدار 11 المثبت لعملاء الشبكة (أو الأقدم)، الوصول إلى شبكة KSN الخاصة مباشرة. إذا كنت ترغب في إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KSN الخاصة، 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 شبكة KSN الخاصة مباشرةً.

• **منفذ TCP**

رقم منفذ TCP الذي ستستخدمه الأجهزة المُدارة للاتصال بخادم وكيل KSN. رقم المنفذ الافتراضي هو 13111.

• **استخدام منفذ UDP**

إذا احتجت أن تكون الأجهزة المُدارة متصلة بخادم وكيل KSN عبر منفذ UDP، فقم بتمكين خيار **استخدام منفذ UDP** وحدد رقم منفذ UDP. يتم تمكين هذا الخيار افتراضيًا. والمنفذ الافتراضي لـ UDP للاتصال بخادم وكيل KSN هو 15111.

في القسم الفرعي **تحديثات**، يمكنك تحديد ما إذا كان يجب على عميل الشبكة **تنزيل ملفات مختلفة** من خلال تمكين خيار **تنزيل ملفات تفضيلية** 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.

مقارنة الميزات من خلال أنظمة تشغيل عميل الشبكة

يوضح الجدول أدناه إعدادات سياسة عميل الشبكة التي يمكنك استخدامها لتكوين وكيل الشبكة مع نظام تشغيل محدد.

إعدادات نهج عميل الشبكة: المقارنة حسب أنظمة التشغيل

قسم السياسة	Windows	Mac	Linux
عام	✓	✓	✓
تكوين الحدث	✓	✓	✓
إعدادات	✓	✓	✓
المستودعات	✓	—	✓
تحديثات البرنامج والثغرات الأمنية	✓	—	—
إدارة إعادة التشغيل	✓	—	—
مشاركة سطح المكتب لـ Windows	✓	—	—
إدارة التصحيحات والتحديثات	✓	—	—
الاتصال ← الشبكة	✓	✓	✓

فيما عدا خيار فتح منافذ عميل الشبكة في جدار حماية Microsoft Windows .			
الاتصال ← ملفات تعريف الاتصال	✓	✓	—
الاتصال ← جدول الاتصال	✓	✓	✓
نقاط التوزيع ← استقصاء الشبكة	✓	—	يتوفر فقط قسم استقصاء نطاق IP.
نقاط التوزيع ← إعدادات الاتصال بالإنترنت	✓	✓	✓
نقاط التوزيع ← وكيل KSN	—	—	✓
نقاط التوزيع ← تحديثات	—	—	✓
سجل المراجعة	✓	✓	✓

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 نوعين من الحسابات:

- حسابات موظفي المؤسسة. يقوم خادم الإدارة باسترداد بيانات حسابات هؤلاء المستخدمين 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.

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 المستخدمين 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.

يمكن عرض جميع حسابات المستخدمين في المجلد **حسابات المستخدمين** في شجرة وحدة التحكم. مجلد **حسابات المستخدمين** هو مجلد فرعي من مجلد **خيارات متقدمة** بشكل افتراضي.

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 و SMS**
- 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 المستخدم) 

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 تتضمن كلمة المرور من 8 إلى 16 حرفاً.
- 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. افتراضياً، 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 مقدماً 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 تفويضاً 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 حديثاً 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** للاتصال المستخدم بـ Kaspersky Security Center

يجب أن تتوافق كلمة المرور مع القواعد التالية:

- يجب أن تتضمن كلمة المرور من 8 إلى 16 حرفاً.
- 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. افتراضياً، 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، بعد استقالة الموظف من الشركة وتركها.

• 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 تفويضاً للمستخدم مع حق **تعديل قوائم التحكم في الوصول للكائن** للمجال الوظيفي **الميزات العامة: أدوات 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.

افتراضياً، 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: محلياً، باستخدام الأمر regedit من القائمة **بدء** ← **تشغيل**).

2. انتقل إلى المفتاح التالي:

• لنظام 64 بت:

Y_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

• لنظام 32 بت:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

3. إذا لم تكن قيمة SrvSpiPpcLogonAttempts موجودة، فقم بإنشائها. نوع القيمة هو DWORD.

افتراضياً، لا يتم إنشاء هذه القيمة بعد تثبيت Kaspersky Security Center.

4. حدد العدد المطلوب من المحاولات في القيمة SrvSpiPpcLogonAttempts.

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 تمييز اسم أحد المستخدمين الداخليين

يمكنك تكوين التحقق من تمييز اسم أحد مستخدمي Kaspersky Security Center الداخليين عند إضافة هذا الاسم إلى التطبيق. يمكن تنفيذ التحقق من تمييز 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 تمييز اسم أحد المستخدمين الداخليين على جميع خوادم الإدارة الافتراضية وعلى خادم الإدارة الرئيسي.

لتمكين التحقق من تمييز 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:

• لنظام 64 بت:

LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\core\independent\KLLIM

• لنظام 32 بت:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM

3. للمفتاح (DWORD LP_InterUserUniqVsScope)، قم بتعيين القيمة 00000001.

0 هي القيمة الافتراضية المحددة لهذا المفتاح.

4. قم بإعادة تشغيل خدمة خادم الإدارة.

سيتم التحقق فقط من تمييز 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:

• لنظام 64 بت:

LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\core\independent\KLLIM

• لنظام 32 بت:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\core\independent\KLLIM

3. للمفتاح (DWORD LP_InterUserUniqVsScope)، قم بتعيين القيمة 00000001.

0 هي القيمة الافتراضية المحددة لهذا المفتاح.

4. قم بإعادة تشغيل خدمة خادم الإدارة.

سيتم تنفيذ عملية التحقق من تمييز الاسم على جميع خوادم الإدارة الافتراضية وعلى خادم الإدارة الرئيسي.

إضافة مجموعة أمان

يمكنك إضافة مجموعات أمان (مجموعات مستخدمين)، وإجراء تكوين مرّن 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 المستخدمون.

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 تضمينه 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 مسبقاً من الحقوق وتعيين هذه الأدوار للمستخدمين اعتماداً على مدى نطاق واجباتهم.

دور المستخدم (يُشار إليه أيضاً بالدور) هو مجموعة محددة مسبقاً 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 وفقاً للمهام القياسية ونطاق واجبات المستخدمين.

يمكن تعيين أسماء لأدوار المستخدمين وفقاً لأغراض كل منها. يمكنك إنشاء عدد غير محدود من الأدوار في التطبيق.

يمكنك استخدام [أدوار المستخدم المحددة مسبقاً](#) مع مجموعة الحقوق المكونة بالفعل، أو [إنشاء أدوار جديدة](#) لتكوين 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 [القراءة والتعديل والتنفيذ](#) على أي مهمة أو تقرير أو إعداد. بالإضافة إلى هذه الحقوق، يجب أن يكون لدى المستخدم حق [تنفيذ العمليات على تحديدات الجهاز](#) لإدارة المهام أو التقارير أو الإعدادات في تحديدات الجهاز.

تنتمي جميع المهام والتقارير والإعدادات وحزم التنصيب المفقودة في الجدول إلى الميزات العامة: [المجال الوظيفي للوظيفة الأساسية](#).

حقوق الوصول إلى ميزات التطبيق

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
الميزات العامة: إدارة المجموعات الإدارية	تعديل	<ul style="list-style-type: none">• إضافة جهاز إلى مجموعة الإدارة: قم بالتعديل• حذف الجهاز من مجموعة الإدارة: قم بالتعديل• أضف مجموعة إدارة إلى مجموعة إدارة أخرى: قم بالتعديل• حذف مجموعة إدارة من مجموعة إدارة أخرى: قم بالتعديل	لا شيء	لا شيء	لا شيء
الميزات العامة: الوصول إلى الكائنات بغض النظر عن قوائم التحكم في	قراءة	الوصول على وصول القراءة لجميع الكائنات: اقرأ	لا شيء	لا شيء	لا شيء

					الوصول (ACLs) الخاصة بهم
لا شيء	<ul style="list-style-type: none"> • "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" 	<ul style="list-style-type: none"> • "تنزيل التحديثات إلى مستودع خادم الإدارة" • "تسليم التقارير" • "توزيع حزم التثبيت" • "تثبيت التطبيق عن بُعد على خوادم الإدارة الثانوية" 	<ul style="list-style-type: none"> • قواعد نقل الجهاز (إنشاء أو تعديل أو حذف) للخادم الافتراضي: قم بالتعديل، وتنفيذ العمليات على تحديدات الجهاز • احصل على شهادة مخصصة لبروتوكول (Mobile (LWNGT: اقرأ • تعيين شهادة بروتوكول (Mobile (LWNGT المخصصة: اكتب • احصل على قائمة الشبكة المعرفة من قبل NLA: اقرأ • إضافة أو تعديل أو حذف قائمة الشبكة المعرفة من قبل NLA: قم بالتعديل • اعرض قائمة مجموعات التحكم في الوصول: اقرأ • اعرض سجل أحداث Kaspersky: اقرأ 	<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديدات الجهاز 	الميزات العامة: الوظائف الأساسية

<ul style="list-style-type: none"> • "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" 	<p>لا شيء</p>	<p>لا شيء</p>	<ul style="list-style-type: none"> • عرض الكائنات المحذوفة في سلة المحذوفات: اقرأ • حذف كائنات من سلة المحذوفات: قم بالتعديل 	<ul style="list-style-type: none"> • قراءة • تعديل 	<p>الميزات العامة: الكائنات المحذوفة</p>
<p>الإعدادات:</p>	<p>لا شيء</p>	<p>لا شيء</p>	<ul style="list-style-type: none"> • تغيير إعدادات تسجيل الأحداث: قم بتحرير 	<ul style="list-style-type: none"> • حذف الأحداث 	<p>الميزات العامة: معالجة الحدث</p>

<ul style="list-style-type: none"> • 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 المخزنة في قاعدة البيانات • فترة زمنية لتخزين الأحداث من الأجهزة المحذوفة 			<p>إعدادات تسجيل الدخول إلى الأحداث</p> <ul style="list-style-type: none"> • تغيير إعدادات إشعار الأحداث: قم بتحرير إعدادات إشعار الحدث • حذف الأحداث: احذف الأحداث 	<ul style="list-style-type: none"> • تحرير إعدادات إشعار الحدث • تحرير إعدادات تسجيل الدخول إلى الأحداث • تعديل 	
لا شيء	لا شيء	<ul style="list-style-type: none"> • "النسخ الاحتياطي لبيانات خادم الإدارة" • "صيانة قاعدة البيانات" 	<ul style="list-style-type: none"> • حدد منافذ خادم الإدارة لاتصال عميل الشبكة: قم بالتعديل • حدد منافذ وكيل التنشيط الذي تم تشغيله على خادم الإدارة: قم بالتعديل • حدد منافذ وكيل التنشيط للجوال التي تم تشغيلها على خادم الإدارة: قم بالتعديل • حدد منافذ خادم الويب لتوزيع الحزم المستقلة: قم بالتعديل • حدد منافذ خادم الويب لتوزيع ملفات تعريف MDM: قم بالتعديل • حدد منافذ SSL لخادم الإدارة للاتصال عبر Kaspersky Security Center :Web Console تعديل • حدد منافذ خادم الإدارة للاتصال الهاتف المحمول: قم بالتعديل 	<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • تعديل كائن ACL • إجراء عمليات على تحدييدات الجهاز 	الميزات العامة: العمليات على خادم الإدارة

			<ul style="list-style-type: none"> • قم بتغيير الحد الأقصى لعدد الأحداث المخزنة في قاعدة بيانات خادم الإدارة: قم بالتعديل • حدد الحد الأقصى لعدد الأحداث التي يمكن أن يرسلها خادم الإدارة: قم بالتعديل • حدد الفترة الزمنية التي يمكن خلالها إرسال الأحداث بواسطة خادم الإدارة: قم بالتعديل 		
<p>حزمة التثبيت: "Kaspersky"</p>	<ul style="list-style-type: none"> • "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" 	لا شيء	<p>اقبل تثبيت التصحيح أو ارفضه: إدارة تصحيحات Kaspersky</p>	<ul style="list-style-type: none"> • إدارة تصحيحات Kaspersky • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديدات الجهاز 	<p>الميزات العامة: نشر برامج Kaspersky</p>
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • تصدير ملف مفتاح: تصدير ملف مفتاح • تعديل إعدادات مفتاح ترخيص خادم الإدارة: قم بالتعديل 	<ul style="list-style-type: none"> • تصدير إلى ملف • تعديل 	<p>الميزات العامة: إدارة المفاتيح</p>
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • إنشاء التقارير بغض النظر عن قوائم ACL الخاصة بهم: اكتب • تنفيذ التقارير بغض النظر عن قوائم ACL الخاصة بهم: اقرأ 	<ul style="list-style-type: none"> • قراءة • تعديل 	<p>الميزات العامة: إدارة التقارير الإجبارية</p>

لا شيء	لا شيء	لا شيء	تسجيل خوادم الإدارة الثانوية أو تحديثها أو حذفها: تكوين التسلسل الهرمي لخوادم الإدارة	تهيئة التسلسل الهرمي لخوادم الإدارة	الميزات العامة: التسلسل الهرمي لخوادم الإدارة
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • تغيير خصائص "الأمان" لأي كائن: تغيير قوائم التحكم في الوصول للكائن • إدارة أدوار المستخدم: تغيير قوائم التحكم في الوصول للكائن • إدارة المستخدمين الداخليين: تغيير قوائم التحكم في الوصول للكائن • إدارة مجموعات الأمان: تغيير قوائم التحكم في الوصول للكائن • إدارة الأسماء المستعارة: تغيير قوائم التحكم في الوصول للكائن 	تعديل كائن ACL	الميزات العامة: أذونات المستخدم
لا شيء	"تقرير حول نتائج تثبيت تحديثات برامج الجهات الخارجية"	لا شيء	<ul style="list-style-type: none"> • الحصول على قائمة خوادم الإدارة الافتراضية: اقرأ • الحصول على معلومات حول خادم الإدارة الافتراضي: اقرأ • إنشاء خادم إدارة افتراضي أو تحديثه أو حذفه: إدارة خوادم الإدارة الافتراضية • نقل خادم الإدارة الافتراضي إلى مجموعة أخرى: إدارة خوادم الإدارة الافتراضية • تعيين أذونات خادم الإدارة الافتراضي: إدارة خوادم الإدارة الافتراضية 	<ul style="list-style-type: none"> • إدارة خوادم الإدارة الافتراضية • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديثات الجهاز 	الميزات العامة: خوادم الإدارة الافتراضية
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • الحصول على بيانات استعادة خدمة إدارة المفاتيح: اقرأ • حذف شهادات المستخدم: إدارة الشهادات 	<ul style="list-style-type: none"> • توصيل أجهزة جديدة • إرسال أوامر المعلومات فقط 	إدارة جهاز المحمول: عام

			<ul style="list-style-type: none"> الحصول على الجزء العام لشهادة المستخدم: اقرأ تحقق مما إذا تم تمكين البنية الأساسية للمفتاح العام: اقرأ تحقق من حساب البنية التحتية للمفتاح العام: اقرأ احصل على قوالب البنية التحتية للمفتاح العام: اقرأ احصل على قوالب البنية التحتية للمفتاح العام عن طريق شهادة استخدام المفتاح الموسع: اقرأ تحقق مما إذا تم إبطال شهادة البنية التحتية للمفتاح العام: اقرأ تحديث إعدادات إصدار شهادة المستخدم: إدارة الشهادات الحصول على إعدادات إصدار شهادة المستخدم: اقرأ احصل على الحزم حسب اسم المنتج والإصدار: اقرأ تعيين أو إلغاء شهادة المستخدم: إدارة الشهادات تجديد شهادة المستخدم: إدارة الشهادات تعيين علامة شهادة المستخدم: إدارة الشهادات تشغيل إنشاء حزمة تثبيت MDM؛ إلغاء إنشاء حزمة تثبيت MDM: قم بتوصيل أجهزة جديدة 	<ul style="list-style-type: none"> إلى الأجهزة المحمولة إرسال أوامر إلى الأجهزة المحمولة. إدارة الشهادات قراءة تعديل 	
لا شيء	"تقرير حول مستخدمي الأجهزة"	لا شيء	<ul style="list-style-type: none"> إنشاء جلسة مشاركة سطح المكتب: الحق في إنشاء جلسة مشاركة سطح المكتب 	<ul style="list-style-type: none"> بدء جلسات RDP الاتصال بجلسات RDP 	إدارة النظام: الاتصال

			<ul style="list-style-type: none"> • إنشاء جلسة RDP: الاتصال بجلسات RDP الموجودة • إنشاء نفق: بدء إنشاء نفق • حفظ قائمة شبكة المحتوى: احفظ الملفات من الأجهزة إلى محطة عمل المسؤول 	<ul style="list-style-type: none"> • حفظ الملفات من الأجهزة إلى محطة عمل المسؤول • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديثات الجهاز 	
لا شيء	<ul style="list-style-type: none"> • "تقرير حول سجل الأجهزة" • "تقرير حول تغييرات التكوين" • "تقرير حول الأجهزة" 	لا شيء	<ul style="list-style-type: none"> • الحصول على كائن مخزون الأجهزة أو تصديره: اقرأ • إضافة جرد الأجهزة أو تعيينه أو حذفه: اكتب 	<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديثات الجهاز 	إدارة النظام: جرد الأجهزة
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • عرض إعدادات CISCO: اقرأ • تغيير إعدادات CISCO: اكتب 	<ul style="list-style-type: none"> • قراءة • تعديل 	إدارة النظام: التحكم في الوصول إلى الشبكة
حزمة التثبيت: "صورة نظام التشغيل"	لا شيء	"إنشاء حزمة التثبيت على مرجع صورة نظام التشغيل للجهاز"	<ul style="list-style-type: none"> • نشر خادم PXE: انشر خادم PXE • عرض قائمة بخوادم PXE: اقرأ • بدأ عملية التثبيت على عملاء PXE أو أوقفها: قم بالتنفيذ • إدارة برامج التشغيل لـ WinPE وصور نظام التشغيل: قم بالتنفيذ 	<ul style="list-style-type: none"> • نشر خادم PXE • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديثات الجهاز 	إدارة النظام: نشر نظام التشغيل
لا شيء	"تقرير تحديثات البرامج"	<ul style="list-style-type: none"> • "مزامنة Windows Update" 	<ul style="list-style-type: none"> • عرض خصائص تصحيح الطرف الثالث: اقرأ 	<ul style="list-style-type: none"> • قراءة • تعديل 	إدارة النظام: إدارة الثغرات الأمنية والتصحيحات

		<ul style="list-style-type: none"> • تثبيت تحديثات Windows "Update" • "إصلاح الثغرات الأمنية" • "قم بتثبيت التحديثات المطلوبة وضبط إعدادات مهمة إصلاح الثغرات الأمنية" 	<ul style="list-style-type: none"> • تغيير خصائص تصحيح الطرف الثالث: قم بالتعديل 	<ul style="list-style-type: none"> • تنفيذ إجراءات عمليات على تحديثات الجهاز 	
<p>حزم التثبيت:</p> <ul style="list-style-type: none"> • "تطبيق مخصص" • "حزمة VAPM" 	لا شيء	لا شيء	<ul style="list-style-type: none"> • عرض خصائص حزمة التثبيت المستندة إلى إدارة الثغرات الأمنية والتصحيحات من جهة خارجية: اقرأ • تغيير خصائص حزمة التثبيت المستندة إلى إدارة الثغرات الأمنية والتصحيحات من جهة خارجية: تعديل 	<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • إجراءات عمليات على تحديثات الجهاز 	إدارة النظام: التثبيت عن بُعد
لا شيء	<ul style="list-style-type: none"> • "تقرير حول التطبيقات المثبتة" • "تاريخ تقرير سجل التطبيقات" • "تقرير حول حالة مجموعات التطبيقات المرخصة" • "تقرير حول مفاتيح ترخيص برامج الجهات الخارجية" 	لا شيء	لا شيء	<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • إجراءات عمليات على تحديثات الجهاز 	إدارة النظام: جرد البرامج

أدوار المستخدم المحددة مسبقاً

توفر أدوار المستخدم المعينة لمستخدمي Kaspersky Security Center مجموعات من [حقوق الوصول إلى ميزات التطبيق](#).

يمكنك استخدام أدوار المستخدم المحددة مسبقاً مع مجموعة الحقوق المكونة بالفعل، أو إنشاء أدوار جديدة وتكوين الحقوق المطلوبة بنفسك. يمكن ربط بعض أدوار المستخدم المحددة مسبقاً والمتوفرة في Kaspersky Security Center بملصقات وظائف محددة، على سبيل المثال، المدقق، مسؤول الأمن، المشرف (هذه الأدوار موجودة في Kaspersky Security Center بدءاً من الإصدار 11). تم تكوين حقوق الوصول لهذه الأدوار مسبقاً وفقاً للمهام القياسية ونطاق واجبات الوظائف المرتبطة. يوضح الجدول أدناه كيف يمكن ربط الأدوار يمكن ربط الأدوار بملصقات وظائف محددة.

أمثلة على أدوار المناصب الوظيفية المحددة

الدور	التعليق
مدقق الحسابات	يسمح بتنفيذ جميع العمليات مع جميع أنواع التقارير، وجميع عمليات العرض بما يشمل عرض الكائنات المحذوفة (يمنح أذونات قراءة وتعديل في حقل الكائنات) المحذوفة. لا يسمح بتنفيذ عمليات أخرى. يمكنك تعيين هذا الدور لشخص يقوم بإجراء تدقيق لمؤسستك.
المشرف	يسمح بتنفيذ جميع عمليات العرض، لا يسمح بتنفيذ عمليات أخرى. يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمن 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 أمن تكنولوجيا المعلومات في مؤسستك.

يوضح الجدول أدناه حقوق الوصول المعينة لكل دور مستخدم محدد مسبقاً.

حقوق الوصول لأدوار المستخدم المحددة مسبقاً

الدور	الوصف
مسؤول خادم الإدارة	<p>يسمح بجميع العمليات في المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> الميزات العامة: الوظائف الأساسية معالجة الحدث التسلسل الهرمي لخوادم الإدارة خوادم الإدارة الافتراضية إدارة النظام: الاتصال مخزون الأجهزة مخزون البرنامج
مشغل خادم الإدارة	<p>يمنح حقوق القراءة والتنفيذ في جميع المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> الميزات العامة: الوظائف الأساسية خوادم الإدارة الافتراضية إدارة النظام: الاتصال مخزون الأجهزة مخزون البرنامج

	<p>للسماح بجميع العمليات في المجالات الوظيفية ، في الميزات العامة :</p> <ul style="list-style-type: none"> • الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم • الكائنات المحذوفة • إدارة التقارير المفروضة <p>يمكنك تعيين هذا الدور لشخص يقوم بإجراء تدقيق لمؤسستك.</p>	مدقق الحسابات
	<p>يسمح بجميع العمليات في المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: • الوظائف الأساسية • نشر برنامج Kaspersky • إدارة مفتاح الترخيص • إدارة النظام: • نشر نظام التشغيل • إدارة الثغرات الأمنية والتصحيحات • التثبيت عن بُعد • مخزون البرنامج <p>منح حقوق القراءة والتنفيذ في الميزات العامة: المجالات الوظيفية لخوادم الإدارة الافتراضية.</p>	مسؤول التثبيت
	<p>يمنح حقوق القراءة والتنفيذ في جميع المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: • الوظائف الأساسية • نشر برنامج Kaspersky (يمنح أيضاً تصحيحات إدارة Kaspersky مباشرة في هذه المنطقة) • خوادم الإدارة الافتراضية • إدارة النظام: • نشر نظام التشغيل • إدارة الثغرات الأمنية والتصحيحات • التثبيت عن بُعد • مخزون البرنامج 	مشغل التثبيت
	<p>يسمح بجميع العمليات في المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: الوظائف الأساسية • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات 	مسؤول Kaspersky Endpoint Security

<p>يمنح حقوق القراءة والتنفيذ في جميع المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: الوظائف الأساسية • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات 	<p>مشغل Kaspersky Endpoint Security</p>
<p>يسمح بجميع العمليات في المجالات الوظيفية، باستثناء المجالات التالية، في الميزات العامة:</p> <ul style="list-style-type: none"> • الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم • إدارة التقارير المفروضة 	<p>المسؤول الرئيسي</p>
<p>يمنح حقوق القراءة والتنفيذ (إن أمكن) في جميع المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: • الوظائف الأساسية • الكائنات المحذوفة • العمليات على خادم الإدارة • نشر برنامج Kaspersky • خوادم الإدارة الافتراضية • إدارة جهاز المحمول: عام • إدارة النظام، بما في ذلك جميع الميزات • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات 	<p>المشغل الرئيسي</p>
<p>يسمح بجميع العمليات في المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: الوظائف الأساسية • إدارة جهاز المحمول: عام 	<p>إدارة جهاز المحمول</p>
<p>يمنح حقوق القراءة والتنفيذ في الميزات العامة: المجالات الوظيفية للوظائف الأساسية.</p> <p>يمنح قراءة وإرسال أوامر المعلومات فقط إلى الأجهزة المحمولة في المجال الوظيفي إدارة الجهاز المحمول: عام.</p>	<p>مشغل إدارة جهاز المحمول</p>
<p>يسمح بجميع العمليات في المجالات الوظيفية التالية، في الميزات العامة:</p> <ul style="list-style-type: none"> • الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم • إدارة التقارير المفروضة <p>يمنح قراءة وتعديل وتنفيذ وحفظ الملفات من الأجهزة على محطة عمل المسؤول وتنفيذ العمليات على حقوق تحديدات الأجهزة في نطاق إدارة النظام: المجالات الوظيفية للاتصال.</p> <p>يمكنك تعيين هذا الدور لموظف أمن مسؤول عن أمن تكنولوجيا المعلومات في مؤسستك.</p>	<p>مسؤول الأمن</p>
<p>يسمح بجميع العمليات في إدارة جهاز المحمول: المجالات الوظيفية لـ Self Service Portal. هذه الميزة غير مدعومة في Kaspersky Security Center 11 والإصدار الأحدث.</p>	<p>مستخدم Self Service Portal</p>
<p>يمنح حق القراءة في الميزات العامة: الوصول إلى الكائنات، بغض النظر عن قوائم التحكم في الوصول ACLs والميزات العامة: المجالات الوظيفية لإدارة التقارير المفروضة.</p> <p>يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمن تكنولوجيا المعلومات في مؤسستك.</p>	<p>المشرف</p>

يسمح بجميع العمليات في الميزات العامة: المجالات الوظيفية للوظائف الأساسية وإدارة النظام (بما في ذلك جميع الميزات).	مسؤول الثغرات الأمنية والتصحيحات
يمنح حقوق القراءة والتنفيذ (إن أمكن) في الميزات العامة: المجالات الوظيفية للوظائف الأساسية وإدارة النظام (بما في ذلك جميع الميزات).	مشغل إدارة الثغرات الأمنية والتصحيحات

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 خانة الاختيار **سماع** ورفض 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 المستخدمين](#) أو المستخدمين المحددين.

تعيين دور لمستخدم أو لمجموعة مستخدمين

لتعيين دور لمستخدم أو لمجموعة 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 إضافة 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 المستخدم.

7. انقر فوق **موافق**.

سيتم تعيين دور مع مجموعة من الحقوق للعمل مع خادم الإدارة لمستخدم أو مجموعة المستخدم. يتم عرض الأدوار التي تم تعيينها في علامة التبويب **الأدوار** في القسم **الأمن** من نافذة خصائص خادم الإدارة.

تعيين أدونات للمستخدمين والمجموعات

يمكنك منح المستخدمين والمجموعات أدونات 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 الأدونات 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 الأدونات 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 الأدونات.

b. حدد خانة الاختيار **سماح** ورفض الموجودة بجوار الأدونات 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 أدونات خادم الإدارة (أو مجموعة الإدارة) إلى المناطق التالية:

- الميزات العامة

- إدارة مجموعات الإدارة (فقط لـ Kaspersky Security Center 11 أو الإصدار الأحدث)
- الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACL) الخاصة بها (فقط لـ Kaspersky Security Center 11 أو الإصدار الأحدث)

- الوظائف الأساسية

- الكائنات المحذوفة (فقط لـ Kaspersky Security Center 11 أو الإصدار الأحدث)

- معالجة الحدث

- عمليات يتم إجراؤها لخادم الإدارة (فقط في نافذة خصائص خادم الإدارة)

- نشر تطبيقات Kaspersky

- إدارة مفتاح الترخيص

- إدارة التقرير المفروضة (فقط لـ Kaspersky Security Center 11 أو الإصدار الأحدث)

- التسلسل الهرمي للخوادم

- حقوق المستخدم

- خوادم الإدارة الافتراضية

- إدارة الأجهزة المحمولة

- عام

- إدارة النظام

- الاتصال

- مخزون الأجهزة

- التحكم في الوصول إلى الشبكة

- نشر نظام التشغيل

- إدارة الثغرات الأمنية والتصحیحات

- 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.

إن حقوق المستخدم هي مجموع ما يلي:

- حقوق المستخدم الخاصة به

- حقوق جميع الأدوار التي تم تعيينها لهذا المستخدم

- حقوق جميع عناصر مجموعة الأمن التي ينتمي إليها المستخدم

- حقوق جميع الأدوار التي تم تعيينها لمجموعات الأمن 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

بشكل 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 الخيار **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، حدد 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. افتراضياً، يتم ملء الحقل مالك الجهاز بقيمة Active Directory ويتم تحديثه مع كل استقصاء [Active Directory](#). يمكنك عرض قائمة بملاك الجهاز في تقرير حول مالكي الجهاز. يمكنك إنشاء تقرير باستخدام [معالج 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. املا الحقول ذات الصلة في نافذة نص رسالة SMS ثم انقر على زر 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 للمستخدم.
- شهادة البريد، والتي تُطلب لإعداد البريد الخاص بالشركة على جهاز محمول للمستخدم.
- شهادة VPN، والتي تُطلب لإعداد الشبكة الخاصة الظاهرية على جهاز محمول للمستخدم.

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 وتثبيت الشهادة للمستخدم. 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 القسم 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 14 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.

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، عليك تثبيت [Windows ADK](#) والوظيفة الإضافية [Windows PE لأدوات Windows ADK](#) على خادم الإدارة. نوصي بتثبيت أحدث إصدارات Windows ADK والوظيفة الإضافية لـ Windows PE لـ Windows ADK. يمكنك إنشاء صورة لأي إصدار من نظام تشغيل Windows يتوافق مع [متطلبات Kaspersky Security Center](#).

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، فحدد خانة الاختيار [إنشاء نسخة احتياطية لحالة الجهاز](#) في معالج إنشاء 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. يقوم خادم PXE بإنشاء اتصال مع جهاز عميل جديد أثناء تمهيده.

2. يصبح الجهاز العميل مضمناً في بيئة التثبيت المسبق لـ 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 أيضاً 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 يدوياً، 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.

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 ذات صورة نظام تشغيل.

4. اتبع إرشادات المعالج.

عند انتهاء المعالج، يتم إنشاء مهمة خادم إدارة تُسمى إنشاء حزمة تثبيت وفقاً لصورة نظام تشغيل الجهاز المرجعي. يمكنك عرض المهمة في المجلد المهام.

عند انتهاء مهمة إنشاء حزمة تثبيت وفقاً 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 سيناريو هان مدعومان لنشر صورة نظام التشغيل:

• النشر على جهاز "خالي" والذي لا يحتوي على أي نظام تشغيل مثبت

• النشر على جهاز به نظام تشغيل Windows قيد التشغيل

يقدم خادم الإدارة ضمنياً صورة خدمة من برامج تشغيل بيئة التثبيت المسبق من Windows (Windows PE) والتي تُستخدم دائماً لالتقاط صور لنظام التشغيل والقيام بنشر هذه الصور. يجب إضافة كل برامج التشغيل المطلوبة لعمل كل الأجهزة المستهدفة بشكل صحيح إلى WinPE. بشكل عام، يجب إضافة برامج تشغيل مجموعة الشرائح المطلوبة لعمل واجهة شبكة الإيثرنت بشكل صحيح.

يجب تحقيق المتطلبات التالية لتطبيق سيناريوهات نشر الصورة والتقاطها:

• يجب تثبيت مجموعة (Windows Automated Installation Kit (WAIK) الإصدار 2.0، أو الأحدث أو مجموعة Windows Assessment and Deployment Kit (WADK) على خادم الإدارة. إذا كان السيناريو يسمح بتثبيت صور لـ Windows XP أو التقاطها، فيجب تثبيت WAIC.

• يجب أن يتوفر خادم DHCP على الشبكة حيث يوجد الجهاز المستهدف.

• يجب أن يكون المجلد المشترك الخاص بخادم الإدارة مفتوحاً للقراءة من الشبكة حيث يوجد الجهاز المستهدف. في حالة وجود المجلد المشترك على خادم الإدارة، يتم طلب الوصول لحساب KIPxeUser (يتم إنشاء هذا الحساب تلقائياً أثناء تشغيل مثبت 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 ضمنياً تحديد بنية وحدة المعالجة المركزية للجهاز الهدف: x86 أو x86-64.

تكوين عنوان وكيل KSN

بشكل افتراضي، يتطابق اسم المجال الخاص بخادم الإدارة مع عنوان وكيل KSN. إذا قمت بتغيير اسم مجال خادم الإدارة، فيجب عليك تحديد عنوان وكيل KSN الصحيح لتجنب فقدان الاتصال بين الأجهزة المضيفة وKSN.

لتكوين عنوان 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 وكيل KSN الجديد في علامة التبويب عام.

4. انقر على زر تطبيق.

من الآن فصاعداً، يتم استخدام العنوان المحدد كعنوان وكيل KSN.

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 عمل مجلد نشر صور الجهاز، انقر على زر إجراءات إضافية وحدد تكوين مجموعة برنامج التشغيل لبيئة التثبيت المسبق لـ Windows rlm ((WinPE في القائمة المنسدلة.

سنفتح نافذة برامج تشغيل بيئة التثبيت المسبق من Windows.

3. في النافذة برامج تشغيل بيئة التثبيت المسبق من Windows، انقر فوق الزر إضافة.

سنفتح 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.

سنفتح 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 sysprep.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 القسم 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**.

2. انقر على زر إجراءات إضافية وحدد إدارة قائمة خوادم PXE على الشبكة في القائمة المنسدلة. افتح 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.

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 بتهيئة 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. 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 العملية المثبت عليها نظام تشغيل آخر بالفعل:

1. في شجرة وحدة التحكم، افتح المجلد التثبيت عن بُعد المجلد وانقر فوق الرابط نشر حزمة التثبيت على الأجهزة المُدارة (محطات العمل) لتشغيل معالج نشر الحماية.
 2. في نافذة المعالج تحديد حزمة التثبيت، حدد حزمة التثبيت ذات صورة نظام تشغيل.
 3. اتبع إرشادات المعالج.
- بعد إنهاء المعالج عملياته، يتم إنشاء مهمة التثبيت عن بُعد لتثبيت نظام التشغيل على الأجهزة العملية. 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 مخزنة في المجلد نفسه. وفي حالة تمكين هذا الخيار، يُضيف التطبيق محتويات المجلد بالكامل، بما في ذلك الملف التنفيذي المحدد إلى حزمة التثبيت.

• حدد معلومات 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 معلومات إضافية للتثبيت الصامت، فيرجى تحديدها في هذا الحقل. راجع وثائق البائع للاطلاع على التفاصيل. يمكنك أيضًا إدخال معلومات أخرى.

• تحويل الإعدادات إلى القيم الموصى بها للتطبيقات التي تم التعرف عليها من قبل Kaspersky Security Center 14

سيتم تثبيت التطبيق من خلال الإعدادات الموصى بها، إذا كانت المعلومات عن التطبيق المحدد مشتملة على قاعدة بيانات Kaspersky. إذا أدخلت المعلومات في الحقل سطر أوامر الملف التنفيذي، تتم إعادة كتابتها باستخدام الإعدادات الموصى بها. يتم تمكين هذا الخيار افتراضيًا.

قام محلو Kaspersky بإنشاء قاعدة بيانات Kaspersky وصيانتها. يحدد محلو 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 تُسمى **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 المجلد **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 المجلد **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 أجريت على الكائن، يتم إنشاء مراجعة. لكل مراجعة رقم.

تشتمل كائنات التطبيق التي تدعم إدارة المراجعة على:

- خوادم 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 أجريت 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 أتم إجراؤه على إعدادات الكائن
- تكون خانة وصف مراجعة الكائن فارغة بشكل افتراضي. لإضافة وصف إلى مراجعة، حدد المراجعة ذات الصلة وانقر فوق الزر **الوصف**. في النافذة **وصف مراجعة الكائن**، أدخل نصاً لوصف المراجعة.

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 أجريت 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 أتم 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

• مجلد المهام

• مجلد مجموعة إدارة

• مجلد حسابات المستخدمين

• مجلد 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 كائناً 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 **Ctrl** و **Shift**.

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 محددين.

• مقارنة بمهمة أخرى ⑤

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 نظرًا مزدوجًا، وانقر فوق أحد الأزرار التالية في نافذة خصائص المراجعة التي تفتح:

• مقارنة بالحالي ⑤

انقر فوق هذا الزر لمقارنة المراجعة المحددة بالمراجعة الحالية.

• مقارنة بالسابق ⑤

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 يشتمل على إعدادات مراجعة الكائن، انقر فوق الرمز تصغير (▲) 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 يمكن إلا للمستخدمين **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.

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 يشتمل على إعدادات مراجعة الكائن، انقر فوق الرمز تصغير (⏏) 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 القيمة **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 حول حذف الكائنات وعرض معلومات حول الكائنات بعد حذفها.

يمكنك حذف الكائنات، بما يشمل الكائنات التالية:

- السياسات
- المهام
- حزم التثبيت
- خوادم الإدارة الافتراضية
- المستخدمين
- مجموعات الأمان
- مجموعات الإدارة

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 يوماً). لا يمكنك تغيير مدة التخزين إلا في حالة حصولك على [إذن التعديل](#) في نطاق حقوق الكائنات المحذوفة.

حذف كائن

يمكنك حذف الكائنات كالسياسات والمهام وحزم التثبيت والمستخدمين الداخليين ومجموعات المستخدم الداخلي إذا كان لديك الإذن تعديل الموجود في فئة حقوق الوظائف الأساسية (انظر [تعيين أدونات للمستخدمين والمجموعات](#) للحصول على المزيد من المعلومات).

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 أدونات للمستخدمين والمجموعات](#) للحصول على المزيد من المعلومات).

لعرض قائمة الكائنات المحذوفة،

في شجرة وحدة التحكم، حدد **الكائنات المحذوفة** (بشكل 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** (بشكل 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 بتحديدده 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 الجهاز المحمول.

يقدم هذا القسم تعليمات لتمكين إدارة الجهاز المحمول وتعطيله وتكوينه. يوضح هذا القسم أيضًا كيفية إدارة الأجهزة المحمولة المتصلة بخادم الإدارة.

للحصول على تفاصيل حول Kaspersky Security للجوال، راجع تعليمات Kaspersky Security للجوال.

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 الجهاز 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 فيما بعد. 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 و iOS باستخدام Kaspersky Security Center. يمكنك العمل مع شهادات الأجهزة المحمولة إرسال الأوامر إلى الأجهزة المحمولة.

حول سياسة المجموعة لإدارة أجهزة iOS MDM و EAS

لإدارة أجهزة iOS MDM و EAS، يمكنك استخدام مكون لإدارة إضافي 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 و EAS دون استخدام أداة تكوين iPhone® المساعدة وملف تعريف إدارة Exchange ActiveSync.

توفر سياسة مجموعة لإدارة أجهزة iOS MDM و EAS الخيارات التالية للمسؤول:

• إدارة أجهزة EAS:

- تكوين كلمة المرور لإلغاء قفل الجهاز.
 - تكوين تخزين البيانات على الجهاز بشكل مشفر.
 - تكوين مزامنة بريد الشركة.
 - تكوين ميزات الأجهزة للأجهزة المحمولة، مثل استخدام محركات الأقراص القابلة للإزالة أو استخدام الكاميرا أو Bluetooth.
 - تكوين قيود على استخدام التطبيقات المحمولة على الجهاز.
- ## • إدارة أجهزة iOS MDM:
- 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 سابقاً، مثل YouTube™ و iTunes® Store و Safari.
 - تكوين قيود على محتوى الوسائط (مثل الأفلام والعروض التلفزيونية) 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 و CardDAV 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 تلقائياً بواسطة الجهاز من هيئة إصدار الشهادات.
 - إضافة إعدادات مخصصة للعمل باستخدام التطبيقات المحمولة.

تحظى السياسة الخاصة بإدارة أجهزة iOS MDM و EAS بأهمية خاصة حيث قد تم تعيينها لمجموعة إدارة تتضمن خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM وخادم الأجهزة المحمولة Exchange ActiveSync (المشار إليهم بشكل جماعي بـ "خوادم الأجهزة المحمولة"). يتم تطبيق جميع الإعدادات المحددة في هذه السياسة أولاً 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.

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 الجهاز المحمول متوفرًا فقط على خادم الإدارة الرئيسي.

لتمكين إدارة الجهاز المحمول:

1. في شجرة وحدة التحكم، حدد المجلد [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 التطبيق](#) حدد [طريقة تفعيل التطبيق](#)، [قم بتفعيل التطبيق باستخدام ملف مفتاح أو رمز التنشيط](#). لن تكون إدارة الأجهزة المحمولة ممكنة ما لم تقوم بتفعيل ميزة إدارة الجهاز 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 التنشيط](#)، حدد أحد الخيارات التالية:

- [التحقق من تحديث المكونات الإضافية وحزم التنشيط](#) 

بدء تشغيل التحقق من حالة التحديث. إذا اكتشفت عملية التحقق إصدارات قديمة لبعض المكونات الإضافية أو حزم التنشيط، فسيطالبك المعالج بتنزيل الإصدارات لاستبدال الإصدارات القديمة بالحدثة.

- [تخطي التحقق](#) 

العمل المستمر بدون التحقق من تحديث المكونات الإضافية وحزم التنشيط. يمكنك تحديد هذا الاختيار، إذا لم يتوفر لديك، على سبيل المثال، ليس 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 المكونات الإضافية المتوفرة](#)، قم بتنزيل آخر إصدارات المكونات الإضافية وتنشيتها باللغة التي يطلبها إصدار تطبيقك. لا يتطلب تحديث المكونات الإضافية وجود رخصة.

بعد تثبيت المكونات الإضافية وحزم التنشيط، يتحقق التطبيق من تثبيت جميع المكونات الإضافية المطلوبة لتشغيل الأجهزة المحمولة بشكل صحيح. في حالة اكتشاف إصدارات قديمة لبعض المكونات الإضافية، سيطلبك المعالج بتنزيل الإصدارات الحديثة واستبدالها بالقديمة.

8. في الصفحة [إعدادات اتصال جهاز 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 الجهاز المحمول

لتمكين دعم الأجهزة المحمولة:

1. في شجرة وحدة التحكم، حدد المجلد 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](#)

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 افتراضياً.

• [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 الجهاز المحمول

يكون تعطيل إدارة الجهاز المحمول متوفرًا فقط على خادم الإدارة الرئيسي.

1. في شجرة وحدة التحكم، حدد المجلد إدارة الجهاز المحمول.

2. في مساحة عمل هذا المجلد، انقر فوق الرابط تكوين مكونات إضافية.
سيتم عرض صفحة مكونات إضافية الخاصة بمعالج البدء السريع لخدمات الإدارة.

3. حدد عدم تمكين إدارة جهاز المحمول إذا لم تعد ترغب في إدارة الأجهزة المحمولة بعد الآن.

4. انقر على موافق.

سيتمتع 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 الجهاز المحمول على الأجهزة المحمولة المُدارة، قد يتعين عليك إعادة تثبيت التطبيقات المحمولة المطلوبة لإدارة الجهاز المحمول.

العمل مع الأوامر للأجهزة المحمولة

يحتوي هذا القسم على معلومات حول الأوامر لإدارة الأجهزة المحمولة المدعومة من قبل التطبيق. 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 الجهاز المحمول.

تستخدم هذه الأوامر لإدارة الجهاز 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
- أجهزة EAS

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 أيضاً 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 الموظفين الذين يعملون لديك. عند استخدام Kaspersky Security Center Service Pack 2 Maintenance Release 1 أو الإصدارات الأقدم، يتم قفل الجهاز المحمول الذي يتلقى الأمر تحديد الموقع. بداية من Kaspersky Security Center 10 Service Pack 3، لم يتم قفل الجهاز.

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 سابقاً.
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.
تنصيب ملف التعريف	تم تثبيت ملف تعريف التكوين على الجهاز المحمول.
إزالة ملف التعريف	تم حذف ملف تعريف التكوين من الجهاز المحمول.
تنصيب ملف تعريف التزويد	تم تثبيت ملف تعريف التزويد على الجهاز المحمول.
إزالة ملف تعريف التزويد	تم حذف ملف تعريف التزويد من الجهاز المحمول.
تنصيب 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

الأوامر	نتائج تنفيذ الأمر
قفل	تم قفل الجهاز المحمول.
فتح	تم تعطيل قفل الجهاز المحمول باستخدام PIN. تم إعادة تعيين PIN المحدد سابقاً.
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	تم تحديد موقع الجهاز وإظهاره على Google Maps™. يتحمل حامل الجهاز المحمول تكلفة إرسال رسائل SMS وتوفير

الاتصال بالإنترنت.	الجهاز
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.	لقطة للوجه
يصدر الجهاز المحمول صوت إنذار.	إنذار

الجدول التالي يعرض الأوامر بأجهزة EAS.

الأوامر المدعومة لإدارة الأجهزة المحمولة: أجهزة EAS

الأوامر	نتائج تنفيذ الأمر
إعادة التعيين إلى إعدادات المصنع	تم حذف جميع البيانات من الجهاز المحمول، وتم استرجاع الإعدادات إلى القيم الافتراضية الخاصة بها.

استخدام مرسله Google 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 إرسال الإخطارات بين أجهزة KES وخادم الإدارة من خلال Google Firebase Cloud Messaging. في وحدة تحكم إدارة Kaspersky Security Center، يمكنك تحديد إعدادات Google Firebase Cloud Messaging لتوصيل أجهزة KES بالخدمة.

لاستعادة إعدادات مرسله Google Firebase Cloud، يجب أن تمتلك حساب Google.

لتكوين مرسله Google Firebase Cloud:

1. في المجلد إدارة الجهاز المحمول في شجرة التحكم، حدد المجلد الفرعي الأجهزة المحمولة.

2. من قائمة سياق المجلد الأجهزة المحمولة، حدد خصائص.

يؤدي هذا إلى فتح نافذة خصائص المجلد الأجهزة المحمولة.

3. حدد القسم إعدادات Google Firebase Cloud Messaging.

4. في الحقل معرف المرسل، حدد عدد مشروعات Google API التي استلمتها عند إنشاء مشروع في Google Developer Console.

5. في الحقل مفتاح الخادم، أدخل مفتاح خادم شائع قمت بإنشائه في Google Developer Console.

في المزامنة التالية مع خادم الإدارة، ستتصل أجهزة KES التي تمت إدارتها بواسطة أنظمة التشغيل Android بمرسله Google Firebase Cloud.

يمكنك تحرير إعدادات Google Firebase Cloud Messaging من خلال النقر فوق الزر إعادة تعيين الإعدادات.

إرسال أوامر

لإرسال أمر لجهاز محمول المستخدم:

1. في المجلد إدارة الجهاز المحمول في شجرة 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 الجهاز 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 الأوامر التي تم إرسالها إلى الجهاز المحمول، مع الحالات التنفيذية لكل منها. انقر فوق تحديث لتحديث قائمة الأوامر.

5. انقر فوق موافق لإغلاق النافذة وأمر إدارة الجهاز 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 بعد 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؛

يحفظ التطبيق بسجل أمر لكل جهاز محمول.

لعرض سجل الأوامر التي تم إرسالها إلى جهاز محمول:

1. في المجلد إدارة الجهاز المحمول في شجرة 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 الجهاز المحمول. تتوافق الأقسام الخاصة بنافذة أوامر إدارة الجهاز 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 التصنيف إظهار الأوامر عرض الأوامر بالحالة المحددة فقط في القائمة.

جار العمل بشهادات الأجهزة المحمولة

يحتوي هذا القسم على معلومات حول كيفية العمل مع شهادات الأجهزة المحمولة. يحتوي القسم على تعليمات حول كيفية تثبيت الشهادات على الأجهزة المحمولة للمستخدم وكيفية تكوين قواعد إصدار الشهادة. يحتوي القسم أيضًا على تعليمات حول كيفية دمج التطبيق مع البنية الأساسية للمفاتيح العامة وكيفية تكوين دعم Kerberos.

بدء معالج تثبيت الشهادة.

يمكنك تثبيت أنواع الشهادات التالية على جهاز محمول للمستخدم:

- 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 للمستخدم:

1. في شجرة وحدة التحكم، قم بتوسيع المجلد إدارة الجهاز المحمول، وحدد المجلد الفرعي الشهادات.

2. في مساحة عمل المجلد الشهادات، انقر فوق الرابط 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

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 مضطراً لتثبيت شهادة على جهاز KES بدون استخدام مصادقة شهادة. في هذه الحالة، في المرحلة الأخيرة من المعالج، في النافذة **طريقة إخطار المستخدم**، يجب على المسؤول تحديد نوع مصادقة المستخدم عند كل اتصال له بخادم الإدارة.

الخطوة 3. تحديد مستخدم

في القائمة، حدد مستخدمين أو مجموعة مستخدمين أو مجموعة مستخدمي Active Directory التي تحتاج لتثبيت الشهادة لها.

في النافذة **تحديد المستخدم**، يمكنك البحث عن **المستخدمين الداخليين** [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 مسبقاً. 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 تحويل 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 المعين 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 نَقم بإخطار المستخدم بالشهادة الجديدة** [9](#)

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 تحويل 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 المثبت عليها Kaspersky Endpoint Security for Android) ④**

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) ④**

في هذه الحالة، يستخدم المستخدم كلمة مرور المجال أو كلمة مرور المستخدم الداخلي لـ Kaspersky Security Center لاستلام شهادة جديدة.

• **كلمة مرور لمرة واحدة ④**

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 ④**

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 ⑤

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 الزر تصدير في الخطوة الأخيرة لمعالج تثبيت الشهادة.

هذا الخيار غير متاح في حال قيامك بتحديد بيانات الاعتماد (المجال أو الاسم المستعار) في الخطوة وسيلة إخطار المستخدم لمعالج تثبيت الشهادة.

• إخطار المستخدم بالشهادة الجديدة ⑤

إذا قمت بتحديد هذا الخيار، يمكنك تكوين إخطار المستخدم بشهادة جديدة.

• بواسطة البريد الإلكتروني ⑤

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 ⑤

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. جاري 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.

• 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.

يمكن تجديد شهادة الجهاز المحمول يدويًا فقط.

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 خانة الاختيار 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.

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.
 3. حدد خانة الاختيار 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 المجلد 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 المجلد خيارات متقدمة وحدد المجلد الفرعي حسابات المستخدمين.

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 المجلد الفرعي الأجهزة المحمولة.

2. في مساحة عمل المجلد الفرعي الأجهزة المحمولة، انقر فوق الزر إضافة جهاز محمول.

يبدأ تشغيل معالج اتصال الجهاز المحمول الجديد.

2. في الصفحة نظام التشغيل الخاصة بالمعالج، حدد iOS بصفته نوع 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 المستخدمين أو مجموعات مستخدمي Active Directory الذين ترغب في إضافة الأجهزة المحمولة الخاصة بهم إلى قائمة الأجهزة المُدارة.

يتم تخطي هذه الخطوة إذا قمت بتشغيل المعالج عن طريق تحديد 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 المعالج مصدر الشهادة، قم بتحديد طريقة إنشاء الشهادة المشتركة التي سيستخدمها خادم الإدارة لتحديد الجهاز المحمول. يمكنك تحديد شهادة مشتركة باستخدام إحدى الطرق التالية:

- إصدار الشهادة من خلال أدوات الإدارة [\[5\]](#)

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](#) 6

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 المعالج طريقة إخطار المستخدم، حدد إعدادات إخطار مستخدم الجهاز المحمول بواسطة رسالة SMS أو بريد إلكتروني حول إنشاء الشهادة:

• [إظهار الرابط في المعالج](#) 6

إذا قمت بتحديد هذا الخيار ، سيتم عرض رابط لحزمة التنصيب في الخطوة الأخيرة من معالج اتصال جهاز جديد.

لا يتوفر هذا الخيار إذا تم تحديد العديد من المستخدمين لاتصال الجهاز.

• [إرسال الرابط إلى المستخدم](#) 6

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 الصفحة 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

إضافة 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 معالج اتصال الجهاز المحمول الجديد خيارين لتسليم وتثبيت شهادة مشتركة و-Kaspersky 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. بدء معالج اتصال الجهاز المحمول الجديد.

2. في الصفحة نظام التشغيل الخاصة بالمعالج، حدد نظام التشغيل Android بصفته نوع نظام تشغيل الجهاز المحمول.

3. في الصفحة طريقة تثبيت Kaspersky Endpoint Security for Android الخاصة بالمعالج، حدد عن طريق استخدام رابط Google Play.

4. في الصفحة حدد المستخدمين الذين ترغب في إدارة أجهزتهم المحمولة الخاصة بالمعالج، حدد المستخدمين أو مجموعات المستخدمين أو مجموعات مستخدمي Active Directory الذين ترغب في إضافة الأجهزة المحمولة الخاصة بهم إلى قائمة الأجهزة المُدارة.

يتم تخطي هذه الخطوة إذا تم تشغيل المعالج عن طريق تحديد إضافة جهاز محمول في قائمة سياق المجلد 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 في القائمة وانقر فوق الزر خصائص.

5. في صفحة المعالج مصدر الشهادة، قم بتحديد 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 5

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 المعالج طريقة إخطار المستخدم، حدد إعدادات إخطار مستخدم الجهاز المحمول بواسطة رسالة SMS أو بريد إلكتروني حول إنشاء الشهادة:

• [إظهار الرابط في المعالج](#)

إذا قمت بتحديد هذا الخيار، سيتم عرض رابط لحزمة التنصيب في الخطوة الأخيرة من معالج اتصال جهاز جديد.

لا تتوفر هذا الخيار إذا تم تحديد العديد من المستخدمين لاتصال الجهاز.

• [إرسال الرابط 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 الصفحة النتيجة، انقر فوق إنهاء لإغلاق المعالج.

بعد انتهاء المعالج، سيتم إرسال رابط ورمز QR إلى جهاز محمول المستخدم مما يتيح تنزيل 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. بدء معالج اتصال الجهاز المحمول الجديد.

2. في الصفحة نظام التشغيل الخاصة بالمعالج، حدد نظام التشغيل Android بصفته نوع نظام تشغيل الجهاز المحمول.

3. في صفحة طريقة تثبيت Kaspersky Endpoint Security for Android الخاصة بالمعالج، حدد باستخدام رابط من خادم الويب.
في الحقل الذي يظهر أدناه، حدد حزمة تثبيت أو قم بإنشاء حزمة جديدة بالنقر فوق جديد.

4. في الصفحة حدد المستخدمين الذين ترغب في إدارة أجهزتهم المحمولة الخاصة بالمعالج، حدد المستخدمين أو مجموعات المستخدمين أو مجموعات مستخدمي Active Directory الذين ترغب في إضافة الأجهزة المحمولة الخاصة بهم إلى قائمة الأجهزة المُدارة.

يتم تخطي هذه الخطوة إذا تم تشغيل المعالج عن طريق تحديد إضافة جهاز محمول في قائمة سياق المجلد 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 المعالج مصدر الشهادة، قم بتحديد طريقة إنشاء الشهادة المشتركة التي سيستخدمها خادم الإدارة لتحديد الجهاز المحمول. يمكنك تحديد شهادة مشتركة باستخدام إحدى الطرق التالية:

• إصدار الشهادة من خلال أدوات 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 المعالج طريقة إخطار المستخدم، حدد إعدادات إخطار مستخدم الجهاز المحمول بواسطة رسالة SMS أو بريد إلكتروني حول إنشاء الشهادة:

• إظهار الرابط في المعالج

إذا قمت بتحديد هذا الخيار، سيتم عرض رابط لحزمة التنشيط في الخطوة الأخيرة من معالج اتصال جهاز جديد.

لا يتوفر هذا الخيار إذا تم تحديد العديد من المستخدمين لاتصال الجهاز.

• إرسال الرابط 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 الصفحة 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. سيطلب 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 الأجهزة المحمولة في Exchange ActiveSync

يوضح هذا القسم المزايا المتقدمة لإدارة أجهزة EAS من خلال Kaspersky Security Center.

بالإضافة إلى إدارة أجهزة EAS بواسطة الأوامر، يستطيع المسؤول استخدام الخيارات التالية:

• [إنشاء ملفات تعريف إدارة أجهزة EAS، وتعيينهم إلى صناديق بريد المستخدمين.](#) ملف تعريف إدارة جهاز EAS هو سياسة Exchange ActiveSync المستخدمة على خوادم Microsoft Exchange لإدارة أجهزة EAS. في ملف تعريف إدارة جهاز EAS، يمكنك تكوين مجموعات الإعدادات التالية:

- إعدادات إدارة كلمة مرور المستخدم
- إعدادات مزامنة البريد
- القيود على استخدام ميزات الجهاز المحمول
- القيود على استخدام تطبيقات المحمول على الجهاز المحمول

بناءً على طراز الجهاز المحمول، يمكن تطبيق الإعدادات الخاصة بملف تعريف الإدارة بشكل جزئي. يمكن عرض حالة سياسة Exchange ActiveSync التي تم تطبيقها في خصائص الجهاز المحمول.

- [عرض معلومات حول إعدادات إدارة جهاز EAS.](#) على سبيل المثال، في خصائص الجهاز المحمول، يمكن للمسؤول عرض آخر وقت للمزامنة مع خادم Microsoft Exchange، ومعرف جهاز EAS، واسم سياسة Exchange ActiveSync وحالتها الحالية على الجهاز المحمول.
- [قطع اتصال أجهزة EAS من الإدارة إذا كانت خارج نطاق الاستخدام.](#)
- تحديد إعدادات استقضاء Active Directory بواسطة خادم الأجهزة المحمولة Exchange، مما يتيح تحديث المعلومات حول صناديق بريد المستخدمين وأجهزتهم المحمولة.

إضافة ملف تعريف الإدارة

لإدارة أجهزة EAS، يمكنك إنشاء ملفات تعريف إدارة جهاز EAS وتعيينهم إلى صناديق بريد Microsoft Exchange.

يمكن تعيين ملف تعريف إدارة جهاز EAS واحد فقط لصندوق بريد Microsoft Exchange.

لإضافة ملف تعريف إدارة جهاز EAS لصندوق بريد Microsoft Exchange:

1. في شجرة وحدة التحكم، افتح المجلد إدارة الجهاز المحمول.
2. في مجلد إدارة الجهاز المحمول في شجرة وحدة التحكم، حدد المجلد الفرعي خوادم الأجهزة المحمولة.
3. في مساحة عمل مجلد خوادم الأجهزة المحمولة، حدد أحد خوادم الأجهزة المحمولة Exchange.
4. في قائمة السياق لخادم الأجهزة المحمولة Exchange، حدد خصائص. يتم فتح نافذة خصائص خادم الجهاز المحمول.
5. في نافذة خصائص خادم Exchange للأجهزة المحمولة، حدد القسم صناديق البريد.
6. حدد صندوق بريد وانقر فوق الزر تعيين ملف تعريف.

ستفتح نافذة ملفات تعريف السياسة.

7. في نافذة ملفات تعريف السياسة، انقر على زر إضافة.

ستفتح نافذة ملف تعريف جديد.

8. قم بتكوين ملف التعريف على علامات تبويب النافذة ملف تعريف جديد.

- إذا كنت ترغب في تحديد اسم ملف التعريف والفواصل الزمني للتحديث، فحدد علامة التبويب عام.
- إذا كنت ترغب بتكوين كلمة المرور لمستخدم الجهاز المحمول، فحدد علامة التبويب كلمة المرور.
- إذا كنت ترغب بتكوين المزامنة مع خادم Microsoft Exchange، فحدد علامة التبويب المزامنة.
- إذا كنت تحتاج إلى تكوين قيود على ميزات الجهاز المحمول، فحدد علامة التبويب قيود المزايا.
- إذا كنت ترغب في تكوين قيود على استخدام تطبيقات المحمول على الجهاز المحمول، فحدد علامة التبويب قيود التطبيقات.

9. انقر على موافق.

سيتم عرض ملف التعريف الجديد في قائمة ملفات التعريف في النافذة ملفات تعريف السياسة.

إذا كنت ترغب في أن يتم تعيين ملف التعريف هذا تلقائيًا إلى صناديق بريد جديدة، وكذلك إلى صناديق البريد التي تم حذف ملفات التعريف الخاصة بها، قم بتحديدتها في قائمة ملفات التعريف وانقر فوق الزر تعيين كملف تعريف افتراضي.

لا يمكن حذف الملف التعريفي الافتراضي. لحذف الملف التعريفي الافتراضي الحالي، يجب تعيين السمة "ملف التعريف الافتراضي" على ملف تعريف مختلف.

10. في نافذة ملفات تعريف السياسة، انقر على موافق.

سيتم تطبيق إعدادات ملف تعريف الإدارة على جهاز EAS في المزامنة التالية للجهاز مع خادم الأجهزة المحمولة Exchange.

إزالة ملف تعريف الإدارة

لإزالة ملف تعريف إدارة جهاز EAS لصندوق بريد Microsoft Exchange:

1. في شجرة وحدة التحكم، افتح المجلد إدارة الجهاز المحمول.
2. في مجلد إدارة الجهاز المحمول في شجرة وحدة التحكم، حدد المجلد الفرعي خوادم الأجهزة المحمولة.
3. في مساحة عمل مجلد خوادم الأجهزة المحمولة، حدد أحد خوادم الأجهزة المحمولة Exchange.
4. في قائمة السياق لخادم الأجهزة المحمولة Exchange، حدد خصائص. يتم فتح نافذة خصائص خادم الجهاز المحمول.
5. في نافذة خصائص خادم الأجهزة المحمولة Exchange، حدد قسم صناديق البريد.
6. حدد صندوق بريد وانقر على زر تغيير ملفات التعريف. يتم فتح نافذة ملف تعريف السياسة.
7. في النافذة ملفات تعريف السياسة، حدد ملف التعريف الذي ترغب في إزالته وانقر فوق زر الحذف الأحمر. سيتم إزالة ملف التعريف المحدد من قائمة ملفات تعريف الإدارة. سوف يتم تطبيق ملف التعريف الافتراضي الحالي إلى أجهزة EAS المدارة بواسطة ملف التعريف الذي تمت إزالته.

إذا كنت ترغب في إزالة ملف التعريف الافتراضي الحالي، قم بإعادة تعيين ملكية "ملف التعريف الافتراضي" لملف تعريف آخر، ثم قم بإزالة ملف التعريف الأول.

التعامل مع سياسات Exchange ActiveSync

بعد تثبيت خادم الأجهزة المحمولة Exchange، في قسم **صناديق البريد** لنافذة خصائص الخادم، يمكنك عرض المعلومات حول حسابات خادم Microsoft Exchange التي تمت استعادتها عن طريق استقصاء المجال الحالي أو المجال الرئيسي.

وكذلك، في نافذة خصائص خادم الأجهزة المحمولة Exchange، يمكنك استخدام الأزرار التالية:

- **تغيير ملفات التعريف** يتيح لك فتح النافذة **ملفات تعريف السياسة** والتي تحتوي على قائمة السياسات التي تمت استعادتها من خادم Microsoft Exchange. في هذه النافذة، يمكنك إنشاء سياسات Exchange ActiveSync أو تحريرها أو حذفها. نافذة **ملفات تعريف السياسة** مشابهة تقريبًا لنافذة تحرير السياسة في وحدة تحكم Exchange Management.
- **تعيين ملفات تعريف إلى الأجهزة المحمولة** يتيح لك تعيين سياسة Exchange ActiveSync محددة لحساب واحد أو حسابات متعددة.
- **تعيين/تعطيل ActiveSync** يتيح لك تمكين HTTP الخاص بـ Exchange ActiveSync أو تعطيله لحساب واحد أو حسابات متعددة.

تكوين نطاق الفحص

في خصائص خادم الأجهزة المحمولة Exchange المثبت حديثًا، في قسم **الإعدادات**، يمكنك تكوين نطاق الفحص، بشكل افتراضي، نطاق الفحص هو المجال الحالي الذي يتم فيه تثبيت خادم الأجهزة المحمولة Exchange. يؤدي تحديد القيمة **المجال الرئيسي** كاملاً إلى توسيع نطاق الفحص ليشمل المجال الرئيسي بالكامل.

العمل باستخدام أجهزة EAS

ستتم إضافة الأجهزة التي تمت استعادتها عن طريق فحص خادم Microsoft Exchange إلى القائمة الشائعة للأجهزة، والموجودة في العقدة **إدارة الجهاز المحمول**، في **المجلد الأجهزة المحمولة**.

إذا أردت أن يقوم **المجلد الأجهزة المحمولة** بعرض أجهزة Exchange ActiveSync فقط (يُشار إليها فيما باسم أجهزة EAS)، قم بتصفية قائمة الأجهزة عن طريق النقر فوق الرابط **(Exchange ActiveSync (EAS** الموجود فوق هذه القائمة.

يمكنك إدارة أجهزة EAS باستخدام الأوامر. على سبيل المثال، يتيح لك الأمر **إعادة التعيين إلى إعدادات المصنع** إزالة كل البيانات من جهاز وإعادة تعيين إعدادات الجهاز إلى إعدادات المصنع. هذا الأمر مفيد في حالة تعرض الجهاز للفق أو السرقة، أو إذا أردت منع وقوع بيانات الشركة أو البيانات الشخصية في أيدي جهة خارجية.

إذا تم حذف كل البيانات من الجهاز، سيتم حذفها مرة أخرى في المرة التالية التي يتم فيها اتصال الجهاز بخادم Microsoft Exchange Server. سيكرر هذا الأمر حتى تتم إزالة الجهاز من قائمة الأجهزة. يتسبب في هذا السلوك المبادئ التشغيلية لخادم Microsoft Exchange server.

لإزالة جهاز EAS من القائمة، في قائمة السياق الخاصة بالجهاز، حدد **حذف**. إن لم يتم حذف حساب Exchange ActiveSync من جهاز EAS، سيعاود الأخير الظهور في قائمة الأجهزة بعد المزامنة التالية للجهاز المثبت عليه خادم Microsoft Exchange.

عرض معلومات حول جهاز EAS

لعرض معلومات حول جهاز EAS

1. في المجلد إدارة الجهاز المحمول في شجرة التحكم، حدد المجلد الفرعي الأجهزة المحمولة.
تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصفية أجهزة EAS عن طريق النقر فوق الرابط (Exchange ActiveSync (EAS).

3. من قائمة سياق الجهاز المحمول، حدد خصائص.

تفتح نافذة خصائص جهاز EAS.

تعرض نافذة خصائص الجهاز المحمول معلومات حول جهاز EAS المتصل.

قطع اتصال جهاز EAS من الإدارة

لقطع اتصال جهاز EAS عن الإدارة بواسطة خادم الأجهزة المحمولة Exchange:

1. في المجلد إدارة الجهاز المحمول في شجرة التحكم، حدد المجلد الفرعي الأجهزة المحمولة.
تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصفية أجهزة EAS عن طريق النقر فوق الرابط (Exchange ActiveSync (EAS).

3. حدد الجهاز المحمول الذي ترغب قطع اتصاله عن الإدارة بواسطة خادم الأجهزة المحمولة Exchange.

4. من قائمة سياق الجهاز المحمول، حدد حذف.

يتم تمييز الجهاز EAS للإزالة برمز صليب أحمر. يتم إزالة الجهاز المحمول من قائمة الأجهزة المدارة عقب إزالته من قاعدة بيانات خادم Exchange ActiveSync. لعمل ذلك، ينبغي على المسؤول إزالة حساب المستخدم على خادم Microsoft Exchange.

حقوق المستخدم لإدارة الأجهزة المحمولة Exchange ActiveSync

لإدارة الأجهزة المحمولة التي تعمل تحت بروتوكول Exchange ActiveSync مع خادم Microsoft Exchange 2010 أو خادم Microsoft Exchange 2013، تأكد من وضع المستخدم في مجموعة الدور حيث يُسمح له بتنفيذ الأوامر التالية:

- Get-CASMailbox
- Set-CASMailbox
- Remove-ActiveSyncDevice
- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings
- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy

لإدارة الأجهزة المحمولة التي تعمل قيد التشغيل تحت بروتوكول Exchange ActiveSync مع خادم Microsoft Exchange 2007، تأكد من حصول المستخدم على حقوق المسؤول. إذا لم يتم منح الحقوق، قم بتنفيذ الـ commandlets لتعيين حقوق المسؤول إلى المستخدم (انظر الجدول أدناه).

يتم طلب حقوق المسؤول لإدارة الأجهزة المحمولة Exchange ActiveSync خادم Microsoft Exchange 2007

الوصول	الكائن	Cmdlet
كاملاً	Branch "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	ermission -User <User or group > -Identity "CN=Mobile Mailbox Policies,CN=<Organization name>,CN=Microsoft =Services,CN=Configuration,DC= name>" -InheritanceType All - AccessRight GenericAll
قراءة	Branch "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC= yourdomain"	ermission -User <User or group e> -Identity "CN=<Organization name>,CN=Microsoft =Services,CN=Configuration,DC= name>" -InheritanceType All - AccessRight GenericRead
قراءة\كتابة	Properties msExchMobileMailboxPolicyLink and msExchOmaAdminWirelessEnable for objects in Active Directory	ermission -User <User or group -Identity "DC=<Domain name>" - heritanceType All -AccessRight erty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable
كاملاً	Mailbox repositories for ms-Exch-Store-Admin	xDatabase Add-ADPermission - or group name> -ExtendedRights ms-Exch-Store-Admin

للحصول على معلومات مُفصلة حول كيفية استخدام commandlets في وحدة تحكم Exchange Management Shell، يُرجى الرجوع إلى موقع ويب [الدعم الفني لخادم Microsoft Exchange](#).

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.

للتوقيع على ملف تعريف iOS MDM بشهادة:

1. في المجلد إدارة الجهاز المحمول في شجرة 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 المجلد 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.

ستفتح نافذة ملف تعريف التكوين الجديد.

7. في النافذة ملف تعريف التكوين الجديد، حدد اسمًا ومعرّفًا 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 المجلد إدارة الجهاز المحمول في شجرة 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 تثبيته 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 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 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 و**حذفه إذا لزم الأمر**.

إزالة ملف تعريف التكوين من جهاز

لإزالة ملف تعريف التكوين من جهاز محمول:

1. في المجلد **إدارة الجهاز المحمول** في شجرة التحكم، حدد المجلد الفرعي **الأجهزة المحمولة**.
تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.

2. في مساحة العمل، قم بتصنيف 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 الأوامر**.

5. في النافذة أوامر إدارة الجهاز 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 مكمّل.

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 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 الجهاز المحمول.

إضافة جهاز جديد بواسطة نشر رابط على ملف تعريف

في وحدة تحكم الإدارة، يقوم المسؤول بإنشاء ملف تعريف iOS MDM، باستخدام معالج اتصال الجهاز المحمول الجديد. يقوم المعالج بالإجراءات 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 صرامة التي تم إدخالها بواسطة شركة Apple، عليك إعداد إصدارات بروتوكول TLS 1.1 و TLS 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 الاتصال بالجهاز الجديد.
2. قم بإنشاء ملف تعريف iOS MDM جديد عن طريق تحديد خانة الاختيار **إظهار الشهادة بعد اكتمال المعالج** من نافذة معالج ملف التعريف الجديد.
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 صرامة التي تم إدخالها بواسطة شركة Apple، عليك إعداد إصدارات بروتوكول TLS 1.1 و TLS 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 المجلد **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 للأجهزة المحمولة. تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.
2. في مساحة العمل، قم بتصنيفية أجهزة iOS MDM بحسب نوع بروتوكول (iOS MDM).
3. حدد جهاز محمول المستخدم الذي يجب تثبيته 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 مكمّل. يمكنك النقر فوق الزر إعادة إرسال 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 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 المجلد إدارة الجهاز المحمول في شجرة التحكم، حدد المجلد الفرعي للأجهزة المحمولة. تعرض مساحة عمل المجلد قائمة بالأجهزة المحمولة المدارة.
2. في مساحة العمل، قم بتصنيفية 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 الجهاز 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 مكمّل. 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 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 الجهاز 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 مدار إلى خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM:

1. في شجرة وحدة التحكم، افتح المجلد 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.

ستفتح 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 الرابط المؤدي إلى متجر التطبيقات حدد معرف Apple ID للتطبيق الذي تريد إضافته أو حدد رابط إلى ملف البيان الذي يمكن استخدامه لتنزيل التطبيق.

9. إذا أردت إزالة تطبيق مدار 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 المجلد إدارة الجهاز المحمول في شجرة 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.

سنتفح 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 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

إزالة تطبيق من جهاز محمول:

1. في المجلد إدارة الجهاز المحمول في شجرة 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 الجهاز 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 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 الجهاز المحمول.

تكوين التجوال على جهاز محمول iOS MDM

لتكوين التجوال:

1. في شجرة وحدة التحكم، افتح المجلد 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 الأوامر.
5. في النافذة أوامر إدارة الجهاز 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 النافذة إعدادات التجوال حدد الإعدادات ذات الصلة:

• تمكين التجوال الصوتي

إذا تم تمكين هذا الخيار، سيتم تمكين التجوال الصوتي على الجهاز المحمول iOS MDM. يمكن لمستخدم الجهاز المحمول iOS MDM إجراء المكالمات والإجابة عليها أثناء التجوال. يتم تمكين هذا الخيار افتراضياً.

• 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 افتراضياً.

يتم تكوين التجوال للأجهزة المحددة.

عرض معلومات حول جهاز iOS MDM

لعرض معلومات حول جهاز iOS MDM:

1. في المجلد إدارة الجهاز المحمول في شجرة 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 المجلد إدارة الجهاز المحمول في شجرة 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.

إدارة أجهزة KES

في Kaspersky Security Center، يمكنك إدارة أجهزة KES المحمولة بالطرق التالية:

- إدارة أجهزة KES مركزياً [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** وقم بتحديد إدارة **حزم تطبيقات محمولة** في القائمة المنسدلة.
3. في نافذة **إدارة حزمة تطبيقات محمولة**، انقر على زر **جديد**.
4. يبدأ معالج إنشاء حزمة تطبيقات المحمول. اتبع إرشادات المعالج.
يتم عرض حزمة تطبيقات المحمول التي تم إنشاؤها حديثاً في النافذة **إدارة حزمة تطبيقات محمولة**.

تمكين المصادقة الثنائية لأجهزة KES

لتمكين المصادقة الثنائية لجهاز KES:

1. افتح سجل النظام الخاص بالجهاز العميل المثبت عليه خادم الإدارة (على سبيل المثال: محلياً، باستخدام الأمر regedit من القائمة بدء > تشغيل).
2. انتقل إلى الخلية التالية:

- لنظام 64 بت:

LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\core\independent\KLLIM

- لنظام 32 بت:

HKLM\Software\KasperskyLab\Components\34\core\independent\KLLIM

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 الإجبارية الثنائية لجهاز KES باستخدام شهادة مشتركة بعد قيامك بتشغيل 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 المجلد إدارة الجهاز المحمول في شجرة 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. ستفتح 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، ويمكن المسؤول من إزالة الجهاز المحمول من قائمة الأجهزة المدارة.

لإزالة جهاز KES من قائمة الأجهزة المدارة:

1. في المجلد إدارة الجهاز المحمول في شجرة 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 قطعه 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 قبل 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 وفقاً 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](#).

يُدمج Kaspersky Security Center وظائف إدارة التشفير للأجهزة التي تعمل بأنظمة تشغيل MAC. 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:

- تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة. يحتوي هذا التقرير على معلومات حول حالة تشفير الأجهزة لكافة مجموعات الأجهزة.
- تقرير حول حقوق الوصول إلى الأجهزة المشفرة. يحتوي هذا التقرير على معلومات حول حالة حسابات المستخدمين الذين منحوا الوصول إلى أجهزة مشفرة.
- تقرير حول أخطاء تشفير الملف. يحتوي هذا التقرير على معلومات حول الأخطاء التي حدثت عند تشغيل مهام تشفير البيانات أو فك تشفيرها على الأجهزة.
- تقرير حول حالة تشفير الأجهزة المُدارة. يحتوي هذا التقرير على معلومات حول ما إذا كانت حالة تشفير الأجهزة تتوافق مع سياسة التشفير أم لا.
- تقرير حول حجب الوصول إلى الملفات المشفرة. يحتوي هذا التقرير على معلومات حول منع وصول التطبيق إلى الملفات المشفرة.

لإنشاء تقرير حول تشفير الأجهزة:

1. في شجرة وحدة التحكم، حدد المجلد **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، فسيبدأ معالج قالب تقرير جديد. 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 المجلد **تشفير البيانات وحمايتها**.

2. قم بأحد الإجراءات التالية:

- انقر فوق الرابط **الإبلاغ عن حقوق الوصول إلى برامج التشغيل المشفرة** في القسم **إدارة محركات الأقراص المشفرة** لبدء تشغيل معالج قالب التقرير الجديد.

- حدد المجلد الفرعي **برامج التشغيل المشفرة**، ثم انقر فوق الزر **الإبلاغ عن حقوق الوصول إلى برامج التشغيل المشفرة** لبدء تشغيل معالج قالب تقرير جديد.

3. اتبع خطوات معالج قالب تقارير جديد.

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 المجلد **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 تقارير جديد.

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 التبويب **التقارير**.

3. انقر فوق الزر **قالب التقرير الجديد** لتشغيل معالج قالب التقرير الجديد.

4. اتبع تعليمات معالج قالب تقارير جديد. في النافذة **تحديد نوع قالب التقرير**، حدد **تقرير حول حالة تشفير الأجهزة المُدارة** في القسم **غير ذلك**.

بعد انتهاء معالج قالب التقارير الجديد، يظهر قالب تقارير جديد في عقدة خادم الإدارة على 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 التبويب **التقارير**.

3. انقر فوق الزر **قالب التقارير الجديد** لبدء تشغيل معالج قالب التقرير الجديد.

4. اتبع تعليمات معالج قالب تقارير جديد. 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 عقدة خادم الإدارة على 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 خادمي الإدارة الاثنان 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.

- يدويًا من خادم إدارة واحد إلى آخر عن طريق تصدير واستيراد الملف الذي يحتوي على مفاتيح التشفير.

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. قم بتفعيل 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.

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.

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 المخزنة على خادم الإدارة والمستخدم لتعقب حالة الأجهزة العملية وخدمتها.

يعرض المجلد المستودعات من شجرة وحدة التحكم البيانات المستخدمة لتتبع حالات الأجهزة العملية.

يحتوي المجلد المستودعات على الكائنات التالية:

• التحديثات التي تم تنزيلها بواسطة خادم الإدارة والتي يتم توزيعها على الأجهزة العملية.

• 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 العملية.

- الملفات التي تأجل فحصها بواسطة تطبيقات الأمان.

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 وبأعي 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 خطراً، وتعيّن الحالات إلى الملفات، وتضع بعضها في المستودع.

على سبيل المثال، تقوم تطبيقات الأمان بالتالي:

- تحفظ نسخة 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 بالأمان.

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 جزئياً مع قسامة 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 يدوياً في المستودع لأن سلوك الملف يبعث على الشك باحتوائه على بعض التهديدات. يمكن للمستخدم فحص الملف بحثاً 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.
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 لخدام إدارة Kaspersky Security Center. يتم تخزين هذه المعلومات كقائمة في المجلد الفرعي **تشغيل القواعد في حالة التدريب الذكي** للمجلد **المستودعات**. يمكنك **تأكيد عمليات الكشف باعتبارها صحيحة** أو **إضافتها باعتبارها استثناءات**، حتى لا يتم اعتبار هذا النوع من السلوك مخالفاً 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 **تشغيل القواعد 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 وتأكيد. تستمر هذه الحالة إلى حين إجراء المزامنة التالية للجهاز العميل مع خادم الإدارة؛ وبعد إجراء المزامنة، يختفي العنصر من القائمة.
فارغ—إذا لم يتم المسؤول بمعالجة هذا العنصر.

• تم تشغيل إجمالي قواعد الأوقات ⑤

عدد الاكتشافات ضمن قاعدة تجريبية واحدة، وعملية واحدة، وجهاز عميل واحد. يتم احتساب هذا العدد بواسطة Kaspersky Endpoint Security.

• اسم المستخدم ⑤

اسم مستخدم الجهاز العميل الذي قام بتشغيل العملية التي قامت بتوليد الكشف.

• مسار معالجة المصدر ⑤

المسار إلى عملية المصدر، أي العملية التي تؤدي الإجراء (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

• تجزئة معالجة المصدر ⑤

تجزئة SHA-256 لملف العملية المصدر (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

• مسار كائن المصدر ⑤

المسار إلى الكائن الذي بدأ العملية (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

• تجزئة كائن المصدر ⑤

تجزئة SHA-256 لملف المصدر (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

• مسار معالجة الهدف ⑤

المسار إلى العملية المستهدفة (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

• تجزئة معالجة الهدف ⑤

تجزئة SHA-256 للملف المستهدف (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

• مسار كائن الهدف ⑤

المسار إلى الكائن المستهدف (لمزيد من المعلومات، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

• تجزئة كائن الهدف ⑤

تجزئة SHA-256 للملف المستهدف (لمزيد من المعلومات ، يُرجى الرجوع إلى تعليمات Kaspersky Endpoint Security).

• تمت المعالجة 9

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 تشغيل القواعد في حالة التدريب الذكي (بشكل افتراضي، يصبح هذا المجلد الفرعي لـ خيارات متقدمة ← المستودعات).
3. في مساحة العمل تشغيل القواعد 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 في قائمة السياق.

يبدأ تشغيل [معالج إضافة الاستثناءات](#). اتبع تعليمات المعالج.

إذا قمت برفض أو تأكيد عنصر ما، فسيتم استنواؤه 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 الاستثناءات بإضافة استثناءات من قواعد مراقبة عيوب التكيف لـ Kaspersky Endpoint Security.

يمكنك بدء تشغيل المعالج من خلال أحد الإجراءات الثلاثة أدناه.

لبدء معالج إضافة الاستثناءات من خلال عقدة مراقبة عيوب التكيف:

1. في شجرة وحدة التحكم، حدد عقدة خادم الإدارة المطلوب.

2. حدد تشغيل القواعد في حالة التدريب الذكي (بشكل افتراضي، يصبح هذا المجلد الفرعي لخيارات 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 الاستثناءات.

يمكنك بدء معالج إضافة الاستثناءات 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 أيضاً.

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 Kaspersky الموجودة على الأجهزة. يتم من خلال عملاء الشبكة الموجودة على الأجهزة العملية 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 مكافحة الفيروسات على هذه المستودعات، وحذف الملفات من عليها. [رموز حالات الملف موضحة في الملحق.](#)

يتم دعم عمليات العزل والنسخ الاحتياطي في الإصدارات 6.0 أو الأحدث من تطبيق Kaspersky Anti-Virus for Windows Workstations و Kaspersky Anti-Virus for Windows Servers بالإضافة إلى Kaspersky Endpoint Security 10 for Windows أو الإصدارات الأحدث.

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 افتراضياً 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 خانة الاختيار على تطبيق الأمن المستخدم حالياً.

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 المفاتيح **Ctrl** و **Shift**.

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 العملية 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 المفاتيح **Ctrl** و **Shift**.
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 العملية 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 ملفاً 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 المفاتيح **Ctrl** و **Shift**.

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 المخزن 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 تأجيلها 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 المجلد الفرعي **تهديدات نشطة**.

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**.

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. يتم نسخ الملفات إلى المجلد المحدد في الجهاز الذي تم تثبيت Kaspersky Security Center عليه. يمكنك تنزيل ملف فقط إذا تم تخزين الملف في **تخزين النسخ الاحتياطي** للجهاز 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 المجلد الفرعي **تهديدات نشطة**.

2. في مساحة عمل مجلد **تهديدات نشطة**، حدد الملفات التي ينبغي عليك حذفها باستخدام المفاتيح **Ctrl** و **Shift**.

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**.

(Kaspersky Security Network (KSN

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.

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 ضماناً 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 صيبت Kaspersky لاسترداد المعلومات حول التطبيقات المثبتة على الأجهزة المُدارة.

بالمشاركة في KSN، فأنت توافق على إرسال معلومات بشكل تلقائي إلى Kaspersky حول تشغيل تطبيقات Kaspersky المثبتة على الأجهزة العميلة والمُدارة عبر Kaspersky Security Center. يتم نقل المعلومات وفقاً لإعدادات [وصول KSN](#) الحالية.

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، سيتم عرضه لك عندما تحدث خادم الإدارة أو تقوم بتفريته. 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 DNS العام. يعد ذلك ضرورياً للتأكد من الحفاظ على مستوى الأمان للأجهزة المُدارة.

تتفاعل الأجهزة العميلة المُدارة بواسطة خادم الإدارة مع KSN عبر خدمة وكيل KSN. يوفر 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.

يمكنك تكوين خادم وكيل KSN في القسم **وكيل KSN** من 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، مكن 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 بتفعيل خيار **أوافق على استخدام شبكة 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 **شبكة KSN الخاصة**، مكن خيار **تكوين شبكة KSN الخاصة** وانقر على زر **تحديد ملف** من خلال **إعدادات وكيل شبكة KSN** لتنزيل إعدادات شبكة KSN الخاصة (الملفات بالامتدادين pkcs7 و pem). عقب تنزيل الإعدادات، تعرض الواجهة اسم المزود وجهات الاتصال، وكذلك تاريخ إنشاء الملف مع إعدادات شبكة KSN الخاصة.

عند تمكين شبكة KSN الخاصة، انتبه إلى نقاط التوزيع التي تم تكوينها لإرسال طلبات KSN مباشرة إلى سحابة KSN. ستواصل نقاط التوزيع المثبت 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 KSN الخاصة، مكن 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 شبكة KSN الخاصة**، تظهر رسالة بالتفاصيل حول شبكة KSN الخاصة. تدعم تطبيقات Kaspersky التالية شبكة KSN الخاصة:

- Kaspersky Security Center 10 Service Pack 1 أو أحدث
- Kaspersky Endpoint Security 10 Service Pack 1 for Windows أو أحدث
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

في حالة تمكين الخيار **تكوين شبكة KSN الخاصة** في Kaspersky Security Center، تتلقى هذه التطبيقات معلومات حول دعم شبكة KSN الخاصة. في نافذة إعدادات التطبيق وفي القسم الفرعي **Kaspersky Security Network** الخاص بالقسم **الحماية المتقدمة من التهديد**، يظهر **موفر شبكة KSN**: شبكة KSN الخاصة. وإلا، يظهر **موفر شبكة KSN**: شبكة KSN العالمية.

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 KSN الخاصة، نوصيك باستخدام خوادم الإدارة الثانوية التي لم يتم تمكين استخدام شبكة KSN الخاصة لها.

لا يرسل Kaspersky Security Center أي بيانات إحصائية إلى Kaspersky Security Network في حالة تكوين شبكة KSN الخاصة 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 KSN الخاصة مباشرة، مكن خيار **تجاهل إعدادات خادم وكيل عند الاتصال بشبكة KSN الخاصة**. وإلا، لا يمكن وصول الطلبات الصادرة من التطبيقات المُدارة إلى شبكة KSN الخاصة.

6. تكوين اتصال خادم الإدارة بخدمة وكيل KSN:

• ضمن **إعدادات الاتصال**، للمنفذ **منفذ TCP**، حدد رقم منفذ TCP الذي سيستخدم للاتصال بخادم وكيل KSN. والمنفذ الافتراضي للاتصال بخادم وكيل KSN هو 13111.

• إذا أردت أن يكون خادم الإدارة متصلًا بخادم وكيل KSN عبر منفذ UDP، مكن خيار **استخدام منفذ UDP** وحدد رقم منفذ لـ **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.

7. قم بتفعيل خيار **توصيل خوادم الإدارة الثانوية بشبكة KSN عبر خادم الإدارة الأساسي**.

إذا تم تحديد هذا الخيار، ستستخدم خوادم الإدارة الثانوية خادم الإدارة الرئيسي 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

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 المدارة إلى Kaspersky مباشرة دون استخدام خادم الإدارة.

لإعداد وصول نقطة التوزيع إلى KSN (Kaspersky Security Network):

1. تأكد من أن نقطة التوزيع **معيّنة 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 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. حدد صندوق التحديد أو افق على استخدام شبكة Kaspersky Security Network.
سيتم تمكين KSN.
إذا تم تحديد خانة الاختيار هذه، فسترسل الأجهزة العملية 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 أو افق على استخدام شبكة Kaspersky Security Network.
إذا تم إلغاء تحديد خانة الاختيار هذه، فلن ترسل الأجهزة العملية نتائج تثبيت التصحيح إلى Kaspersky.
إذا كنت تستخدم شبكة KSN خاصة، قم بإلغاء تحديد خانة الاختيار تكوين شبكة KSN الخاصة.
سيتم تعطيل KSN.
5. انقر على موافق.

عرض بيان KSN المقبول

عندما تقوم بتمكين KSN (Kaspersky Security Network)، 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.

عرض إحصائيات خادم وكيل KSN

خادم وكيل KSN هو خدمة تضمن التفاعل بين البنية الأساسية [Kaspersky Security Network](#) والأجهزة العملية التي يديرها خادم الإدارة.

يوفر لك استخدام خادم وكيل KSN الميزات التالية:

- يمكن للأجهزة العملية 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 إحصائيات تشغيل خادم وكيل KSN. إذا لزم الأمر، قم باتخاذ الإجراءات الإضافية التالية:

- انقر فوق **تحديث لتحديث** الإحصائيات حول استخدام خادم وكيل 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 متصلًا 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 بتحديثه. 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 ترفيقته، 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 وفقاً 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 كوكيل KSN

يمكنك تمكين وكيل KSN على جهاز مُدار تم تعيينه للعمل كنقطة توزيع. يعمل الجهاز المُدار كوكيل KSN عند تشغيل خدمة ksnproxy على الجهاز. يمكنك التحقق من هذه الخدمة أو تشغيلها أو إيقاف تشغيلها على الجهاز محليًا.

للتحقق مما إذا كانت نقطة التوزيع تعمل كوكيل 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 كوكيل 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.

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 14 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).

السيناريو: تكوين تصدير الحدث إلى نظام SIEM

يسمح Kaspersky Security Center بالتكوين بإحدى الطرق التالية: التصدير إلى أي نظام SIEM يستخدم تنسيق Syslog أو التصدير إلى أنظمة QRadar و Splunk و ArcSight SIEM التي تستخدم تنسيقات LEEF و CEF أو تصدير الأحداث إلى أنظمة SIEM مباشرة 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](#)، و [وضع علامة على الأحداث العامة للتصدير بتنسيق Syslog](#)

○ Kaspersky Security Center 14 Web Console: [وضع علامة على أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog](#)، و [وضع علامة على الأحداث العامة للتصدير بتنسيق Syslog](#)

- قم بتكوين تصدير الأحداث إلى نظام SIEM باستخدام إحدى الطرق التالية:

○ استخدام TCP/IP أو UDP أو TLS من خلال بروتوكولات TCP.

تعليمات للمساعدة:

■ وحدة تحكم الإدارة: [تكوين تصدير الأحداث إلى أنظمة SIEM](#)

■ Kaspersky Security Center 14 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 [\(klakdb.chm\)](#)).

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 للتصدير 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 المدارة. 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 الاستجابة السريعة لأحداث نظام الأمن التي تحدث في الأجهزة المدارة أو مجموعات الأجهزة.

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 بناءً على 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.

يحتوي كل حدث على مستوى الأهمية الخاص به. بناءً 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 خطيراً بالضرورة، غير أنه يشير إلى مشكلة محتملة في المستقبل. يتم تعيين معظم الأحداث كتحذيرات إذا كان من الممكن استعادة التطبيق بدون فقدان البيانات أو الإمكانات 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 مدة تخزين محددة، يمكنك خلالها عرضها في Kaspersky Security Center أو تعديلها. لا يتم حفظ بعض البيانات في قاعدة بيانات خادم الإدارة بشكل افتراضي لأن مدة 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 تنشأها 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 أيضاً وظيفة تجميع البيانات التي تم رصدها لمساعدتك في تجنب فقدان الأحداث الحرجة. إضافة إلى ذلك، تُجري الأنظمة تحليلاً تلقائياً 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 الموافقة على التحديثات [عبر وحدة تحكم الإدارة](#) أو [عبر Kaspersky Security Center 14 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 و LEED إلى أنظمة QRadar و Splunk و ArcSight.

يمكنك استخدام بروتوكولي CEF و LEED لتصدير الأحداث العامة. عند تصدير الأحداث عبر بروتوكولات CEF و LEED، فلن يكون لديك إمكانية تحديد أحداث محددة لتصديرها. وبدلاً من ذلك، يتم تصدير جميع الأحداث العامة. خلافاً لبروتوكول Syslog، لا تعتبر البروتوكولات CEF و LEED بروتوكولات عامة. تكون البروتوكولات CEF و LEED مخصصة لأنظمة SIEM المناسبة (QRadar و Splunk و ArcSight). لذا، عند اختيارك لتصدير الأحداث عبر واحد من هذه البروتوكولات، فستستخدم المحلل المطلوب في نظام SIEM.

لتصدير الأحداث عبر بروتوكولات CEF و LEED، يجب تنشيط ميزة التكامل مع أنظمة SIEM في خادم الإدارة باستخدام [مفتاح ترخيص نشط أو رمز تنشيط صالح](#).

• بشكل مباشر من قاعدة بيانات Kaspersky Security Center إلى نظام SIEM.

يمكن استخدام هذه الوسيلة الخاصة بتصدير الأحداث لاستلام الأحداث مباشرة 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](#)

هذا هو بروتوكول نقل الرسالة، إما أن يكون TCP/IP أو UDP. يجب أن يكون هذا البروتوكول مطابقاً لما حددته في Kaspersky Security Center.

• [المنفذ](#)

رقم المنفذ للاتصال بـ Kaspersky Security Center. يجب أن يكون هذا المنفذ مطابقاً 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 وفقاً 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.

Edit Receiver

If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.

Name: tcp cef

IP/Host: All

Port: 616

Encoding: UTF-8

Source Type: CEF

Enable:

Save Cancel

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 محلات الرسالة جزءًا من نظام SIEM، إذ تُستخدم لتجزئة محتويات الرسالة في الحقول ذات الصلة، مثل معرف الحدث والخطورة والوصف والمعلومات وما إلى ذلك. يتيح هذا الإجراء لنظام SIEM معالجة الأحداث المستلمة من Kaspersky Security Center حتى يمكن تخزينها في قاعدة بيانات نظام SIEM.

يحتوي كل نظام من أنظمة SIEM على مجموعة من محلات الرسالة القياسية. يوفر Kaspersky أيضًا محلات الرسالة لبعض أنظمة SIEM، على سبيل المثال، QRadar و ArcSight. يمكنك تنزيل هذه الرسائل من مواقع ويب أنظمة SIEM المطابقة. عند تكوين المستلم، يمكنك استخدام أحد محلات الرسالة القياسية أو محلل رسالة من Kaspersky.

وضع علامة على الأحداث للتصدير إلى أنظمة SIEM بتنسيق Syslog

يصف هذا القسم كيفية وضع علامة على الأحداث لتصدير المزيد منها إلى أنظمة SIEM بتنسيق Syslog.

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 وفقاً لأحد الشروط التالية:

- وضع علامة على الأحداث العامة. إذا وضعت علامة على الأحداث التي تريد تصديرها في سياسة، فسيتم تلقي 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، فسيتم تلقي 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 سابقاً 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 حدثاً 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 حدثاً 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.

The screenshot shows a configuration window titled "الخصائص: انتشار الفيروسات" (Properties: Virus Distribution). It has a close button (X) in the top left. The window is divided into two main sections: "تسجيل الحدث" (Event Logging) and "الإخطارات بالأحداث" (Event Notifications). In the "تسجيل الحدث" section, there is a dropdown menu set to "180". Below it, there are three checkboxes: "تخزين في قاعدة البيانات الخاصة بخادم الإدارة لمدة (بالأيام):" (checked), "تصدير إلى نظام SIEM باستخدام Syslog" (unchecked), "تخزين في سجل أحداث نظام التشغيل (OS) على جهاز" (unchecked), and "تخزين في سجل أحداث نظام التشغيل (OS) على خادم إدارة" (unchecked). The "الإخطارات بالأحداث" section has four checkboxes: "إخطار عبر البريد الإلكتروني" (unchecked), "إخطار عبر رسالة SMS" (unchecked), "إخطار عن طريق تشغيل ملف تنفيذي أو برنامج نصي" (unchecked), and "الإخطار بواسطة SNMP" (unchecked). Below these checkboxes, there is a note: "يشكل افتراضى، يتم استخدام إعدادات الإخطار التي تم تحديدها في علامة تبويب خصائص خادم الإدارة (مثل عنوان المستلم). لتحديد إعدادات فردية، انقر فوق رابط الإعدادات." (By default, the system uses the notification settings specified in the Administration Server Properties tab (such as recipient address). To specify individual settings, click the Settings link). At the bottom of the window, there are two buttons: "إعدادات" (Settings) and "موافق" (OK). The "موافق" button is highlighted with a blue border.

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 المعيار [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 و LEEF

يمكنك استخدام تنسيقات CEF و LEEF لتصدير [الأحداث العامة](#) إلى أنظمة SIEM، وكذلك الأحداث التي تنقلها تطبيقات Kaspersky إلى خادم الإدارة. تم تحديد مجموعة تصدير الأحداث مسبقاً، ولا يمكنك تحديد أحداث لتصديرها.

لتصدير الأحداث عبر بروتوكولات CEF و LEEF، يجب تنشيط ميزة التكامل مع أنظمة SIEM في خادم الإدارة باستخدام [مفتاح ترخيص نشط أو رمز تنشيط صالح](#).

حدد تنسيق التصدير بناءً على نظام SIEM المستخدم. يوضح الجدول أدناه أنظمة SIEM وتنسيقات التصدير المطابقة.

تنسيقات تصدير الحدث إلى نظام SIEM

تنسيق التصدير	نظام SIEM
LEEF	QRadar
CEF	ArcSight
CEF	Splunk

• LEEF (Log Event Extended Format) - تنسيق حدث مخصص لـ IBM Security QRadar SIEM. 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.

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 و LEEF. يتعذر تصدير [الأحداث المخصصة للتطبيق](#) من التطبيقات المُدارة عبر تنسيقات CEF و LEEF. 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.

لتمكن 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** وحدد **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 تلقائياً 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)، و ArcSight (تنسيق CEF) و Splunk® (تنسيق CEF) و Syslog (RFC 5424).

• **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 مطابقاً للرقم الذي يستخدمه نظام SIEM الخاص بك لاستلام الأحداث (راجع قسم تكوين نظام SIEM للاطلاع على التفاصيل).

• البروتوكول 9

حدد البروتوكول الذي سيستخدم لنقل الرسائل إلى نظام SIEM. يمكنك تحديد إما بروتوكول TCP/IP، أو UDP أو TLS من خلال بروتوكول TCP.

حدد إعدادات TLS التالية إذا قمت بتحديد TLS عبر بروتوكول TCP:

• مصادقة الخادم

في حقل مصادقة الخادم، يمكنك تحديد قيم الشهادات الموثوق بها أو بصمات أصابع SHA:

• **شهادات موثوقة.** يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى Kaspersky Security Center. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم نظام SIEM موقعة أيضاً من قبل مرجع مصدق موثوق أم لا. لإضافة شهادة موثوقة، انقر فوق الزر **تصفح ملف شهادات CA**، ثم قم بتحميل الشهادة.

• **بصمات SHA.** يمكنك تحديد بصمات الإبهام SHA-1 لشهادات نظام SIEM في Kaspersky Security Center. لإضافة بصمة إبهام SHA-1، أدخلها في حقل **بصمات الإبهام**، ثم انقر فوق الزر **إضافة**.

باستخدام إعداد **إضافة مصادقة العميل**، يمكنك إنشاء شهادة لمصادقة Kaspersky Security Center. وبالتالي، ستستخدم شهادة موقعة ذاتياً صادرة عن Kaspersky Security Center. في هذه الحالة، يمكنك استخدام شهادة موثوقة وبصمة SHA لمصادقة خادم نظام SIEM.

• أضف اسم الموضوع/الاسم البديل للموضوع

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 **أضف اسم الموضوع/الاسم البديل للموضوع**. إذا تطابق أي من أسماء الموضوعات المحددة مع اسم موضوع شهادة نظام SIEM، فسيتحقق Kaspersky Security Center من صحة شهادة خادم نظام SIEM.

• إضافة مصادقة العميل

لمصادقة العميل، يمكنك إدخال شهادتك أو إنشائها في Kaspersky Security Center.

• **أدخل شهادة.** 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 شهادة PEM.** قم بتحميل ملف بشهادة في الحقل **ملف مع شهادة**، وملف بمفتاح خاص في الحقل **ملف مع مفتاح**. كلا الملفين لا يعتمدان على بعضهما البعض وترتيب تحميل الملفات ليس مهماً. عند تحميل كلا الملفين، حدد كلمة المرور لفك تشفير المفتاح الخاص في حقل **التحقق من كلمة المرور أو الشهادة**. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

• **X.509 شهادة PKCS12.** قم بتحميل ملف واحد يحتوي على شهادة ومفتاحها الخاص في الحقل **ملف مع شهادة**. عند تحميل الملف، حدد كلمة المرور لفك تشفير المفتاح الخاص في حقل **التحقق من كلمة المرور أو الشهادة**. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

• **إنشاء مفتاح.** يمكنك إنشاء شهادة موقعة ذاتياً في Kaspersky Security Center. نتيجة لذلك، يخزن Kaspersky Security Center الشهادة الموقعة ذاتياً التي تم إنشاؤها، ويمكنك تمرير الجزء العام من الشهادة أو بصمة SHA1 إلى نظام SIEM.

إذا قمت بتحديد تنسيق Syslog، فيجب عليك تحديد:

• الحد الأقصى لحجم الرسالة، بوحدات البايت 9

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.

5. إذا كنت تريد تصدير الأحداث التي حدثت بعد تاريخ محدد في الماضي إلى قاعدة بيانات نظام SIEM، فانقر فوق الزر تصدير الأرشيف وحدد تاريخ بدء تصدير الأحداث. سيبدأ تصدير الحدث بشكل افتراضي بعد تمكينك له على الفور.

6. 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 هذه آراء الجمهور في وثيقة klakdb.chm.

يشتمل الرأي العام v_akpub_ev_event على مجموعة حقول تمثل معلمات الحدث في قاعدة البيانات. في الوثيقة klakdb.chm يمكنك أيضاً 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 لإنشاء استعلام SQL بواسطة أداة klsq2 المساعدة ومثال الاستعلام.

لإنشاء استعلامات SQL أو آراء قاعدة البيانات، يمكنك أيضاً استخدام أي برنامج آخر للتعامل مع قوعد البيانات. يتم ذكر معلومات حول كيفية عرض المعلمات للاتصال بقاعدة بيانات Kaspersky Security Center، مثل اسم الممثل واسم قاعدة البيانات، في [القسم المقابل](#).

إنشاء استعلام SQL باستخدام أداة klsq2 المساعدة

يوضح هذا القسم كيفية تنزيل أداة klsq2 المساعدة واستخدامها، وكيفية إنشاء استعلام SQL باستخدام هذه الأداة المساعدة. عندما تقوم بإنشاء استعلام SQL بواسطة أداة klsq2 المساعدة، لا يتعين عليك توفير اسم قاعدة البيانات ومعلمات الوصول، لأن الاستعلام يتعامل مع الرؤى العامة لـ Kaspersky Security Center بشكل مباشر.

لتنزيل أداة klsq2 المساعدة واستخدامها:

1. تنزيل klakdb.chm من الموقع الإلكتروني لـ Kaspersky.

2. انسخ ملف klsq2.zip الذي تم تنزيله وفك ضغطه في أي مجلد على الجهاز المثبت عليه خادم إدارة Kaspersky Security Center. تشتمل حزمة klsq2.zip على الملفات التالية:

- klsql2.exe
- src.sql
- start.cmd

3. افتح ملف src.sql في أي محرر نصوص.

4. في ملف src.sql، اكتب الاستعلام الذي تريده. ثم احفظ الملف.

5. في الجهاز المثبت عليه خادم إدارة Kaspersky Security Center، في سطر الأوامر، اكتب الأمر التالي لتشغيل استعلام SQL من الملف src.sql واحفظ النتائج على الملف result.xml:

```
klsql2 -i src.sql -o result.xml
```

6. افتح الملف result.xml الذي تم إنشاؤه حديثاً لعرض نتائج الاستعلام.

يمكنك تحرير الملف src.sql وإنشاء أي استعلام للرؤى العامة. بعد ذلك، من سطر الأوامر، قم بتنفيذ استعلامك واحفظ النتائج على ملف.

مثال لاستعلام SQL في أداة klsql2 المساعدة

يعرض هذا القسم مثالاً لاستعلام SQL، الذي يتم إنشاؤه بواسطة أداة klsql2 المساعدة.

يوضح المثال التالي استعادة الأحداث التي حدثت في الأجهزة خلال السبعة أيام الماضية، وعرض للأحداث التي طُلبت وقت حدوثها، ويتم عرض الأحداث الأخيرة أولاً.

مثال:

```

تحديد
e.nId , /* معرّف الحدث */
e.tmRiseTime /* الوقت، وقت وقوع الحدث.
e.strEventType /* الاسم الداخلي لنوع الحدث */
e.wstrEventTypeDisplayName /* الاسم المعروف للحدث */
e.wstrDescription /* الوصف المعروف للحدث */
e.wstrGroupName /* اسم المجموعة حيث يوجد الجهاز */
h.wstrDisplayName /* الاسم المعروف للجهاز الذي وقع عليه الحدث */
+ '.' + ((CAST(((h.nIp / 16777216) & 255) AS varchar(4
+ '.' + ((CAST(((h.nIp / 65536) & 255) AS varchar(4
+ '.' + ((CAST(((h.nIp / 256) & 255) AS varchar(4
*/CAST(((h.nIp) & 255) AS varchar(4)) as strIp
الحدث
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
(())WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE
ORDER BY e.tmRiseTime DESC

```

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 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.

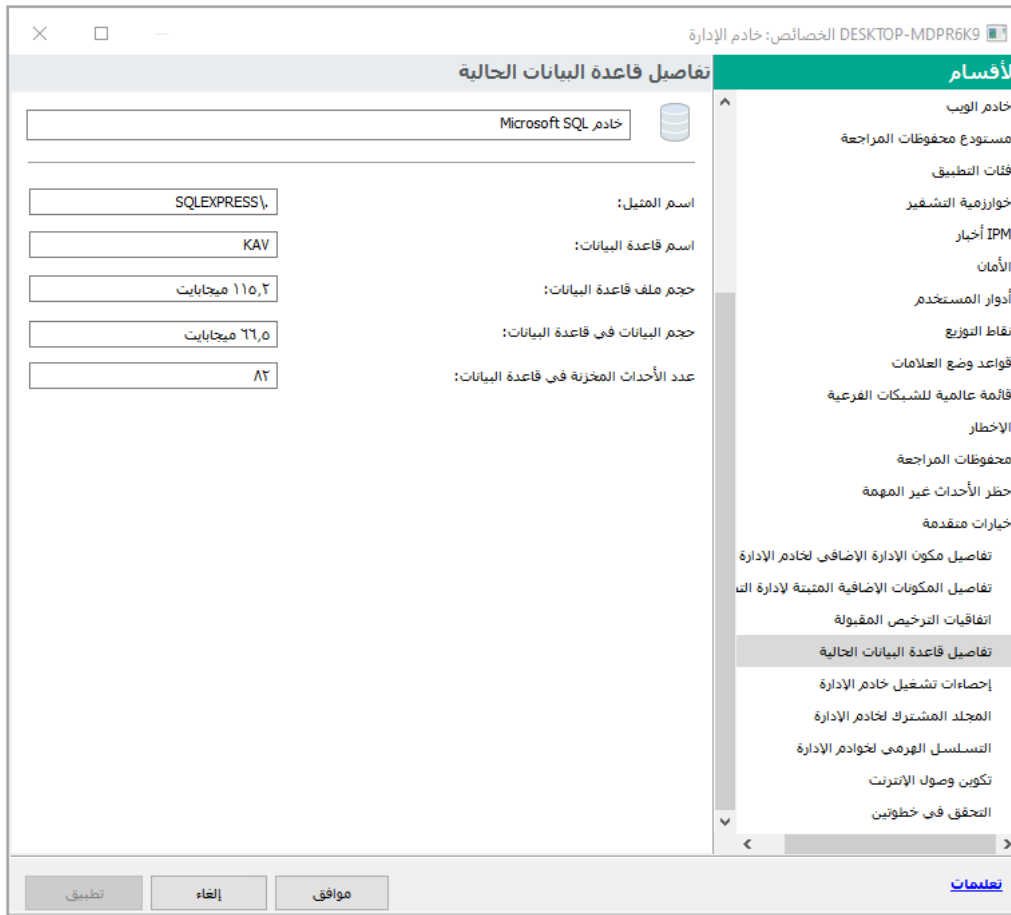
3. في القسم تفاصيل قاعدة البيانات الحالية، لاحظ خصائص قاعدة البيانات التالية (انظر الشكل أدناه):

• 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.



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.

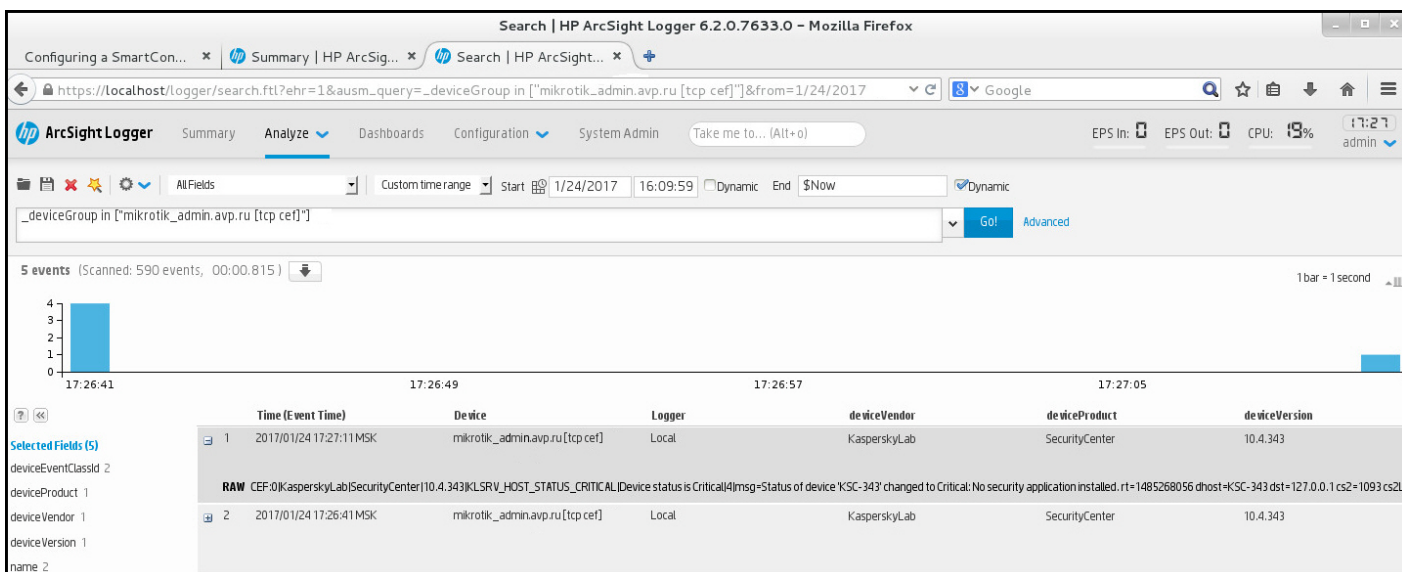
عرض نتائج التصدير

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 المرسله 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 لخدم 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. 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.

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 بلاحة تصف العداد. على سبيل المثال: العداد الذي يحتوي على قيمة 1.3.6.1.4.1.23668.1093.11.4 له لاحقة بقيمة 11.4.

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 لمعرفة الكائن 1.1.4، ستكون اللائحة هي "1 kladminkit" (`::= { counters`).

3. حدد مساحة الاسم التي تصف القيمة الثانية.

على سبيل المثال: بالنسبة لمعرفة الكائن 1.1.4، ستكون اللائحة هي `counters 1`، والتي تمثل النشر.

4. حدد مساحة الاسم التي تصف القيمة الثالثة.

على سبيل المثال: بالنسبة لمعرفة الكائن 1.1.4، ستكون اللائحة هي النشر 4، والتي تمثل `hostsWithAntivirus`.

اسم عداد السلسلة هو سلسلة من هذه القيم، على سبيل المثال `MIB base`

`namespace>.counters.deployment.hostsWithAntivirus` و هو 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

الوصف	معرف الكائن	نوع البيانات الرقمية	قيمة معرف الكائن
<p>حالة النشر. يمكن أن تكون الحالة أي مما يلي:</p> <ul style="list-style-type: none"> • معلومات الترخيص لم يعد صالحًا لعدد N أجهزة. • تحذير واحد مما يلي: <ul style="list-style-type: none"> يوجد M أجهزة مثبت عليها تطبيقات Kaspersky على إجمالي N في مجموعات خادم الإدارة ($N > M$). الترخيص L ينتهي على N أجهزة خلال M أيام. المهمة T لثبيت التطبيقات قد اكتملت بنجاح على N أجهزة، وإعادة التشغيل مطلوبة لعدد M أجهزة. • حرج الترخيص انتهى لعدد N أجهزة. • جيد. ولا واحد مما سبق. 	1.3.6.1.4.1.23668.1093.1.1.1.	<p>INTEGER } جيد (0)، معلومات (1)، تحذير (2)، حرج (3) {</p>	deploymentStatus
سبب أن deploymentStatus تعرض	1.3.6.1.4.1.23668.1093.1.1.2.1.	INTEGER }	noAntivirusSoftware

أن مجموعة خادم الإدارة تحتوي على الكثير من الأجهزة دون تطبيقات مُدارة. القيمة تساوي 1 في حال العثور على عدد قليل من الأجهزة دون تطبيقات مُدارة، و 0 بخلاف ذلك.		معطل (0) ، مفعّل (1) }	
سبب أن deploymentStatus تعرض أن مهمة التثبيت عن بُعد قد تعذرت على بعض الأجهزة. يمكن معرفة عدد تلك الأجهزة عبر .hostsRemoteInstallFailed	1.3.6.1.4.1.23668.1093.1.1.2.2.	} INTEGER معطل (0) ، مفعّل (1) }	remoteInstallTaskFailed
سبب أن deploymentStatus تعرض أنه يوجد بعض الأجهزة بترخيص ينتهي خلال ال 7 أيام القادمة. يمكن معرفة عدد تلك الأجهزة عبر .hostsLicenseExpiring	1.3.6.1.4.1.23668.1093.1.1.2.3.	} INTEGER معطل (0) ، مفعّل (1) }	licenceExpiring
سبب أن deploymentStatus تعرض أنه يوجد بعض الأجهزة ذات ترخيص منتهي. يمكنك معرفة عدد تلك الأجهزة عبر .hostsLicenseExpired	1.3.6.1.4.1.23668.1093.1.1.2.4.	} INTEGER معطل (0) ، مفعّل (1) }	licenceExpired
عدد الأجهزة في مجموعات خادم الإدارة.	1.3.6.1.4.1.23668.1093.1.1.3.	Counter32	hostsInGroups
عدد الأجهزة في مجموعات خادم الإدارة المثبت عليها تطبيقات مُدارة.	1.3.6.1.4.1.23668.1093.1.1.4.	Counter32	hostsWithAntivirus
عدد الأجهزة التي تعذر عليها مهمة التثبيت عن بُعد.	1.3.6.1.4.1.23668.1093.1.1.5.	Counter32	hostsRemoteInstallFailed
معرف مفتاح ترخيص ينتهي قريباً (خلال أقل من 7 أيام).	1.3.6.1.4.1.23668.1093.1.1.6.	سلسلة ثمانية	licenceExpiringSerial
معرف مفتاح الترخيص المنتهي.	1.3.6.1.4.1.23668.1093.1.1.7.	سلسلة ثمانية	licenceExpiredSerial
عدد الأيام قبل انتهاء ترخيص.	1.3.6.1.4.1.23668.1093.1.1.8.	Unsigned32	licenceExpiringDays
عدد الأجهزة ذات ترخيص ينتهي قريباً (خلال أقل من 7 أيام).	1.3.6.1.4.1.23668.1093.1.1.9.	Counter32	hostsLicenceExpiring
عدد الأجهزة التي قد انتهى ترخيصها.	1.3.6.1.4.1.23668.1093.1.1.10.	Counter32	hostsLicenceExpired
الحالة الحالية لقواعد مكافحة الفيروسات. يمكن أن تكون الحالة أي مما يلي: • معلومات. لم يتم تحديث خادم الإدارة منذ أكثر من يوم، وقد مر أقل من يوم منذ تثبيت التطبيق. • تحذير. لم يتم تحديث خادم الإدارة منذ أكثر من يوم. • حرج. لم يتم تحديث خادم الإدارة منذ أكثر من يومين. • جيد. ولا واحد مما سبق.	1.3.6.1.4.1.23668.1093.1.2.1.	} INTEGER جيد (0) ، معلومات (1) ، تحذير (2) ، حرج (3) }	updatesStatus
هذا السبب يظهر أنه لم يتم تحديث خادم الإدارة لفترة طويلة. كمية الوقت التي تعتبر طويلة يتم تحديدها في .updatesStatus	1.3.6.1.4.1.23668.1093.1.2.2.1.	} INTEGER معطل (0) ، مفعّل (1) }	serverNotUpdated
هذا السبب يظهر أنه لم يتم تحديث بعض الأجهزة لفترة طويلة (7 أيام أو أكثر للحالات	1.3.6.1.4.1.23668.1093.1.2.2.2.	} INTEGER معطل (0) ،	notUpdatedHosts

حرج و3 أيام لحالات تحذير). يمكنك معرفة عدد تلك الأجهزة عبر .hostsNotUpdated		{ مفعّل (1)	
آخر مرة تم فيها تحديث قواعد مكافحة الفيروسات على خادم الإدارة.	1.3.6.1.4.1.23668.1093.1.2.3.	سلسلة ثمانية	lastServerUpdateTime
عدد الأجهزة التي تحتوي على قواعد مكافحة الفيروسات غير المحدثة.	1.3.6.1.4.1.23668.1093.1.2.4.	Counter32	hostsNotUpdated
حالة الحماية في الوقت الحقيقي. واحد مما يلي: <ul style="list-style-type: none"> تحذير. واحد مما يلي: تم الكشف عن وجود اختراق أمني على جهاز ينتمي إلى مجموعة خادم الإدارة. أخطاء التشفير جعلت بعض الأجهزة تغيّر 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. 	1.3.6.1.4.1.23668.1093.1.3.1.	} INTEGER جيد (0)، تحذير (1)، حرج (2) {	protectionStatus
يوضح هذا السبب أن تطبيق الأمان لا يعمل على بعض الأجهزة. يمكنك معرفة عدد تلك الأجهزة عبر .hostsAntivirusNotRunning	1.3.6.1.4.1.23668.1093.1.3.2.1.	} INTEGER معطل (0)، مفعّل (1) {	antivirusNotRunning
يوضح هذا السبب أن الحماية في الوقت الحقيقي لا تعمل على بعض الأجهزة. يمكنك معرفة عدد تلك الأجهزة عبر .hostsRealtimeNotRunning	1.3.6.1.4.1.23668.1093.1.3.2.2.	} INTEGER معطل (0)، مفعّل (1) {	realtimeNotRunning
يوضح هذا السبب أنه يوجد أجهزة تحتوي على كائنات لم يتم تنظيفها. يمكنك معرفة عدد تلك الأجهزة عبر .hostsNotCuredObject	1.3.6.1.4.1.23668.1093.1.3.2.4.	} INTEGER معطل (0)، مفعّل (1) {	notCuredFound
يوضح هذا السبب أنه تم العثور على تهديدات على بعض الأجهزة. يمكنك معرفة عدد تلك الأجهزة عبر .hostsTooManyThreats	1.3.6.1.4.1.23668.1093.1.3.2.5.	} INTEGER معطل (0)، مفعّل (1) {	tooManyThreats
يوضح هذا السبب 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.	1.3.6.1.4.1.23668.1093.1.3.2.6.	} INTEGER معطل (0)، مفعّل (1) {	virusOutbreak
عدد الأجهزة التي لا تعمل عليها تطبيقات الأمان.	1.3.6.1.4.1.23668.1093.1.3.3.	Counter32	hostsAntivirusNotRunning
عدد الأجهزة التي لا تعمل عليها الحماية في الوقت الحقيقي.	1.3.6.1.4.1.23668.1093.1.3.4.	Counter32	hostsRealtimeNotRunning
عدد الأجهزة المزودة بمستوى غير مقبول من الحماية في الوقت الحقيقي.	1.3.6.1.4.1.23668.1093.1.3.5.	Counter32	hostsRealtimeLevelChanged

عدد الأجهزة التي تحتوي على كائنات لم يتم تنظيفها.	1.3.6.1.4.1.23668.1093.1.3.6.	Counter32	hostsNotCuredObject
عدد الأجهزة التي تحتوي على تهديدات.	1.3.6.1.4.1.23668.1093.1.3.7.	Counter32	hostsTooManyThreats
حالة الفحص الكامل لتطبيق مكافحة الفيروسات. واحد مما يلي: <ul style="list-style-type: none"> • 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. 	1.3.6.1.4.1.23668.1093.1.4.1.	} INTEGER جيد (0) ، معلومات (1) ، تحذير (2) ، حرج (3) {	fullscanStatus
يوضح هذا السبب أنه لم يتم فحص بعض الأجهزة لفترة زمنية معينة. يمكنك معرفة عدد تلك الأجهزة عبر hostsNotScannedLately .كمية الوقت يتم تحديدها في .fullScanStatus .	1.3.6.1.4.1.23668.1093.1.4.2.1.	} INTEGER معطل (0) ، مفعل (1) {	notScannedLately
عدد الأجهزة التي لم يتم فحصها لفترة زمنية معينة. كمية الوقت يتم تحديدها في .fullScanStatus .	1.3.6.1.4.1.23668.1093.1.4.3.	Counter32	hostsNotScannedLately
حالة الشبكة المنطقية لخادم الإدارة. واحد مما يلي: <ul style="list-style-type: none"> • 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 فقدتها خادم الإدارة، أو إذا كان هناك أجهزة في حالة حرجة ولا يمكن الوصول إليها. • جيد. ولا واحد مما سبق. 	1.3.6.1.4.1.23668.1093.1.5.1.	} INTEGER جيد (0) ، تحذير (1) ، حرج (2) {	logicalNetworkStatus
يوضح هذا السبب أن بعض الأجهزة لم يتم توصيلها بخادم الإدارة لفترة طويلة (7 أيام أو أكثر لجهاز بحالة تحذير و4 أيام لجهاز بحالة حرجة). يمكنك معرفة عدد تلك الأجهزة عبر hostsNotConnectedLongTime .	1.3.6.1.4.1.23668.1093.1.5.2.1.	} INTEGER معطل (0) ، مفعل (1) {	notConnectedLongTime
يوضح هذا السبب أن هناك أجهزة فقدت خادم الإدارة التحكم فيها. يمكنك معرفة عدد تلك الأجهزة عبر .hostsControlLost .	1.3.6.1.4.1.23668.1093.1.5.2.2.	} INTEGER معطل (0) ، مفعل (1) {	controlLost
عدد الأجهزة التي وجدها خادم الإدارة والتي لا تنتمي إلى أي مجموعات خادم إدارة.	1.3.6.1.4.1.23668.1093.1.5.3.	Counter32	hostsFound
عدد المجموعات داخل خادم الإدارة.	1.3.6.1.4.1.23668.1093.1.5.4.	Counter32	groupsCount

عدد الأجهزة التي لم يتم توصيلها بخادم الإدارة لفترة طويلة. كمية الوقت التي تعتبر طويلة يتم تحديدها في <code>.notConnectedLongTime</code> .	1.3.6.1.4.1.23668.1093.1.5.5.	Counter32	hostsNotConnectedLongTime
عدد الأجهزة التي لا يتحكم فيها خادم الإدارة.	1.3.6.1.4.1.23668.1093.1.5.6.	Counter32	hostsControlLost
حالة النظام الفرعي للأحداث. واحد مما يلي: <ul style="list-style-type: none"> • 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 ذو أهمية "حرجة" على جهاز واحد على الأقل. يوجد حدث ذو أهمية "خطأ" على جهاز واحد على الأقل. يوجد حدث لمهمة 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. • جيد. ولا واحد مما سبق. 	1.3.6.1.4.1.23668.1093.1.6.1. } INTEGER جيد (0) ، تحذير (1) ، حرج (2) {	eventsStatus	
يوضح سبب <code>eventsStatus</code> أن هناك بعض الأحداث الحرجة على خادم الإدارة. يمكنك معرفة عدد تلك الأجهزة عبر <code>criticalEventsCount</code> تساوي القيمة 1 إذا كان هناك حدث حرج واحد على الأقل على أي جهاز، و 0 بخلاف ذلك.	1.3.6.1.4.1.23668.1093.1.6.2.1.	} INTEGER معطل (0) ، مفعّل (1) {	criticalEventOccured
عدد الأحداث الحرجة على خادم الإدارة.	1.3.6.1.4.1.23668.1093.1.6.3.	Counter32	criticalEventsCount

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 دعم SNMP في Windows. دعم SNMP معطل افتراضياً.

للسماح بدعم SNMP في نظام التشغيل Windows 10:

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 UPD قياسي.

يُسمح بدعم SNMP في نظام التشغيل Windows 10.

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 127.0.0.1 loopback.

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 86 بت:

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug]

• لأنظمة 64 بت:

Y_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug]

TraceLevel"=dword:00000004"

"\\:TraceDir"="C"

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.

حول العمل في بيئة السحابة

لا يعمل Kaspersky Security Center 14 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). مثل Amazon EC2 هو جهاز ظاهري يتم إنشاؤه على أساس منصة Amazon Web Services (AWS). يستخدم Kaspersky Security Center AWSAPI (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 مثل 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 مثل 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 استخدام [معالج تكوين بيئة السحابة](#) لتكوين Kaspersky Security Center، مع مراعاة خصائص العمل في بيئة السحابة.

سيناريو: النشر لسيناريو بيئة السحابة

يوضح هذا القسم نشر Kaspersky Security Center للعمل في بيئات السحابة مثل Amazon Web Services و Microsoft Azure و Google Cloud.

بعد الانتهاء من سيناريو النشر، سيتم بدء تشغيل [خادم إدارة Kaspersky Security Center](#) ووحدة تحكم الإدارة وتكوينهما باستخدام المعلمات الافتراضية. سيتم نشر الحماية ضد 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 تحضير

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 تنفيذ كل الإجراءات التي يقوم بها المعالج.

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 على Google Cloud** (يرجى 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 مثل 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 (يرجى 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. يمكن إكمال هذه المرحلة في معالج تكوين بيئة السحابة.

هذه المرحلة مطلوبة إذا كنت تستخدم Kaspersky Security Center المثبت من صورة AMI المجانية الجاهزة للاستخدام بناءً على نموذج BYOL، أو إذا كنت تثبت 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 التحويل 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. يمكن إكمال هذه المرحلة في معالج تكوين 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 المكتشفة 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 الاستقصاء 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، وتثبيت 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 تشغيل معالج تكوين بيئة السحابة. كما يمكنك إنشاء المهمة يدويًا. تقوم هذه المهمة باكتشاف تحديثات التطبيق المطلوبة وتنزيلها للتثبيت التالي لأجهزة الشبكة باستخدام أدوات Kaspersky Security Center.

يوصى بإكمال المراحل التالية بعد انتهاء معالج تكوين بيئة السحابة:

16 تكوين إدارة التقارير

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 14 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

لنشر 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:

• AML 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 لنظام التشغيل Linux و Kaspersky 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 100000 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 الأولى، سيطالبك Kaspersky Security Center برمز التنشيط أو ملف المفاتيح.

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.

قد تواجه خطأ ما عند محاولة تنشيط ميزة دعم البيئة السحابية باستخدام ترخيص Kaspersky Hybrid Cloud Security.

عند الاشتراك في Kaspersky Security Center، ستحصل على مثل Amazon EC2 (Amazon Elastic Compute Cloud) أو جهاز افتراضي في Microsoft Azure مزود بخادم إدارة Kaspersky Security Center. تتوفر حزم التثبيت لـ Kaspersky Security for Windows Server و Kaspersky Endpoint Security لنظام التشغيل 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 لخدام الإدارة لفترة تزيد عن أسبوع، فسيتحول التطبيق (Kaspersky Security for Windows Server أو Kaspersky Endpoint Security لنظام التشغيل Linux) إلى وضع الوظائف المحدودة. لتفعيل التطبيق مرة أخرى، يجب أن تجعل الجهاز المثبت عليه التطبيق مرئيًا لخدام 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 بخدام 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 كافيًا 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 بخدام 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 [Amazon Web Services](#).

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 ل خادم الإدارة. تشمل هذه الإجراءات العمل مع أدوار الهوية وإدارة الوصول (IAM) وحسابات المستخدمين. ويصف كذلك الإجراءات الواجب اتخاذها على الأجهزة العملية لتنصيب عميل الشبكة عليهم ثم تثبيت Kaspersky Security for Windows Server و Kaspersky Endpoint Security for Linux.

التأكد من أن خادم إدارة Kaspersky Security Center لديه الأذونات للعمل مع خدمات AWS

تحديد معايير التشغيل في بيئة سحابة Amazon Web Services أنه ينبغي تعيين [دور IAM خاص](#) لممثل خادم الإدارة للعمل باستخدام خدمات AWS. دور IAM هو كيان IAM يحدد مجموعة الأذونات الخاصة بتنفيذ الطلبات لخدمات AWS. يقدم دور IAM أذونات لاستقضاء قطاع السحابة وتنصيب 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.
- التخطيط 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 مزود 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 لخدم الإدارة

قبل قيامك بنشر خادم الإدارة، في وحدة التحكم الخاصة بإدارة AWS، قم بإنشاء دور IAM يحتوي على الأذونات المطلوبة لتنصيب التطبيقات على المثيلات. لمزيد من التفاصيل، راجع أقسام مساعدة AWS حول أدوار IAM.

لإنشاء دور IAM لخدم 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 لتنصيب التطبيقات على مثيلات EC2 باستخدام AWS API.

• **AmazonSSMFullAccess** و **AmazonEC2ReadOnlyAccess**، في حال كنت تخطط لتشغيل استقصاء قطاع السحابة وتنصيب 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 تنصيب 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 وتنصيب 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:

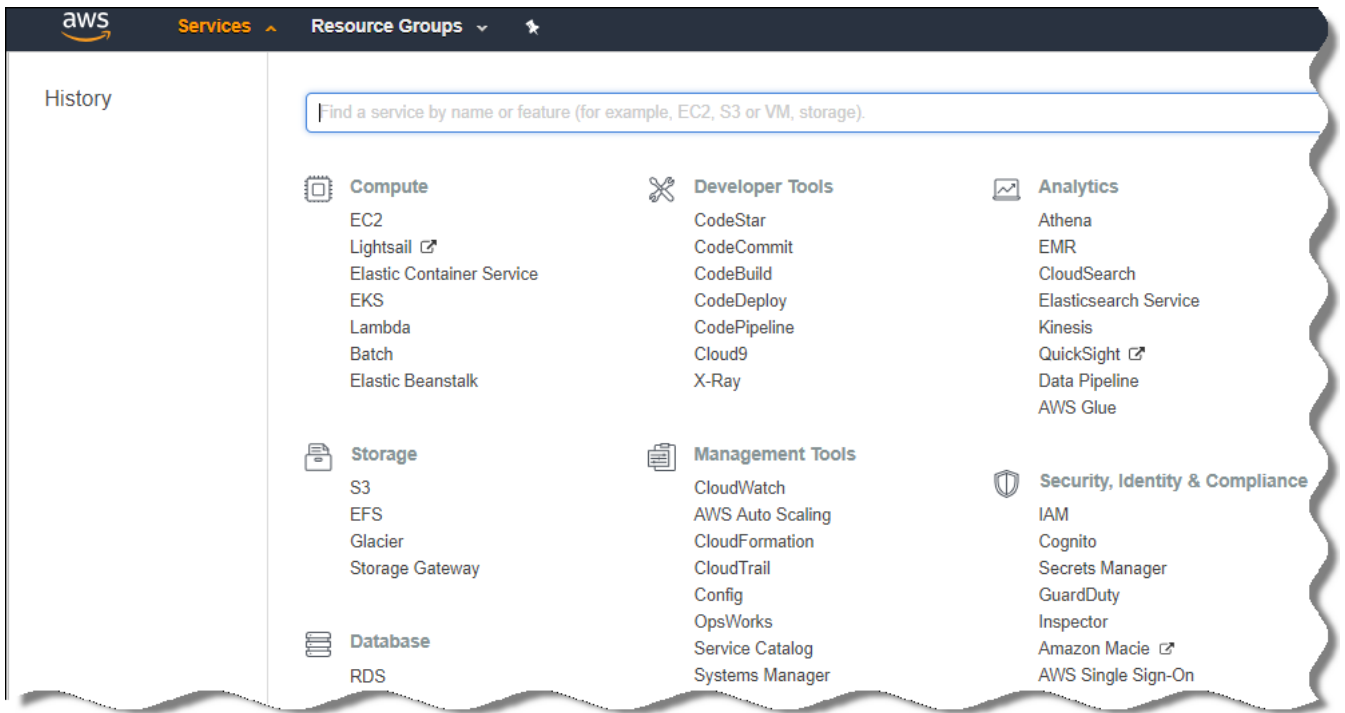
• <http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

• 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 حديثاً 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 اعتباراً 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](#) 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 المثل 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 حديثاً لإنشاء مثيلات EC2 جديدة تنوي حمايتها باستخدام Kaspersky Security Center، بالإضافة إلى ربطها بالمثيلات الحالية.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتباراً من تاريخ إصدار Kaspersky Security Center.

استخدام Amazon RDS

يصف هذا القسم أي الإجراءات يجب اتخاذها لإعداد قاعدة بيانات لـ Amazon 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

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 الأمان: 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، فاضغط 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 المثل، يمكنك استخدامه للعمل مع بيانات Kaspersky Security Center.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

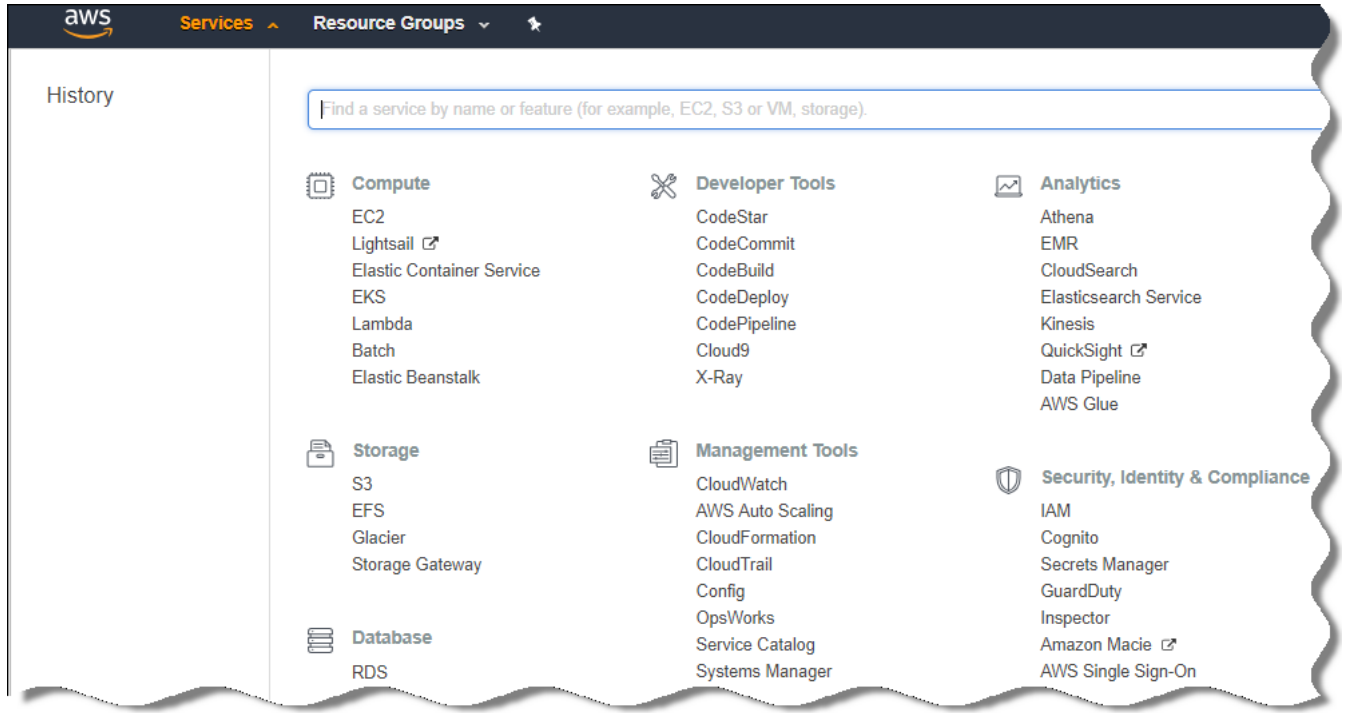
إنشاء مجموعة خيارات لمثيل Amazon RDS

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>) وأنت قممت 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 الاختبارات هذه.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتبارًا من تاريخ إصدار Kaspersky Security Center.

تعديل مجموعة الخيارات

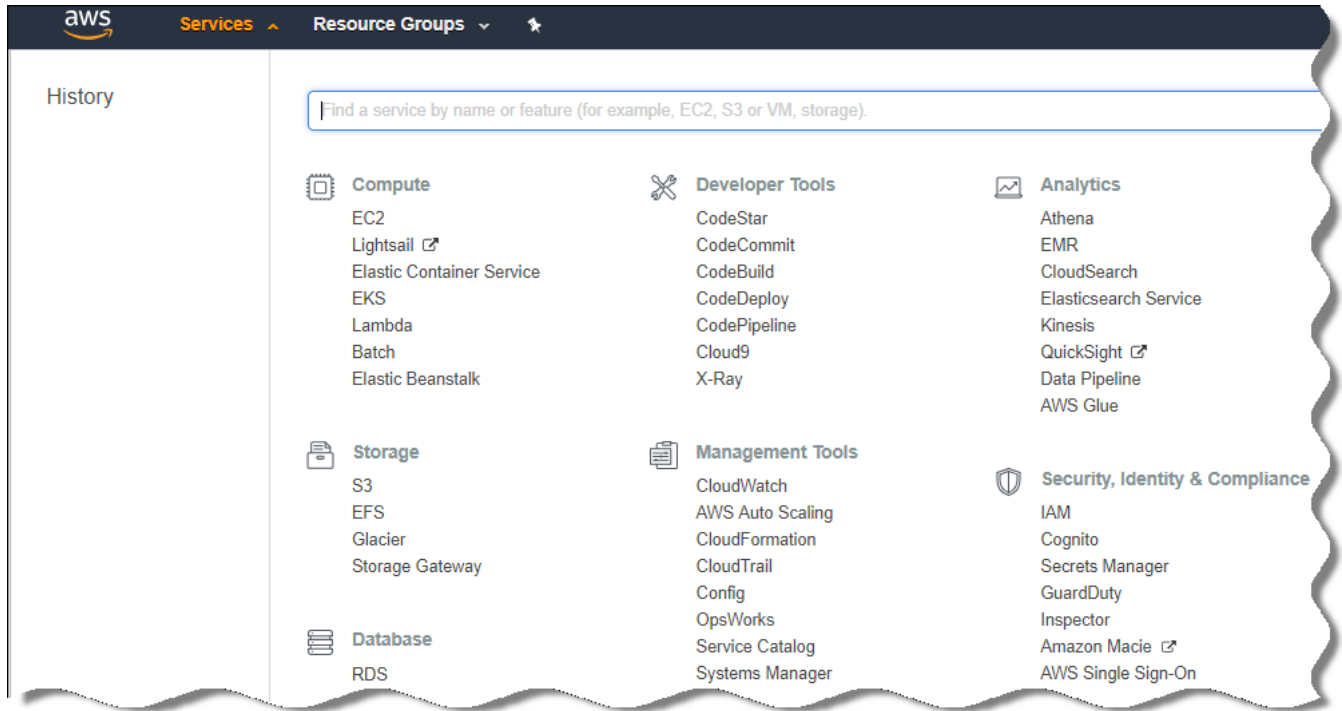
لا يعد التكوين الافتراضي لمجموعة الخيارات التي وضعت فيها مثيل Amazon RDS كافيًا للعمل بقاعدة بيانات Kaspersky Security Center. يجب عليك إضافة خيارات إلى مجموعة الخيارات وإنشاء دور IAM جديد للعمل مع قاعدة البيانات.

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 مثل 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 اقتراضية من الأدونات. وفي وقت لاحق، سوف يتعين عليك **تغيير الأدونات الخاصة به**.

7. قم بأحد الإجراءات التالية في قسم مستودع S3:

• إذا لم تقم بإنشاء مثل مستودع خدمة Amazon S3 لنسخ البيانات احتياطيًا، فحدد الارتباط **إنشاء مستودع S3 جديد** و**قم بإنشاء مستودع S3 جديد** باستخدام واجهة **AWS**.

• إذا كنت قد قمت بالفعل بإنشاء مثل 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 الأدونات لدور IAM لمثيل قاعدة بيانات Amazon RDS

بعد [إضافة خيارات إلى مجموعة الخيارات](#)، يجب عليك تعيين الأدونات المطلوبة لدور IAM الذي قمت بإنشائه للعمل مع مثيل قاعدة بيانات Amazon RDS.

قم بما يلي لتعيين الأدونات 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) (<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 `sqlNativeBackup-<date>`.
 6. باستخدام واجهة AWS، قم بإرفاق سياسة `AmazonS3FullAccess` بالدور.
- يتم تعيين الأدونات 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 [صفحات تعليمات Amazon S3](#). 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 من أن [وحدة التحكم الخاصة بإدارة AWS](#) مفتوحة وأنك قمت بتسجيل 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 متواجداً 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](#).

ترحيل قاعدة البيانات إلى Amazon RDS

يمكنك ترحيل قاعدة بيانات Kaspersky Security Center الخاصة بك من جهاز موجود في مكان العمل إلى مثل خدمة Amazon S3 الذي يدعم Amazon RDS. لإجراء ذلك، تحتاج إلى [مستودع S3](#) لقاعدة بيانات RDS وحساب مستخدم IAM مزود بإذن [AmazonS3FullAccess](#) لمستودع S3 هذا.

قم بما يلي لتنفيذ عملية ترحيل قاعدة البيانات هذه:

1. تأكد من قيامك بإنشاء مثل RDS (يرجى 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 مثل EC2 المثبت عليه خادم الإدارة.

تأكد من وجود مساحة قرص كافية على مثل EC2 المثبت عليه خادم الإدارة. في بيئة AWS، يمكنك إضافة مساحة قرص إلى المثل 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 الاستعادة والنسخ الاحتياطي.
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، املاً 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 قيامك بنشر خادم الإدارة، قم بإنشاء معرف تطبيق Azure مجهز بالأذونات المطلوبة لتثبيت التطبيقات على الأجهزة الظاهرية.

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 إجراء عملية النشر، يمكنك بدء وحدة تحكم الإدارة والاتصال بخادم الإدارة لبدء العمل مع 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، فيمكنك العمل مع خادم الإدارة كما لو كان خادم الإدارة مثبتًا على جهاز مادي. 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 مالكة إمكانية الوصول إلى Microsoft Azure Platform Management Portal وإلى خدمات Microsoft Azure. يمكن للمالك استخدام Microsoft Azure Platform لإدارة الخدمات مثل Azure SQL و Azure Storage.

لإنشاء اشتراك Microsoft Azure،

انتقل إلى <https://account.windowsazure.com/Subscriptions> واتبع التعليمات 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 تسجيل الدخول.

2. اتبع التعليمات على [صفحة المراجع](#)، لإنشاء معرف التطبيق الخاص بك.

3. انتقل إلى القسم [مفاتيح](#) في إعدادات التطبيق.

4. في القسم [مفاتيح](#)، املا الحقول الوصف وانتهاء الصلاحية و اترك 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/j4XVyJCvcpPHk2M/UYJ+QlFvdu). 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 لاحقاً عرض كلمة المرور بعد الآن ولن تتمكن من استعادتها.

عناوين صفحات الويب المذكورة في هذا المستند صحيحة اعتباراً من تاريخ إصدار Kaspersky Security Center.

تعيين دور لمعرفة 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 أيضاً 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 لمعرفة 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 وتطبيقاتي أمان لحماية المثيلات: Kaspersky Endpoint Security for Linux و Kaspersky Security for Windows Server.

5. في قائمة النتائج، حدد Kaspersky Hybrid Cloud Security (BYOL أو Kaspersky Hybrid Cloud Security). 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 واحداً مما يلي، وفقاً لخطة:

- محلي—إذا كنت تريد قاعدة بيانات على نفس الجهاز الظاهري حيث سيتم نشر خادم الإدارة. يأتي Kaspersky Security Center مجهزاً 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 استخدام 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 [بوابة 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. املا 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 و خادم SQL Server

تحتاج إلى قاعدة بيانات SQL و خادم SQL Server في بيئة Azure.

قم بما يلي لإنشاء قاعدة بيانات Azure SQL و خادم 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 بدلاً من إنشاء واحد جديد.

2. بعد إنشاء قاعدة بيانات SQL و خادم SQL Server، تأكد من أنك تعرف اسم المورد ومجموعة الموارد الخاصة به:

a. انتقل إلى <https://portal.azure.com> وتأكد من تسجيل 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 و SQLSysCLRTypes 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 و SQLSysCLRTypes لديك على خادم الإدارة الخاص بك.

يمكنك تنزيل [إطار عمل تطبيق DacFx \(17.0.1 Microsoft SQL Server Data-Tier\)](#) 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 الاستعادة والنسخ الاحتياطي.

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، املاً 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 (المفتاح 1 أو المفتاح 2).

• **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 أولاً 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 للعمليات 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 للعمليات](#)

البريد الإلكتروني للعمليات 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، و عميل 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):
- HTTPS 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 المعارف](#). تشمل الأمثلة على التكوينات غير الافتراضية على عدم تثبيت وحدة تحكم الإدارة على جهاز خادم الإدارة ولكن تثبيتها بدلاً 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 لمعالج تكوين بيئة السحابة

معالج تكوين بيئة السحابة في Kaspersky Security Center متوفر إذا كان لديك حزم التثبيت ومكونات الإدارة الإضافية الخاصة بالبرامج التالية:

• Kaspersky Security for Windows Server

• Kaspersky Endpoint Security for Linux

حزم التثبيت هذه مطلوبة لتثبيت كلٍ من Kaspersky Security for Windows Server و Kaspersky Endpoint Security for Linux على المثيلات أو الأجهزة الظاهرية التي ترغب في حمايتها. إذا لم يكن لديك حزم التثبيت هذه، يجب عليك إنشائها. بخلاف ذلك لا يمكن أن يعمل المعالج.

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: <file name>\<folder> ثم انقر على **التالي**.

8. اقرأ اتفاقية ترخيص المستخدم النهائي وحدد خانة الاختيار مؤكداً على قبولك لشروطها، ثم انقر على **التالي**.

سيتم رفع حزمة التثبيت إلى خادم الإدارة، وستتوفر في قائمة حزم التثبيت.

سيتم معالج تكوين بيئة السحابة بمجرد أن تنشئ حزم التثبيت وتقوم بتثبيت مكونات الإدارة الإضافية لتطبيقات Kaspersky Security for Windows Server و Kaspersky Endpoint Security for Linux على خادم الإدارة.

معالج تكوين بيئة السحابة

لتكوين Kaspersky Security Center باستخدام هذا المعالج، 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، والاشترك** (للعمل في بيئة السحابة - Microsoft Azure)

• البريد الإلكتروني لعمل Google ومعرف المشروع والمفتاح الخاص (لعمل مع Google Cloud)

إذا كنت لا ترغب في استخدام إمكانيات بيئة السحابة (إذا كنت ترغب، على سبيل المثال، في إدارة حماية الأجهزة العملية الفعلية فقط)، فيمكنك إغلاق معالج تكوين بيئة السحابة وتشغيل [معالج البدء السريع لخادم الإدارة](#) يدويًا.

سيبدأ تشغيل معالج 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. يمكنك 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 **All Tasks** ← **معالج تكوين بيئة السحابة**.

ويستمر متوسط جلسة العمل مع هذا المعالج حوالي 15 دقيقة.

حول معالج تكوين بيئة السحابة

يسمح لك هذا المعالج بتكوين Kaspersky Security Center مع أخذ متطلبات العمل في بيئة السحابة في الاعتبار.

يقوم المعالج بإنشاء الكائنات التالية:

• سياسة عميل الشبكة مع الإعدادات الافتراضية.

• السياسة لـ Kaspersky Endpoint Security for Linux

• السياسة لـ 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 و Windows

• مهام لكل جهاز مدار:

• فحص سريع للبحث عن الفيروسات

• تنزيل التحديث

إذا حددت خيار ترخيص BYOL، فسيقوم المعالج أيضًا بنشيط Kaspersky Security Center باستخدام ملف مفتاح أو رمز تنشيط ويضع المفتاح أو رمز التنشيط 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 - Kaspersky Security Center، سيطلبك المعالج بتحديد طريقة تفعيل التطبيق.

تفعيل التطبيق باستخدام رمز التنشيط (أو ملف مفتاح) - Kaspersky Security for Virtualization أو - 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 المثل 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 لوحة احتفاظ بمخزون تتم المحاسبة عليها شهرياً 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 AWS: Kaspersky Security Center أو Azure.

الخطوة 3. التحويل 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 حرفاً. 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.

حدد هذا الخيار إذا كان لديك حساب مستخدم IAM لديه الأذونات المطلوبة ويمكنك إدخال معرف مفتاح والمفتاح السري.

• [معرف مفتاح الوصول](#) ④

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 للتحويل بدلاً من دور IAM.

• [المفتاح السري](#) ④

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 للتحويل بدلاً من دور IAM.

يتم حفظ الاتصال في إعدادات التطبيق. يسمح لك معالج تكوين بيئة السحابة بإنشاء مفتاح وصول AWS IAM واحد فقط. 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 بحسابه 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](#) ④

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفاً. 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](#) ④

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 أولاً بحذف اتصال Azure الموجود.

• [معرف اشتراك Azure](#) ④

لقد قمت بإنشاء الاشتراك على مدخل Azure.

• [كلمة مرور تطبيق Azure](#) ④

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 ④

لقد قمت بإنشاء اسم حساب تخزين Azure لاستخدام Kaspersky Security Center.

• مفتاح وصول تخزين Azure ④

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 ④

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 ④

البريد الإلكتروني للعميل هو عنوان البريد الإلكتروني الذي استخدمته لتسجيل مشروعك في Google Cloud.

• معرف المشروع ④

معرف المشروع هو المعرف الذي استلمته عند تسجيل مشروعك في Google Cloud.

• مفتاح خاص ④

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** ورفضها. 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، فسيقوم المعالج بإنشاء مهمة لتثبيت تطبيقات أمان 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 أدوات لتثبيت التطبيقات على مثيلات EC2 أو على الأجهزة الظاهرية لـ Azure، يمكنك تكوين مهمة **التثبيت عن بُعد** يوميًا وتحديد حساب يمتلك الأدوات 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 يوميًا 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 العملية 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 العملية. وستستخدم 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. رقم المنفذ الافتراضي هو 25.

• [استخدام مصادقة ESMTP](#)

تمكين دعم مصادقة ESMTP. عند تحديد خانة الاختيار الموجودة في الحقول اسم المستخدم وكلمة المرور، يمكنك تحديد إعدادات مصادقة ESMTP بشكل افتراضي، يتم إلغاء تحديد هذه الخانة، وتكون إعدادات مصادقة ESMTP غير متوفرة.

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 لخدم 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 إنشاء 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 إنشاء 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 للتحويل 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 لخدم 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 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 أولاً 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.

سيتم توفير 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 وقت 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 الإجراءات عندما يتعين إعادة تشغيل نظام التشغيل أثناء التثبيت (البيئة السحابية)

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.

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 14 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 قاعدة البيانات

• 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 14 على النحو الصحيح للعمل في بيئة السحابة.

مجموعة جهاز السحابة

يمكنك إدارة أجهزة السحابة من خلال دمجها في مجموعات. في مرحلة التكوين الأولى 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 حددت الخيار **مزامنة هيكل مجموعة الإدارة مع قطاع السحابة عند تكوين المزامنة**، فإن هيكل المجموعات الفرعية في مجموعة الإدارة هذه مطابق لهيكل قطاع السحابة الخاصة بك. (مع ذلك، في AWS، لا يتم تمثيل مناطق التوفر ومجموعات المواضع في الهيكل. في Microsoft Azure لا يتم تمثيل الشبكات الفرعية في الهيكل). يتم حذف المجموعات الفرعية الفارغة داخل المجموعة التي تم اكتشافها أثناء الاستقصاء تلقائيًا.

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 خانة الاختيار **التحرير متاح** في خصائص الإعدادات والسياسات 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، Azure API، و Google API. يستخدم Kaspersky Security Center هذه المعلومات لتحديث محتويات مجلد **الأجهزة غير المخصصة والأجهزة 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 للميل على Google** و **معرف مشروع Google** و **المفتاح 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**.

4. حدد اسم بيئة السحابة للاتصال الذي سيتم استخدامه لإجراء المزيد من الاستقصاءات على قطاع السحابة:

بيئة السحابة ⑤

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 ⑤

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفاً. 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 ⑤

حدد هذا الخيار إذا قمت بالفعل بإنشاء دور IAM لخدمة الإدارة ليستخدم خدمات AWS.

• استخدام حساب مستخدم AWS IAM ⑤

حدد هذا الخيار إذا كان لديك حساب مستخدم IAM لديه الأذونات المطلوبة ويمكنك إدخال معرف مفتاح والمفتاح السري.

• معرف مفتاح الوصول ⑤

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 للتحويل بدلاً من دور IAM.

• المفاتيح السري ⑤

المفتاح السري الذي تلقينته 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 للتحويل 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 ⑤

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفاً. 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 أولاً 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 متاحاً. 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 متاحاً 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 حرفاً. 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 و**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 اتصالات خاصة باستقصاء قطاع السحابة

إذا لم بعد 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 الاستقصاء تلقائيًا في غضون 5 دقائق بواسطة معالج 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:

- **البداء 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 6:00:00 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 6:00:00 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) و Kaspersky 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 14 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.
- يبدأ تشغيل معالج إضافة مهمة. 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 حقل معرف مفتاح الوصول والمفتاح السري.

إذا قمت بتحديد Azure، فقم بإدخال بيانات الاعتماد لحساب Azure الذي يمتلك حقوق تثبيت التطبيقات على الأجهزة المحددة، في حقل معرف اشتراك Azure وكلمة 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 ⑤

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 ⑤

بالنسبة للمثيلات التي تعمل بنظام 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.

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 المجلد المهام.

في Microsoft Azure، قد تؤدي عملية التثبيت عن بُعد لتطبيقات الأمان على جهاز ظاهري إلى حذف Custom Script Extension المثبت 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 وتفصيله 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 AWS API** أو **Azure** أو **Google Cloud**؛ إذا تعذر اكتشاف الجهاز باستخدام أدوات API، فسيتم عرض القيمة لا .

• **منطقة السحابة**.

- **Cloud VPC** (لأجهزة AWS و Google Cloud فقط).
 - **منطقة توفر السحابة** (لأجهزة AWS و Google 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 تشغيل معالج تكوين بيئة السحابة، سيتم إنشاء القاعدة مزمنة 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 الجزء 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.

• **تضمن 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 تفرع لاحق. يتم تمكين هذا الخيار افتراضيًا.

• إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثاً 9

إذا تم تمكين هذا الخيار، في حالة عدم اشتغال بنية مجموعة الأجهزة المُدارة/السحابية 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 المُدارة/السحابية. 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/السحابية، وسيتم نقل الأجهزة الموجودة في هذه الشبكة الفرعية إلى المجموعة الأجهزة المُدارة/السحابية. يتم تمكين هذا الخيار افتراضياً.

• حذف المجموعات الفرعية التي لم يتم العثور على تطابق لها في قطاعات السحابية 9

إذا تم تمكين هذا الخيار، فسيحذف التطبيق من مجموعة السحابية جميع المجموعات الفرعية التي لا تطابق أي من كائنات السحابية الموجودة. إذا تم تعطيل هذا الخيار، فسيتم الاحتفاظ بالمجموعات الفرعية التي لا تطابق أي من كائنات السحابية الموجودة. يتم تمكين هذا الخيار افتراضياً.

إذا قمت بتمكين الخيار **المزامنة باستخدام السحابية** عند تشغيل معالج تكوين بيئة السحابية، فيتم إنشاء قاعدة المزامنة باستخدام السحابية مع تحديد خانة الاختيار **إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثاً وحذف المجموعات الفرعية التي لم يتم العثور على تطابق لها في قطاعات السحابية**.

إذا لم يتم تمكين الخيار **المزامنة مع السحابية**، فسيتم إنشاء قاعدة المزامنة مع السحابية 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/السحابية مع بنية قطاعات السحابية، فقم بتمكين الخيارين **إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثاً وحذف المجموعات الفرعية التي لم يتم العثور على تطابق لها في قطاعات السحابية** 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 API أو Azure API أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة ولكن لا يمكن اكتشافه باستخدام API لسبب ما.
- دون قيمة. يتعذر تطبيق هذا المعيار.

7. 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/السحابية** مع بنية قطاعات السحابية الخاصة بك.

9. انقر على زر **موافق**.

يتم إعداد الخصائص وحفظها.

لتعطيل قاعدة المزامنة مع السحابية:

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 الجزء 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.

استخدام البرامج النصية للنشر لنشر تطبيقات الأمان

عند نشر برنامج Kaspersky Security Center في بيئة سحابية، يمكنك استخدام البرامج النصية للنشر لأتمتة نشر تطبيقات الأمان. تتوفر البرامج النصية لعمليات النشر الخاصة بـ Amazon Web Services و Microsoft Azure و Google Cloud كملفات ZIP في [صفحة دعم Kaspersky](#).

يمكنك نشر أحدث إصدارات Kaspersky Endpoint Security for Linux و Kaspersky Security for Windows Server باستخدام البرامج النصية للنشر فقط إذا كنت قد أنشأت بالفعل حزم تثبيت لهذه البرامج ومكونات الإدارة الإضافية لهذه البرامج. لنشر أحدث إصدارات تطبيقات الأمان باستخدام البرامج النصية للنشر، قم بإجراء ما يلي على خادم الإدارة في بيئة السحابة:

1. [شغل معالج تكوين بيئة السحابة](#).

2. اتبع التعليمات الواردة على <https://support.kaspersky.com/14713>.

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

يقدم 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 أيضاً 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 المُسمى Remote Desktop Connection.
- **إدارة الكمبيوتر** هو مكون Microsoft Windows قياسي.

لإضافة أداة مخصصة أو إلزالتها أو تحرير إعداداتها:

من قائمة سياق الجهاز العميل، حدد أدوات مخصصة ← تكوين أدوات مخصصة.

ستفتح نافذة أدوات مخصصة. في هذه النافذة، يمكنك إضافة أدوات مخصصة أو إلزالتها وتحرير إعداداتها باستخدام الأزرار **إضافة وتعديل وإزالة** (X).

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 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 لعمل 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. يمكنك تغيير عنوان IP لاحقاً 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 لإنشاء 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 الصراف 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 أيضاً 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: محلياً، باستخدام الأمر regedit من القائمة بدء ← تشغيل).

2. انتقل إلى الخلية التالية:

• لنظام 64 بت:

Y_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0\ServerFlags

• لنظام 32 بت:

HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0\ServerFlags

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 للفواصل 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 للفواصل 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 وأكثر 10 أجهزة يتم تشغيلها بشكل متكرر مزودة بقواعد مراقبة سلامة الملف/مراقبة نظام التكامل.

صيانة خادم الإدارة

تتيح لك صيانة خادم الإدارة خفض حجم قاعدة البيانات، وتحسين أداء التطبيق ومصادقته 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 بحثاً عن أخطاء.
- إعادة تنظيم فهرس قاعدة البيانات.
- تحديث إحصائيات قاعدة البيانات.
- تقليص قاعدة البيانات (إذا لزم الأمر).

لا تدعم مهمة صيانة خادم الإدارة خادم MariaDB. في حالة استخدام خادم DBMS هذا في شبكتك، فسيتعين على المسؤولين صيانة MariaDB بأنفسهم.

لإنشاء مهمة صيانة خادم الإدارة:

1. في شجرة وحدة التحكم، حدد الجزء الخاص بخادم الإدارة الذي تريد إنشاء مهمة صيانة خادم الإدارة له.

2. حدد مجلد المهام.

3. بالنقر فوق الزر مهمة جديدة في مساحة عمل المجلد المهام.

يبدأ تشغيل معالج إضافة مهمة.

4. في النافذة تحديد نوع المهمة الخاصة بالمعالج، حدد صيانة خادم الإدارة كنوع المهمة وانقر فوق التالي.

5. إذا كان يتعين عليك تقليص قاعدة بيانات خادم الإدارة أثناء الصيانة، فحدد خانة الاختيار **تقليص قاعدة البيانات** من النافذة إعدادات الخاصة بالمعالج.

6. اتبع بقية إرشادات المعالج.

يتم عرض المهمة التي تم إنشاؤها حديثاً في قائمة المهام في مساحة عمل المجلد المهام. يمكن تشغيل مهمة صيانة خادم الإدارة واحدة فقط لخادم إدارة واحد فقط. في حالة إنشاء مهمة صيانة خادم الإدارة بالفعل لخادم إدارة، فلا يمكن إنشاء مهمة صيانة خادم الإدارة جديدة.

نافذة طريقة إخطار المستخدم

في النافذة طريقة إخطار المستخدم، يمكنك تكوين إخطار المستخدم المتعلق بتثبيت الشهادة على الجهاز المحمول:

- إظهار الرابط في المعالج. إذا قمت بتحديد هذا الخيار، سيتم عرض رابط لحزمة التثبيت في الخطوة الأخيرة من معالج اتصال جهاز جديد.
- إرسال الرابط 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 وعبر رسالة SMS لعرض رسالة الإخطار وتحريرها، إذا لزم الأمر.

القسم عام

في هذا القسم يمكنك ضبط إعدادات ملف التعريف العامة للأجهزة المحمولة Exchange ActiveSync.

- **الاسم**

اسم ملف التعريف.

- **السماح بالأجهزة غير القابلة للتزويد**

إذا تم تمكين هذا الخيار، فسيسمح للأجهزة التي لا يمكنها الوصول إلى كافة إعدادات سياسة Exchange ActiveSync [بالاتصال بخادم الجهاز المحمول](#). باستخدام الاتصال، يمكنك [إدارة الأجهزة المحمولة Exchange ActiveSync](#). على سبيل المثال، يمكنك تعيين كلمات المرور أو تكوين إرسال رسائل البريد الإلكتروني أو عرض معلومات حول الأجهزة، مثل معرف الجهاز أو حالة السياسة.

إذا تم تعطيل هذا الخيار، فلا يمكنك الاتصال بخادم الأجهزة المحمولة وإدارة أجهزة Exchange ActiveSync المحمولة.

يتم تمكين هذا الخيار افتراضياً. يمكنك تعطيل هذا الخيار إذا كنت لا تريد إدارة أجهزة Exchange ActiveSync المحمولة وتلقي معلومات عنها.

• [معدل التحديث \(بالساعات\)](#)

إذا تم تمكين هذا الخيار، فسيقوم التطبيق بتحديث معلومات سياسة Exchange ActiveSync بمعدل تكرار محدد في حقل الإدخال.

إذا تم تعطيل هذا الخيار، فلن تكون معلومات سياسة Exchange ActiveSync محدثة.

يتم تمكين هذا الخيار، بشكل افتراضي ويكون الفاصل الزمني للتحديث ساعة واحدة.

نافذة تحديد الجهاز

اختر تحديداً من قائمة **تحديد الجهاز**. تحتوي القائمة على التحديدات الافتراضية 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 حديثاً. لا يمكن أن يحتوي اسم على أكثر من 100 حرف ولا يمكن أن يتضمن أي رموز خاصة (*\<>:|).).

قسم فئات التطبيق

في هذا القسم، يمكنك تكوين توزيع المعلومات حول فئات التطبيق على الأجهزة العملية.

[نقل البيانات بالكامل \(لـ Network Agents Service Pack 2 والإصدارات السابقة\)](#)

إذا تم اختيار هذا الخيار، فسيتم نقل كل البيانات إحدى فئات التطبيق إلى الأجهزة العملية بعد تعديل تلك الفئة. يتم استخدام الخيار الخاص بنقل البيانات مع عميل الشبكة حزمة الخدمة 2 أو الإصدارات السابقة.

[نقل البيانات المعدلة فقط \(لـ Network Agents Service Pack 2 والإصدارات الأحدث\)](#)

إذا تم تحديد هذا الخيار، عندما يتم تعديل إحدى فئات التطبيق، فسيتم فقط نقل البيانات المعدلة إلى الأجهزة العملية، وليس كل البيانات من تلك الفئة. يتم استخدام خيار نقل البيانات مع عميل الشبكة حزمة الخدمة 2 والإصدارات اللاحقة.

مميزات 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 المثبتة 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 المدارة 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 تحديثات الأحداث التي تم إنشاؤها تلقائيًا، وكذلك إنشاء تحديثات 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 الجهاز المحمول على المجلدات الفرعية التالية:
- **خوادم الأجهزة المحمولة.** مخصص لإدارة خوادم الأجهزة المحمولة التي تعمل بنظام iOS MDM وXoادم Microsoft Exchange Mobile Devices.
- **الأجهزة المحمولة.** مخصص لإدارة الأجهزة المحمولة وKES وExchange ActiveSync وiOS MDM.
- **الشهادات.** مخصص لإدارة شهادات الأجهزة المحمولة.
- **تحديثات 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 التحديثات المُعدة مسبقًا أو إنشاء اختيارك 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 المثبتة 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 المثبت عليها عميل الشبكة.
- **الملفات التنفيذية.** يحتوي على قائمة الملفات التنفيذية المُخزنة على أجهزة العميل المثبت عليها عميل الشبكة.
- **الثغرات الأمنية بالبرنامج.** يحتوي على قائمة الثغرات الأمنية في التطبيقات على الأجهزة المثبت 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 لقيود 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، ونطاقات IP، و Active Directory.
- **المستودعات.** هذا المجلد مخصص للعمليات باستخدام الكائنات المستخدمة 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 المضمنة في مجلد الخيارات المتقدمة. يمكن نقل المجلدات الفرعية الأكثر استخدامًا إلى مستوى أعلى من مجلد الخيارات المتقدمة. نادرًا ما يمكن نقل المجلدات الفرعية المستخدمة 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 الزر  في مساحة العمل.

كيفية التنقل في شجرة وحدة التحكم

للتنقل في شجرة وحدة التحكم، يمكنك استخدام أزرار شريط الأدوات التالية:

-  - خطوة إلى الخلف.
-  - خطوة 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 المفاتيح **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 الملف، 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 المطابقة (راجع الجدول الموجود بالأسفل).

عناصر قائمة سياق كائنات وحدة تحكم الإدارة

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 ← Large icons	لإظهار الكائنات الموجودة في مساحة العمل على شكل رموز كبيرة.
	عرض ← Small icons	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

الاتصال بخادم الإدارة	الاتصال بخادم الإدارة	إسم خادم الإدارة
للاتصال بخادم الإدارة.	قطع الاتصال عن خادم الإدارة	
لقطع الاتصال مع خادم الإدارة.	تثبيت التطبيق	الأجهزة المُدارة
لبدء تشغيل معالج التثبيت عن بُعد للتطبيق.	عرض ← تكوين الواجهة	
لتكوين عرض عناصر الواجهة.	إزالة	
لإزالة خادم الإدارة من شجرة وحدة التحكم.	تثبيت التطبيق	
لبدء تشغيل معالج التثبيت عن بُعد الخاص بمجموعة الإدارة.	إعادة تعيين عداد الفيروسات	
لإعادة تعيين عدادات الفيروسات الخاصة بالأجهزة المضمنة في مجموعة الإدارة.	عرض تقرير التهديدات	
إنشاء تقرير التهديدات ونشاط الفيروسات على الأجهزة المضمنة في مجموعة الإدارة.	New ← مجموعة	
لإنشاء مجموعة إدارة.	جميع المهام ← بنية مجموعة جديدة	
لإنشاء بنية لمجموعات الإدارة بناءً على بنية المجالات أو Active Directory.	All Tasks ← عرض الرسالة	
لبدء تشغيل معالج رسالة جديدة للمستخدم المعني بمستخدمي الأجهزة المضمنة في مجموعة الإدارة.	New ← خادم الإدارة الثانوي	الأجهزة المُدارة ← خوادم الإدارة
لبدء تشغيل معالج إضافة خادم إدارة ثانوي	New ← خادم الإدارة الافتراضي	
لبدء تشغيل معالج خادم إدارة افتراضي جديد.	جديد ← جهاز محمول	إدارة الجهاز المحمول ← الأجهزة المحمولة
لاتصال جهاز محمول جديد خاص بالمستخدم.	New ← الشهادة	إدارة الجهاز المحمول ← الشهادات
لإنشاء شهادة.	إنشاء ← جهاز محمول	
لاتصال جهاز محمول جديد خاص بالمستخدم.	New ← تحديد جديد	تحديدات الأجهزة
لإنشاء تحديد أجهزة.	جميع المهام ← استيراد	
لاستيراد تحديد من ملف.	إضافة ملف المفتاح أو رمز التنشيط	تراخيص Kaspersky
لإضافة مفتاح ترخيص إلى مستودع خادم الإدارة.	تفعيل التطبيق	
لبدء تشغيل معالج إنشاء مهمة تفعيل التطبيق.	تقرير حول استخدام المفاتيح	
لإنشاء تقرير حول مفاتيح الترخيص المستخدمة على الأجهزة العميلة وعرضه.	New ← الفئة	إدارة التطبيق ← فئات التطبيق
لإنشاء فئة تطبيق.	عامل التصفية	إدارة التطبيق ← سجل التطبيقات
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.	قبول اتفاقيات تراخيص التحديثات	إدارة التطبيق ← تحديثات البرنامج
لقبول اتفاقية ترخيص تحديثات البرامج.	New ← مجموعة التطبيقات المرخصة	إدارة التطبيق ← استخدام تراخيص الجهات الخارجية
لإنشاء مجموعة تطبيقات مرخصة.	عرض إصدارات التطبيق الحالية	التثبيت عن بُعد ← حزم التثبيت
لإظهار قائمة بالإصدارات الحديثة من تطبيقات Kaspersky المتوفرة على خوادم الويب.	New ← حزمة التثبيت	
لإنشاء حزمة تثبيت.	All Tasks ← تحديث قواعد البيانات	
لتحديث قواعد بيانات التطبيقات الموجودة في حزم التثبيت.		

لعرض قائمة الجزم المستقلة التي تم إنشاؤها لجزم التثبيت.	All Tasks ← عرض القائمة العامة للجزم المستقلة	
لإعداد استجابة خادم الإدارة لخمول الأجهزة المتصلة بالشبكة.	All Tasks ← نشاط الجهاز	اكتشاف الأجهزة ← المجالات
لإنشاء نطاق IP.	New ← نطاق IP	اكتشاف الأجهزة ← نطاقات IP
لفتح نافذة خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة.	تنزيل التحديثات	المستودعات ← تحديثات قواعد بيانات Kaspersky ووحدات البرامج النمطية
لتكوين مهمة تنزيل التحديثات إلى المستودع الخاصة بخادم الإدارة.	إعدادات تنزيل التحديثات	
لإنشاء تقرير حول إصدارات قواعد البيانات وعرضه.	تقرير عن استخدام قواعد بيانات مكافحة الفيروسات	
مسح مستودع تحديثات خادم الإدارة.	All Tasks ← مسح مستودع التحديثات	
لإنشاء جهاز جديد.	New ← الجهاز	المستودعات ← الأجهزة

قائمة بالأجهزة المُدارة. وصف الأعمدة

يعرض الجدول التالي أسماء وأوصاف ذات صلة بأعمدة في قائمة الأجهزة المُدارة.

أوصاف الأعمدة في قائمة الأجهزة المُدارة

القيمة	اسم العمود
اسم NetBIOS للجهاز العميل. يتم إعطاء أوصاف رموز أسماء الجهاز في الملحق .	الاسم
نوع نظام التشغيل المثبت على الجهاز العميل.	نوع نظام التشغيل
اسم مجال Windows الذي يقع فيه الكمبيوتر العميل.	مجال Windows
نتيجة تثبيت عميل الشبكة على الجهاز العميل (نعم، لا، غير معروف).	تم تثبيت عميل الشبكة
نتيجة تشغيل عميل الشبكة (نعم، لا، غير معروف).	عميل الشبكة قيد التشغيل
تم تثبيت تطبيق الأمان (نعم، لا، غير معروف).	الحماية في الوقت الحقيقي
الفترة الزمنية التي انقضت منذ أن تم توصيل الجهاز العميل بخادم الإدارة.	آخر اتصال بخادم الإدارة
الفترة الزمنية التي مرت منذ آخر تحديث للأجهزة المُدارة.	تاريخ آخر تحديث للحماية
الحالة الحالية للجهاز العميل (مقبول، حرج، تحذير).	الحالة
أسباب تغيير حالة الجهاز العميل إلى حرج أو تحذير. يتم تغيير حالة الجهاز العميل إلى تحذير أو حرج لوجود أحد الأسباب التالية: <ul style="list-style-type: none"> تطبيق الأمان غير مثبت. تم اكتشاف العديد من الفيروسات. 	وصف الحالة

• يختلف مستوى الحماية في الوقت الحقيقي عن المستوى الذي تم تعيينه من قبل المسؤول.

• لم يتم إجراء فحص الفيروسات منذ وقت طويل.

• قواعد البيانات قديمة.

• لم يتم الاتصال منذ فترة طويلة.

• تم اكتشاف تهديدات نشطة.

• إعادة التشغيل مطلوبة.

• 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 حوادث لم تتم معالجتها.

• حالة الجهاز المحددة بواسطة التطبيق.

• نفذت مساحة قرص الجهاز.

• ستنتهي فترة صلاحية الترخيص قريباً.

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 العملية 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 حرجاً 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 المقدم من التطبيق المدار.

الفترة الزمنية التي مرت منذ آخر مزامنة ناجحة للجهاز العميل مع خادم الإدارة (أي منذ آخر فحص للشبكة).

تاريخ آخر تحديث للمعلومات

اسم مجال DNS الخاص بالجهاز العميل؛

اسم DNS

لاحقة DNS الأساسية.

مجال DNS

عنوان IP الخاص بالجهاز العميل؛ ينصح باستخدام عنوان IPv4.

عنوان IP

الفترة الزمنية التي ظل خلالها الجهاز العميل مرئياً في الشبكة.

آخر وقت مرئي





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 المستخدم للاتصال بخادم إدارة Kaspersky Security Center.
إصدار عميل الشبكة	إصدار عميل الشبكة.
إصدار التطبيق	إصدار تطبيق الأمان المثبت على الجهاز العميل.
آخر ما خضع للتحديث من قواعد البيانات الخاصة بمكافحة الفيروسات	إصدار قواعد بيانات مكافحة الفيروسات
آخر تشغيل للنظام	وقت وتاريخ آخر تشغيل للجهاز العميل.
إعادة التشغيل المطلوبة	يلزم إعادة تشغيل الجهاز العميل.
نقطة توزيع	اسم الجهاز الذي يعمل بمثابة نقطة توزيع لهذا الجهاز العميل.
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 بالبيت	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، لا توجد بيانات من الجهاز)
حالة منع تسريب البيانات	حالة مكون منع تسريب البيانات (قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، لا توجد بيانات من الجهاز)
حالة الحماية الخاصة بتعاون الخوادم	حالة مكون تصفية المحتوى (قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، لا توجد بيانات من الجهاز)
حالة الحماية ضد	حالة مكون الحماية ضد الفيروسات لخادم البريد (قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، لا توجد بيانات من الجهاز)

الفيروسات الخاصة بخوادم البريد	حالة مكون أداة استشعار نقطة النهاية (قيد التشغيل، يجري البدء، متوقف، متوقف مؤقتًا، فشل، لا توجد بيانات من الجهاز)
حالة أداة استشعار نقطة النهاية	تم الإنشاء
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 <u>مجموعة الإدارة</u> 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: <ul style="list-style-type: none"> • 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 <u>تكوين البحث عن جميع أرقام النسخة</u> 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 <u>تكوين البحث عن جميع أرقام معرف الإصدار</u> 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، بالحالة تحذير.
	تضمين جهاز مثبت عليه نظام تشغيل لمحطات عمل في مجموعة إدارة، بالحالة حرج.

تضمين جهاز لمحطات العمل في مجموعة إدارة، فقدت اتصالها بخادم الإدارة.	
اكتشاف جهاز مثبت عليه نظام تشغيل لحواد في النظام وغير مضمن في أي من مجموعات الإدارة.	
تضمين جهاز مثبت عليه نظام تشغيل لحواد في مجموعة إدارة، بالحالة موافق.	
تضمين جهاز مثبت عليه نظام تشغيل لمحطات عمل في مجموعة إدارة، بالحالة تحذير.	
تضمين جهاز مثبت عليه نظام تشغيل لمحطات عمل في مجموعة إدارة، بالحالة حرج.	
تضمين جهاز بنظام تشغيل لحواد 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، بالحالة تحذير.	
تضمين جهاز محمول في مجموعة إدارة، بالحالة 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 الشبكة.	
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 الشبكة.	
تضمين جهاز حماية UEFI في مجموعة إدارة، بالحالة تحذير. يوجد جهاز حماية UEFI في الشبكة.	
تضمين جهاز حماية UEFI في مجموعة إدارة، بالحالة تحذير. جهاز حماية UEFI لا يوجد في الشبكة.	
تضمين جهاز حماية UEFI في مجموعة إدارة، بالحالة حرج. يوجد جهاز حماية UEFI في الشبكة.	
تضمين جهاز حماية UEFI في مجموعة إدارة، بالحالة حرج. جهاز حماية UEFI لا يوجد في الشبكة.	
السياسة المفعلة.	
السياسة غير المفعلة.	
سياسة نشطة موروثه من مجموعة تم إنشاؤها على خادم الإدارة الرئيسي.	
السياسة المفعلة الموروثه 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 محددة) بالحالة فشل.	
مهمة موروثه من مجموعة تم إنشاؤها على خادم الإدارة الرئيسي.	
مهمة موروثه 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 العملية. يتم عرض الأيقونات في مساحات عمل المجلدات العزل، والنسخ الاحتياطي، وتهديدات 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.
	الملف ذو الحالة تتم إضافتها من جانب المستخدم.
	الملف ذو الحالة اكتشافات إيجابية زائفة.
	الملف ذو الحالة تم التنظيف.
	الملف ذو الحالة 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 العملية في مجموعات الإدارة الخاصة بخادم الإدارة وخوادمه التابعة.
- الأجهزة غير المخصصة بواسطة خادم الإدارة وخوادمه التابعة.

للعثور على الأجهزة العملية 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 وخواص الإدارة الثانوية باستخدام قائمة منسدلة في الزاوية العلوية اليمنى من النافذة. لا تتوفر وظيفة البحث عن مجموعات الإدارة وخواص 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 والمورد والوصف

إعدادات البحث عن الجهاز

فيما يلي أوصاف الإعدادات المستخدمة للبحث عن الأجهزة المدارة. وتعرض نتائج البحث في الجزء السفلي من النافذة.

الشبكة

من علامة التبويب الشبكة، يمكنك تحديد المعايير التي ستستخدم للبحث عن الأجهزة وفقًا لبيانات الشبكة الخاصة بهم:

- [اسم الجهاز أو عنوان IP](#)

اسم الجهاز الموجود في شبكة Windows (اسم NetBIOS)

- [مجال Windows](#)

• [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 وظاهري، 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 المركبة 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 افتراضياً.

• مُدار بواسطة خادم إدارة مختلف ⑤

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 سابقاً إلى أوصاف الأجهزة المدارة:

• تطبيق في حالة مطابقة علامة محددة واحدة على الأقل ⑤

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 افتراضياً.

• يجب تضمين العلامة ⑤

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 افتراضياً.

• يجب استثناء العلامة ⑤

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 أيضاً 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

• تضمين وحدات تنظيمية تابعة

• هذا الجهاز عضو في مجموعة **Active Directory**

نشاط الشبكة

في علامة التبويب نشاط الشبكة، يمكنك تحديد المعايير التي ستستخدم للبحث عن الأجهزة وفقاً لنشاط الشبكة الخاص بهم:

• هذا الجهاز هو عبارة عن نقطة توزيع ④

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 ④

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

• مُمكن. 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 ④

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 ④

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 ④

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 افتراضياً.

• الجهاز مرئي ④

- في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختبار عند إجراء البحث:
- **نعم.** يشمل التطبيق في الاختيار الأجهزة المرئية في الوقت الحالي على الشبكة.
- **لا.** يشمل التطبيق في الاختيار 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 ستستخدم للبحث عن الأجهزة وفقاً 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 التحديث عند إجراء بحث باسم التطبيق أو برقم حزمة التحديث.
- إذا تم ترك الحقل فارغاً، 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 مدار بواسطة Kaspersky Security Center 14**

- 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 ⑨

- 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 ⑨

إذا تم تحديد خانة الاختبار، فيمكنك تحديد نظام تشغيل من القائمة. يتم تضمين الأجهزة المثبت عليها أنظمة التشغيل المحددة في نتائج البحث.

• حجم نظام التشغيل بالبت ⑨

في القائمة المنسدلة، يمكنك تحديد بنية نظام التشغيل والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز (غير معروف، AMD64، x86 أو IA64). وبشكل افتراضي، لا يتم تحديد أي خيار في القائمة ومن ثم لا يتم تحديد بنية نظام التشغيل.

• إصدار حزمة خدمة نظام التشغيل ⑨

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 ⑨

لا يكون هذا الإعداد قابلاً 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 أيضاً تكوين البحث عن جميع أرقام النسخة باستثناء الرقم المحدد.

• معرف تحرير نظام التشغيل ⑨

لا يكون هذا الإعداد قابلاً 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 أيضاً 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 خانة 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 افتراضياً.

• **آخر فحص**

إذا تم تمكين هذا الخيار، يمكنك البحث عن أجهزة العميل حسب وقت آخر فحص للفيروسات. في حقول الإدخال، يمكنك تحديد الفترة الزمنية التي تم فيها آخر فحص للفيروسات. يتم تعطيل هذا الخيار افتراضياً.

• **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 افتراضياً.

سجل التطبيقات

في علامة التبويب **سجل التطبيقات**، يمكنك تكوين البحث عن الأجهزة وفقاً 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 ⑤

يمكنك في حقل الإدخال تحديد إصدار التطبيق المحدد.

• المورد ⑤

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة لأي تطبيق مثبت على الجهاز.

• حالة التطبيق ⑤

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 ⑤

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 وإصدار التطبيق وحالة التطبيق إلى اسم التحديث وإصدار التحديث والحالة على التوالي. يتم تعطيل هذا الخيار افتراضياً.

• اسم تطبيق الأمان غير المتوافق ⑤

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 ⑤

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 خوادم الإدارة الثانوية (نزولاً 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 جزءاً من البنية الأساسية لسطح المكتب الافتراضي (VDI).

• هذا جهاز ظاهري ⑤

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- ليس هامًا.
- لا. البحث عن الأجهزة التي لا تعد أجهزة ظاهرية.
- نعم. البحث عن الأجهزة التي تعد أجهزة ظاهرية.

• نوع الجهاز الظاهري ⑤

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 ⑤

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 ⑤

يمكنك في القائمة المنسدلة تحديد نوع الوحدة. يتم تضمين جميع الأجهزة الموجودة بها هذه الوحدة في نتائج البحث. يدعم الحقل البحث بالنص الكامل.

• المورد ⑤

يمكنك في القائمة المنسدلة تحديد اسم الشركة المصنعة للوحدة. يتم تضمين جميع الأجهزة الموجودة بها هذه الوحدة في نتائج البحث. يدعم الحقل البحث بالنص الكامل.

• الوصف ⑤

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 ⑤

سيتم تضمين الأجهزة ذات رقم المخزون والمحدد في هذا الحقل في التحديد.

• [سرعة وحدة المعالجة المركزية \(CPU\) \(بالمجاهرتز\) ⑤](#)

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 ⑤](#)

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 ⑤](#)

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 ⑤](#)

نطاق القيم لحجم ذاكرة الوصول العشوائي للجهاز. سيتم تضمين الأجهزة التي تحتوي على ذاكرة الوصول العشوائي، والتي تطابق النطاق في حقوق الإدخال هذه (ضمنياً) 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 ⑤](#)

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، فستشتمل النتائج على الأجهزة التي تتلقى تحديثات من خلال Windows Update من مصادر أخرى.

المستخدمون

في علامة التبويب المستخدمين، يمكنك إعداد المعايير للبحث عن الأجهزة بحسب حسابات المستخدمين الذين قاموا بتسجيل الدخول إلى نظام التشغيل.

• [آخر مستخدم سجّل الدخول إلى النظام ⑤](#)

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 ⑤](#)

إذا تم تمكين هذا الخيار، فانقر فوق زر استعراض لتحديد حساب مستخدم. ستضمن 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 المُدارة:

• حالة منع تسريب البيانات

البحث عن الأجهزة حسب حالة منع تسرب البيانات (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

• حالة الحماية الخاصة بتعاون الخوادم

البحث عن الأجهزة حسب حالة حماية تعاون الخادم (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

• حالة الحماية ضد الفيروسات الخاصة بخوادم البريد

البحث عن الأجهزة حسب حالة حماية خادم البريد (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

• حالة أداة استشعار نقطة النهاية

البحث عن الأجهزة حسب حالة المكون أداة استشعار نقطة النهاية (لا توجد بيانات من الجهاز، 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: AES56 وAES128 وAES192 وAES256.

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 تشمل فقط على أجهزة من القطاع المحدد.

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 يمكن اكتشاف الجهاز باستخدام AWS API أو Azure API أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة ولكن لا يمكن اكتشافه باستخدام API لسبب ما.
- دون قيمة. يتعذر تطبيق هذا المعيار.

مكونات التطبيق

يحتوي هذا القسم على قائمة المكونات لهذه التطبيقات التي لديها مكونات إدارة إضافية مطابقة مثبتة في وحدة تحكم الإدارة.

في القسم **مكونات التطبيق**، يمكنك تحديد معايير لتضمين الأجهزة في تحديد وفقاً للحالات ولأرقام الإصدار المكونات التي تشير للتطبيق الذي حددته:

• **الحالة** ⑤

البحث عن الأجهزة وفقاً لحالة المكون المرسل بواسطة تطبيق إلى خادم الإدارة. يمكنك تحديد أحد الحالات التالية: لا بيانات من الجهاز، أو متوقف، أو بدء التشغيل، أو تم الإيقاف مؤقتاً، أو قيد التشغيل، أو اختلال تشغيل أو غير مثبت. إذا كان للمكون المحدد للتطبيق المثبت على جهاز مُدار حالة محددة، فإنه يتم تضمين الجهاز في تحديد الجهاز.

الحالات المرسل بواسطة التطبيقات:

- بدء تشغيل—يكون المكون في عملية التهيئة في الوقت الحالي.
- قيد التشغيل—يكون المكون ممكناً ويعمل على النحو الصحيح.
- تم الإيقاف مؤقتاً—تم تعليق المكون، على سبيل المثال، بعد إيقاف المستخدم للحماية مؤقتاً في التطبيق المُدار.
- اختلال التشغيل—حدث خطأ أثناء تشغيل المكون.
- متوقف—تم تعطيل المكون وهو لا يعمل في الوقت الحالي.
- غير مثبت—لم يتم 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** ⑤

البحث عن الأجهزة وفقاً 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 إصداراً مماثلاً أو إصداراً سابقاً أو إصداراً أحدث. يمكنك أيضاً 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: `[9-0]`—أي رقم. `[abcdef]`—أي رمز من الرموز 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 W?rd 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 `[9-0]` في حقل البحث. للبحث عن أحد الأحرف—a، أو b، أو c، أو d، أو e، أو f—أدخل التعبير `[abcdef]` في حقل البحث.

استخدم التعبيرات 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 "تابع" وكلمة "ظاهري"، يمكنك إدخال أي من التعبيرات التالية في حقل البحث: `+تابع+ظاهري`، و `تابع و ظاهري`، و `تابع` و `ظاهري`.
- OR أو `||`. عند وضعها بين كلمتين، فتشير إلى أن إحدى الكلمتين موجودة في النص. للبحث عن عبارة تحتوي على كلمة "تابع" أو كلمة "ظاهري"، يمكنك إدخال أحد التعبيرات التالية في حقل البحث: `تابع` أو `ظاهري` أو `تابع || ظاهري`.
- 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.
- `<some text>`. النص الموضوع بين علامتي الاقتباس يجب أن يكون موجودًا في النص. للبحث عن عبارة تجمع بين الكلمتين `Slave Server`، يجب أن تقوم بإدخال التعبير `"Slave 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

الإعدادات المحددة أثناء إنشاء المهمة

يمكنك تحديد الإعدادات التالية عند إنشاء مهمة. يمكن أيضاً تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

- إعدادات إعادة تشغيل نظام التشغيل:

• لا تقوم بإعادة تشغيل الجهاز ⁵

لم تتم إعادة تشغيل أجهزة العميل تلقائياً بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدوياً 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 أمراً بالغ الأهمية.

• أعد تشغيل الجهاز ⁵

يتم إعادة تشغيل الأجهزة العميلة تلقائياً دائماً 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 ⁵

سيتم عرض تنذير بإعادة التشغيل على شاشة الجهاز العميل، بحيث يطلب من المستخدم إعادة تشغيله يدوياً. يمكن تحديد بعض الإعدادات المتقدمة لهذا الخيار: نص الرسالة التي تظهر للمستخدم وتكرار عرض الرسالة والفواصل الزمنية الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضياً.

• تكرار المطالبة كل (بالدقائق) ⁵

إذا تم تمكين هذا الخيار، فسيطالب التطبيق المستخدم بإعادة تشغيل نظام التشغيل باستخدام التردد المحدد. يتم تمكين هذا الخيار افتراضياً. 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) ⁵

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد. يتم تمكين هذا الخيار افتراضياً. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

• فرض إغلاق التطبيقات في الجلسات المحظورة ④

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 المستخدم 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 يدوياً وإعادة تشغيل هذه الأجهزة. يتم تعطيل هذا الخيار افتراضياً.

• إعدادات جدولة المهام:

• البدء المُجدول ④

حدد الجدول الذي تعمل المهمة وفقاً له، وقم بتكوين الجدول المحدد.

• كل N ساعة ④

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• كل N يوماً ④

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 أسبوعاً ④

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 ④

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.

• يومياً (التوقيت الصيفي غير مدعوم) ④

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. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 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 تمكين 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، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• [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 المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• 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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تمكين 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 المترامنة 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 المترامنة 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 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.

• 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 حقل **الحساب وكلمة 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:

• التوزيع للمجموعات الفرعية 9

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 افتراضياً.

• توزيع إلى خوادم الإدارة الثانوية والافتراضية 9

عند تمكين هذا الخيار، يتم أيضاً 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 إلى مجموعات فرعية.
يتم تعطيل هذا الخيار افتراضياً.

• إعدادات الجدولة المتقدمة:

• قم بتشغيل الأجهزة باستخدام وظيفة Wake-on-Lan قبل بدء المهمة (دقيقة) 9

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 العملية من نطاق المهام، بما في ذلك تلك الأجهزة التي تم إيقاف تشغيلها عندما تكون المهمة على وشك البدء.
إذا كنت تريد إيقاف تشغيل الجهاز تلقائياً بعد اكتمال المهمة، فقم بتمكين خيار أغلق الأجهزة بعد الانتهاء من المهمة. يمكن العثور على هذا الخيار في النافذة نفسها.
يتم تعطيل هذا الخيار افتراضياً.

• أغلق الأجهزة بعد الانتهاء من المهمة 9

على سبيل المثال، قد ترغب في تمكين هذا الخيار لمهمة تحديث تثبيت والتي تقوم بتثبيت التحديثات على الأجهزة العملية كل يوم جمعة بعد ساعات العمل، ثم تقوم بإيقاف تشغيل هذه الأجهزة لعطلة نهاية الأسبوع.
يتم تعطيل هذا الخيار افتراضياً.

• أوقف المهمة إذا كانت أطول من (دقيقة) 9

بعد انتهاء الفترة الزمنية المحددة، يتم إيقاف المهمة تلقائياً، سواء أكانت مكتملة أم لا.
قم بتمكين هذا الخيار إذا كنت تريد مقاطعة (أو إيقاف) المهام التي تستغرق وقتاً طويلاً للتنفيذ.
يتم تعطيل هذا الخيار افتراضياً. وقت تنفيذ المهمة الافتراضي هو 120 دقيقة.

• إعدادات الإخطار:

• تخزين محفوظات المهمة حظر

• على خادم الإدارة لمدة (بالأيام) ④

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 افتراضياً.

• تخزين في سجل أحداث نظام التشغيل (OS) على جهاز ④

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة محلياً في سجل أحداث Windows لكل جهاز عميل.
يتم تعطيل هذا الخيار افتراضياً.

• تخزين في سجل أحداث نظام التشغيل (OS) على خادم إدارة ④

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة على جميع الأجهزة العميلة من نطاق المهام مركزياً في سجل أحداث Windows لنظام تشغيل خادم الإدارة (OS).
يتم تعطيل هذا الخيار افتراضياً.

• حفظ كل الأحداث ④

إذا تم تحديد هذا الخيار، فسيتم حفظ جميع الأحداث المتعلقة بالمهمة في سجلات الأحداث.

• حفظ الأحداث المتعلقة بتقدم المهمة ④

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بتنفيذ المهمة في سجلات الأحداث.

• حفظ نتائج تنفيذ المهمة فقط ④

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بنتائج المهمة في سجلات الأحداث.

• إخطار المسؤول بنتائج تنفيذ المهمة ④

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 ④

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 افتراضياً.

• إعدادات الأمن

• إعدادات نطاق المهمة

اعتماداً 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 أيضاً تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

• [مصادر التحديثات](#)

ويمكن استخدام الموارد التالية كمصدر للتحديثات ل خادم 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 افتراضياً 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 المثبت 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.

إذا قمت بتمكين الخيار لا تستخدم الخادم الوكيل خوادم تحديث Kaspersky أو مصادر التحديث المجلد المحلي أو مجلد الشبكة، فلن يستخدم خادم الإدارة خادمًا وكيلاً لتنزيل التحديثات.

- 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. بخلاف ذلك، تبدأ مهام التحديث على خوادم الإدارة الثانوية بالعمل وفقًا للجدول الزمنية الخاصة بهم. يتم تعطيل هذا الخيار افتراضياً.

- **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 إلى مستودع المهام لخوادم إدارة أخرى، قم بتحديد نفس مشاركة الشبكة كمصدر تحديث.

يتم تعطيل هذا الخيار افتراضياً.

- **لا تفرض تحديث الأجهزة وخوادم الإدارة الثانوية إلا عند اكتمال النسخ**

تبدأ مهام تنزيل التحديثات على الأجهزة العملية وخواص الإدارة الثانوية فقط بعد نسخ تلك التحديثات من مجلد التحديث الرئيسي إلى مجلدات التحديث الإضافية.
يجب تمكين هذا الخيار إذا كانت الأجهزة العملية وخواص الإدارة الثانوية تقوم بتنزيل تحديثات من مجلدات شبكة إضافية.
يتم تعطيل هذا الخيار افتراضياً.

• **تحديث الوحدات النمطية لعمل الشبكة (إصدارات عميل الشبكة الأقدم من Service Pack 2 10) [5]**

إذا تم تمكين هذا الخيار، فسيتم تثبيت التحديثات الخاصة بالوحدات النمطية لبرامج عميل الشبكة تلقائياً بعد انتهاء خادم الإدارة من مهمة تنزيل التحديثات إلى المستودع. خلافاً لذلك، يمكن تثبيت التحديثات التي يتم تلقيها للوحدات النمطية لعمل الشبكة يدوياً.
ينطبق هذا الخيار فقط على إصدارات Network Agent التي تسبق Service Pack 2 10. بدءاً من الإصدار Service Pack 2 10، يتم تحديث وكلاء الشبكة تلقائياً.
يتم تمكين هذا الخيار افتراضياً.

الإعدادات المحددة بعد إنشاء المهمة

يمكنك تحديد الإعدادات التالية بعد إنشاء المهمة فقط.

- إعدادات القسم، محتوى التحديثات حظر

• **تنزيل ملفات تفاضلية [5]**

يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff.
يتم تعطيل هذا الخيار افتراضياً.

- قسم التحقق من صحة التحديث

• **التحقق من صحة التحديثات قبل التوزيع [5]**

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 افتراضياً.

• **مهمة التحقق من صحة التحديث [5]**

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 مسبقاً. وبدلاً من ذلك، يمكنك إنشاء مهمة التحقق من صحة التحديث الجديدة.

إعدادات مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

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 HTTP(S) 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 المثبت 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.

إذا قمت بتمكين الخيار **لا تستخدم الخادم الوكيل** خوادم تحديث Kaspersky أو مصادر التحديث المجلد المحلي أو مجلد الشبكة، فلن تستخدم نقطة التوزيع خادمًا وكلياً لتنزيل التحديثات، حتى عند تمكين الخيار **استخدام الخادم الوكيل** في **إعدادات سياسة عميل الشبكة** الخاصة بنقطة التوزيع.

• 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 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 افتراضياً.

يمكنك تحديد الإعدادات التالية عند إنشاء مهمة. يمكن أيضاً 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 افتراضياً.

• **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، فسيُتصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft لتحديث المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق.

إذا تم تعطيل هذا الخيار، فسيستخدم وكيل تحديث Windows على جهاز مُدار يستخدم المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها من مصدر تحديثات Microsoft في وقت سابق والمُخزنة في الذاكرة المؤقتة للجهاز.

يمكن أن يكون الاتصال بمصدر تحديثات Microsoft مستهلكاً 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 عشوائياً في غضون 360 دقيقة. يتم تمكين هذا الخيار افتراضياً.

يحدد مزيج الخيارات التالية لإعدادات سياسة وكلاء الشبكة طريقة الحصول على التحديثات:

• لا يتصل وكيل تحديث Windows على جهاز مُدار بخادم التحديث للحصول على التحديثات إلا في حالة تمكين الخيار **الاتصال بخادم التحديث لتحديث البيانات** وتحديد الخيار **نشط**، في مجموعة الإعدادات **وضع بحث تحديث Windows**.

• يستخدم وكيل تحديث Windows على جهاز مُدار المعلومات المتعلقة بتحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها مسبقاً من مصدر تحديثات Microsoft وتم تخزينها في الذاكرة المؤقتة للجهاز، في حالة تمكين خيار **الاتصال بخادم التحديث لتحديث البيانات** وتحديد خيار **سلبي**، في مجموعة الإعدادات **وضع بحث تحديث Windows**، أو في حالة تعطيل خيار **الاتصال بخادم التحديث لتحديث البيانات** وتحديد خيار **نشط** في مجموعة الإعدادات **وضع بحث تحديث Windows**.

• بغض النظر عن حالة الخيار **الاتصال بخادم التحديث لتحديث البيانات** (ممكّن أو معطل)، إذا تم تحديد الخيار **معطل**، في مجموعة الإعدادات **وضع بحث تحديث Windows**، لا يطلب Kaspersky Security Center أي معلومات حول 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 افتراضياً.

• **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 بشكل افتراضي على مجلدات النظام التي يتم تثبيت معظم التطبيقات بها.

• **تمكين التشخيصات المتقدمة**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع حتى وإن كان التتبع معطلاً لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الآخر؛ 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 %Temp%\WINDIR. 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 وفقاً 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 لاحقاً 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 افتراضياً.

• **الحد الأقصى لحجم ملفات التشخيصات المتقدمة بالميجا بايت**

القيمة الافتراضية هي 100 ميجابايت، وتكون 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 أيضاً تعديل بعض هذه الإعدادات في خصائص المهمة التي تم إنشاؤها.

• **حدد قواعد لتثبيت التحديثات**

يتم تطبيق تلك القواعد على تثبيت التحديثات على الأجهزة العملية. 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 Microsoft و Kaspersky) في المجلد المحدد في حقل **مجلد تحميل التحديثات**. إذا تم تعطيل هذا الخيار، فسيتم تثبيت التحديثات على الجهاز تلقائيًا. يتم تعطيل هذا الخيار افتراضيًا.

• **مجلد تحميل التحديثات**

يتم استخدام هذا المجلد لتنزيل تحديثات خاصة بتطبيقات الجهات الخارجية (تطبيقات تم تطويرها من قبل بائعي برامج آخرين غير Kaspersky و Microsoft).

• **تمكين التشخيصات المتقدمة**

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع حتى وإن كان التتبع معطلًا لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الآخر؛ 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 %Temp%\WINDIR. 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** 5

القيمة الافتراضية هي 100 ميجابايت، وتكون 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 التالية بعد إنشاء المهمة فقط.

• 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 اختبائي 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 اختبائي 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 اختبائي 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 اختبائي 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**.
5. املأ الحقول التالية:

• الإعدادات العامة

عنوان الشبكة الفرعية للشبكة الفرعية التي تقوم بإضافتها.

• قناع الشبكة الفرعية

قناع الشبكة الفرعية للشبكة الفرعية التي تقوم بإضافتها.

• الاسم

اسم الشبكة الفرعية. يجب أي يكون فريداً ضمن القائمة العمومية للشبكات الفرعية. إذا قمت بإضافة الاسم الموجود بالفعل في القائمة، ستنتم 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 إلزامياً ويمكن تركه فارغاً.

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 في أنظمة التشغيل Windows و macOS و Linux: المقارنة

استخدام عميل الشبكة يتنوع اعتماداً على نظام التشغيل على الجهاز. تختلف إعدادات **سياسة عميل الشبكة** و**حزمة التثبيت** بناءً على نظام التشغيل. الجدول أدناه يقارن بين ميزات عميل الشبكة وسيناريوهات الاستخدام المتوفرة لأنظمة التشغيل Windows و macOS و Linux.

مقارنة ميزة عميل الشبكة

Linux	macOS	Windows	ميزة عميل الشبكة
التثبيت:			
—	—	✓	<u>الإشياء التلقائي لحزمة تثبيت عميل الشبكة بعد تثبيت Kaspersky Security Center</u>
✓	✓	✓	<u>التثبيت في الوضع الإلزامي، استخدام خيارات خاصة في مهمة التثبيت عن بُعد لـ Kaspersky Security Center.</u>
✓	✓	✓	<u>التثبيت عن طريق إرسال روابط الحزم المستقلة التي يتم إنشاؤها بواسطة Kaspersky Security Center إلى مستخدمي الجهاز.</u>
—	—	✓	<u>التثبيت عن طريق استنساخ صورة لمحرك القرص الثابت الخاص بالمسؤول والمثبت عليه نظام التشغيل و عميل الشبكة. استخدام الأدوات المقدمة من Kaspersky Security Center للتعامل مع صور القرص.</u>
✓	✓	✓	<u>التثبيت عن طريق استنساخ صورة لمحرك الأقراص الثابتة الخاص بالمسؤول باستخدام نظام التشغيل ووكيل الشبكة باستخدام أدوات الجهات الخارجية</u>
✓	✓	✓	<u>التثبيت باستخدام أدوات جهة خارجية لتثبيت التطبيقات عن بُعد.</u>
✓	✓	✓	<u>التثبيت يدوياً، عن طريق تشغيل مثبتات التطبيق على الأجهزة.</u>

✓	✓	✓	<u>تثبيت عميل الشبكة في الوضع الصامت</u>
✓	✓	✓	<u>تثبيت عميل الشبكة في الوضع غير التفاعلي</u>
✓	✓	✓	<u>اتصال جهاز عميل بخادم الإدارة يدويًا. الأداة المساعدة klmover</u>
—	—	✓	<u>التثبيت التلقائي للتحديثات والتصحيحات</u> <u>Kaspersky</u> <u>المخصصة لمكونات</u> <u>Security Center</u>
✓	✓	✓	<u>التوزيع التلقائي لمفتاح</u>
✓	✓	✓	<u>المزامنة المفروضة</u>
نقطة توزيع			
✓	✓	✓	<u>استخدام نقطة توزيع</u>
✓ بدون استخدام مصادقة مستوى الشبكة (NLA).	✓ بدون استخدام مصادقة مستوى الشبكة (NLA).	✓	<u>التخصيص التلقائي لنقاط التوزيع</u>
✓	✓	✓	<u>النموذج غير المتصل بالإنترنت الخاص</u> <u>بتنزيل التحديثات</u>
—	—	✓	<u>جميع أنواع استقصاء الشبكة</u>
—	—	✓	<u>تشغيل خدمة وكيل KSN على جانب نقطة التوزيع</u>
✓	— (في حال وجود جهاز أو أكثر من الأجهزة التي تعمل بنظام Linux أو macOS داخل نطاق مهمة تنزيل التحديثات في مستودعات نقاط التوزيع، نكتمل المهمة مع ظهور حالة فشل، حتى إذا تم إكمالها بنجاح على جميع أجهزة Windows).	✓	<u>تنزيل التحديثات إلى مستودعات نقاط التوزيع مباشرة من خوادم تحديث Kaspersky</u>
مقيد: بعد تحديد نوع نظام التشغيل على الأجهزة المتصلة بالشبكة من خلال الاستقصاء، لا يقوم خادم الإدارة بمحاولات لتثبيت الدفع على أجهزة Windows باستخدام نقاط توزيع غير Windows.	مقيد: بعد تحديد نوع نظام التشغيل على الأجهزة المتصلة بالشبكة من خلال الاستقصاء، لا يقوم خادم الإدارة بمحاولات لتثبيت الدفع على أجهزة Windows باستخدام نقاط توزيع غير Windows.	✓	<u>التثبيت عن بُعد للتطبيقات على أجهزة Windows</u>
✓	—	✓	<u>استخدام كخادم إرسال</u>
التعامل مع تطبيقات أخرى			
—	—	✓	<u>التثبيت عن بُعد للتطبيقات على الأجهزة</u>
—	—	✓	<u>تحديثات البرنامج</u>
—	—	✓	<u>تكوين تحديثات نظام التشغيل في سياسة عميل الشبكة</u>
—	—	✓	<u>عرض معلومات حول الثغرات الأمنية بالبرنامج</u>
—	—	✓	<u>فحص التطبيقات بحثًا عن ثغرات أمنية</u>
—	—	✓	<u>مخزون البرامج المثبتة على الأجهزة</u>
—	—	✓	<u>عرض سجل التطبيقات</u>
الأجهزة الظاهرية			

✓	✓	✓	<u>تثبيت عميل الشبكة على جهاز ظاهري</u>
✓	✓	✓	<u>إعدادات التحسين للبنية الأساسية لسطح المكتب الافتراضي (VDI).</u>
✓	✓	✓	<u>دعم الأجهزة الظاهرية الديناميكية</u>
أخرى			
—	—	✓	<u>تدقيق الإجراءات على جهاز عميل بعيد باستخدام مشاركة سطح المكتب لـ Windows</u>
✓	✓	✓	<u>مراقبة حالة الحماية ضد الفيروسات</u>
—	—	✓	<u>إدارة عمليات إعادة تشغيل الجهاز</u>
✓	✓	✓	<u>دعم عودة نظام الملفات</u>
✓	✓	✓	<u>استخدام عميل الشبكة هذا ك بوابة اتصال</u>
✓	✓	✓	<u>مدير الاتصالات</u>
—	✓	✓	<u>تعديل عميل الشبكة من خادم إدارة إلى آخر (تلقائيًا حسب موقع الشبكة).</u>
✓	✓	✓	<u>التحقق من اتصال جهاز عميل بخادم الإدارة الأداة المساعدة klnagchk</u>
—	✓ باستخدام نظام حوسبة الشبكة الافتراضية (VNC).	✓	<u>الاتصال البعيد بسطح مكتب جهاز عميل</u>
✓	✓	✓	<u>تنزيل حزمة تثبيت قائمة بذاتها من خلال معالج الترحيل</u>
✓	—	—	<u>استطلاع شبكة لا تتطلب تكوينًا</u>

Kaspersky Security Center 14 Web Console

يصف هذا القسم العمليات التي يمكنك إجراؤها باستخدام Kaspersky Security Center 14 Web Console.

حول Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console هو تطبيق ويب مصمم لإدارة حالة نظام أمن شبكات المؤسسة التي تتم حمايتها باستخدام تطبيقات Kaspersky.

يمكنك إجراء ما يلي باستخدام التطبيق:

- إدارة حالة نظام أمن 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.

Kaspersky Security Center 14 Web Console يوفر واجهة ويب تضمن تفاعل بين جهازك و خادم 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 مأخذ التوصيل الآمنة (SSL). عند الاتصال بـ Kaspersky Security Center 14 Web Console باستخدام المستعرض لديك، يقوم المستعرض بإنشاء اتصال بخادم Kaspersky Security Center 14 Web Console.

يمكنك تشغيل Kaspersky Security Center 14 Web Console كما يلي:

1. استخدم مستعرض في التوصليل مع Kaspersky Security Center 14 Web Console حيث يتم عرض واجهة بوابة الويب.
2. استخدم عناصر التحكم في بوابة الويب لاختيار أمر ترغب في تشغيله. Kaspersky Security Center 14 Web Console يجري العمليات التالية:
 - إذا حددت أمرًا مستخدمًا لاستقبال المعلومات (مثل عرض قائمة بالأجهزة)، يقوم Kaspersky Security Center 14 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 14 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 14 Web Console هو تطبيق متعدد اللغات. يمكنك تغيير لغة الواجهة في أي وقت، ودون الحاجة إلى إعادة فتح التطبيق. عند تثبيت Kaspersky Security Center 14 Web Console مع Kaspersky Security Center، يكون لدى Kaspersky Security Center 14 Web Console نفس لغة واجهة ملف التثبيت. أما عندما تقوم بتثبيت Kaspersky Security Center 14 Web Console فقط، يتم تثبيت التطبيق بنفس لغة الواجهة التي يعمل بها نظام التشغيل. إذا كان Kaspersky Security Center 14 Web Console لا يدعم لغة ملف التثبيت أو نظام التشغيل، تكون اللغة الإنجليزية هي اللغة الافتراضية.

إدارة الأجهزة المحمولة ليس مدعومًا في Kaspersky Security Center 14 Web Console. لكن إذا أضفت أجهزة محمولة إلى مجموعة إدارة عبر استخدام Microsoft Management Console، سيتم عرض تلك الأجهزة في Kaspersky Security Center 14 Web Console.

متطلبات الأجهزة والبرامج لـ Kaspersky Security Center 14 Web Console

خادم Kaspersky Security Center 14 Web Console

الحد الأدنى لمتطلبات الجهاز:

- وحدة المعالجة المركزية: 4 مراكز معالجة وتردد تشغيلي بسعة 2.5 جيجاهرتز
 - ذاكرة الوصول العشوائي: 8 جيجابايت
 - مساحة القرص المتوفرة: 40 جيجابايت
- أنظمة التشغيل التالية مدعومة:
- Microsoft Windows (لإصدارات 64-بت فقط):
 - Microsoft Windows 10 Enterprise 2015 LTSC
 - Microsoft Windows 10 Enterprise 2016 LTSC
 - Microsoft Windows 10 Enterprise 2019 LTSC
 - Microsoft Windows 10 Pro RS5 (تحديث أكتوبر 2018، رقم 1809)
 - Microsoft Windows 10 Pro for Workstations RS5 (تحديث أكتوبر 2018، رقم 1809)
 - Microsoft Windows 10 Enterprise RS5 (تحديث أكتوبر 2018، رقم 1809)
 - Microsoft Windows 10 Education RS5 (تحديث أكتوبر 2018، رقم 1809)
 - Microsoft Windows 10 Pro 19H1
 - Microsoft Windows 10 Pro for Workstations 19H1
 - Microsoft Windows 10 Enterprise 19H1
 - Microsoft Windows 10 Education 19H1
 - Microsoft Windows 10 Pro 19H2
 - Microsoft Windows 10 Pro for Workstations 19H2
 - Microsoft Windows 10 Enterprise 19H2
 - Microsoft Windows 10 Education 19H2
 - Microsoft Windows 10 Home 20H1 (تحديث مايو 2020)
 - Microsoft Windows 10 Pro 20H1 (تحديث مايو 2020)
 - Microsoft Windows 10 Enterprise 20H1 (تحديث مايو 2020)
 - Microsoft Windows 10 Education 20H1 (تحديث مايو 2020)
 - Microsoft Windows 10 Home 20H2 (تحديث أكتوبر 2020)
 - Microsoft Windows 10 Pro 20H2 (تحديث أكتوبر 2020)

- Microsoft Windows 10 Enterprise 20H2 (تحديث أكتوبر 2020)
- Microsoft Windows 10 Education 20H2 (تحديث أكتوبر 2020)
- Microsoft Windows 10 Home 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Pro 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Education 21H1 (تحديث مايو 2021) 32 بت/64 بت
- Microsoft Windows 10 Home 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Pro 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Enterprise 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 10 Education 21H2 (تحديث أكتوبر 2021) 32 بت/64 بت
- Microsoft Windows 11 Home
- Microsoft Windows 11 Pro
- Microsoft Windows 11 Enterprise
- Microsoft Windows 11 Education
- Windows Server 2012 Server Core
- Windows Server 2012 Datacenter
- Windows Server 2012 Essentials
- Windows Server 2012 Foundation
- Windows Server 2012 Standard
- Windows Server 2012 R2 Server Core
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 R2 Essentials
- Windows Server 2012 R2 Foundation
- Windows Server 2012 R2 Standard
- (Windows Server 2016 Datacenter (LTSC
- (Windows Server 2016 Standard (LTSC
- (Windows Server 2016 Server Core (Installation Option) (LTSC
- Windows Server 2019 Standard 64 بت

- Windows Server 2019 Datacenter 64 بت
- Windows Server 2019 Core 64 بت
- Windows Server 2022 Standard 64 بت
- Windows Server 2022 Datacenter 64 بت
- Windows Server 2022 Core 64 بت
- Windows Storage Server 2012 64 بت
- Windows Storage Server 2012 R2 64 بت
- Windows Storage Server 2016 64 بت
- Windows Storage Server 2019 64 بت
- Linux (إصدارات 64 بت فقط):
 - (Debian GNU/Linux 11.x (Bullseye
 - (Debian GNU/Linux 10.x (Buster
 - (Debian GNU/Linux 9.x (Stretch
 - (Ubuntu Server 20.04 LTS (Focal Fossa
 - (Ubuntu Server 18.04 LTS (Bionic Beaver
 - CentOS 7.x
 - Red Hat Enterprise Linux Server 8.x
 - Red Hat Enterprise Linux Server 7.x
 - SUSE Linux Enterprise Server 12 (جميع حزم الخدمات)
 - SUSE Linux Enterprise Server 15 (جميع حزم الخدمات)
 - SUSE Linux Enterprise Desktop 15 (حزمة الخدمة 3) ARM
 - Astra Linux Special Edition 1.7 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي)
 - Astra Linux Special Edition 1.6 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي)
 - Astra Linux Common إصدار 2.12
 - Alt Server 10
 - Alt Server 9.2
 - (Alt 8 SP Server (LKNV.11100-01
 - (Alt 8 SP Server (LKNV.11100-02

(Alt 8 SP Server (LKNV:11100-03 •

Oracle Linux 8 •

Oracle Linux 7 •

RED OS 7.3 Server •

RED OS 7.3 إصدار معتمد •

من بين منصات المحاكاة الافتراضية، يتم دعم Virtual Machine المستندة إلى Kernel لأنظمة التشغيل التالية:

Alt 8 SP Server (LKNV:11100-01) 64 •

Alt Server 10 64 بت •

Astra Linux Special إصدار 1.7 (بما في ذلك وضع بيئة البرامج المغلقة والوضع الإلزامي) 64 بت •

Debian GNU/Linux 11.x (Bullseye) 32 بت/64 بت •

Ubuntu Server 20.04 LTS (Focal Fossa) 32 بت/64 بت •

RED OS 7.3 Server 64 بت •

RED OS 7.3 إصدار معتمد 64 بت •

لا يتوافق خادم Kaspersky Security Center 14 Web Console Server مع أنظمة التشغيل:

Microsoft Windows Essential Business Server 2008 Standard/Premium •

Microsoft Windows Small Business Server 2003 Standard/Premium مع SP1 •

Microsoft Windows Small Business Server 2003 R2 Standard/Premium •

Microsoft Windows Small Business Server 2008 Standard/Premium •

Microsoft Windows Small Business Server 2011 Essentials •

Microsoft Windows Small Business Server 2011 Premium Add-on •

Microsoft Windows Small Business Server 2011 Standard •

Microsoft Windows Home Server 2011 •

Microsoft Windows MultiPoint Server 2010 Standard/Premium •

Microsoft Windows MultiPoint Server 2011 Standard/Premium •

Microsoft Windows MultiPoint Server 2012 Standard/Premium •

Microsoft Windows Server 2000 •

Microsoft Windows Server 2003 Enterprise مع SP2 •

Microsoft Windows Server 2003 Standard مع SP2 •

• Microsoft Windows Server 2003 R2 Enterprise مع SP2

• Microsoft Windows Server 2003 R2 Standard مع SP2

الأجهزة العميلة

بالنسبة لجهاز عميل، لا يتطلب استخدام Kaspersky Security Center 14 Web Console إلا وجود مستعرض.

تتطابق متطلبات الأجهزة والبرامج في الجهاز مع تلك الخاصة بالمستعرض المستخدم للعمل مع Kaspersky Security Center 14 Web Console.

المستعرضات:

• إصدار Mozilla Firefox Extended Support 91.8.0 أو إصدار أحدث (91.8.0 تم إصداره في 5 أبريل 2022)

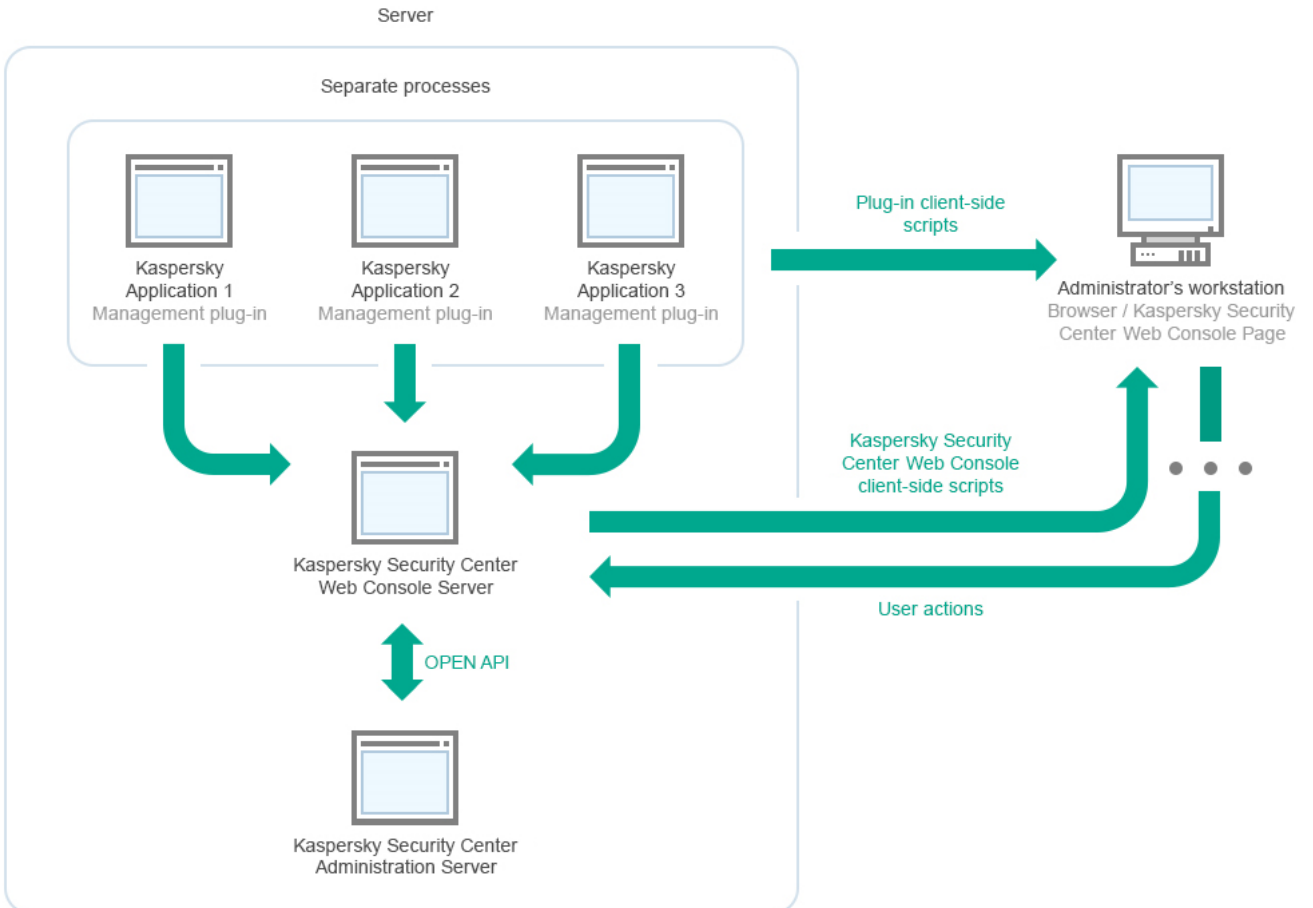
• إصدار Mozilla Firefox 99.0 أو إصدار أحدث (تم إصدار 99.0 في 5 أبريل 2022)

• Google Chrome 100.0.4896.88 أو إصدار أحدث (إصدار رسمي)

• Microsoft Edge 100 أو إصدار أحدث

نشر مخطط خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console

يوضح الشكل أدناه مخطط النشر لكل من خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console.



إدارة المكونات الإضافية لتطبيقات Kaspersky المثبتة على الأجهزة المحمية (مكون إضافي واحد لكل تطبيق) يتم نشرها مع خادم Kaspersky Security Center 14 Web Console.

وبصفتك مديرًا، يمكنك الوصول إلى Kaspersky Security Center 14 Web Console عبر استخدام مستعرض على محطة العمل لديك.

عند تنفيذ إجراءات محددة في Kaspersky Security Center 14 Web Console، يتواصل خادم Kaspersky Security Center 14 Web Console مع Console Server إدارة Kaspersky Security Center عبر OpenAPI. يطلب Kaspersky Security Center 14 Web Console Console Server المعلومات المطلوبة من خادم إدارة Kaspersky Security Center ويعرض نتائج عملياتك في Kaspersky Security Center 14 Web Console.

المنافذ المستخدمة بواسطة وحدة تحكم الويب لـ Kaspersky Security Center 14

يسرد الجدول أدناه المنافذ التي يجب أن تكون مفتوحة على الجهاز حيث تم تثبيت خادم Kaspersky Security Center 14 Web Console (يُشار إليه أيضًا باسم Kaspersky Security Center 14 Web Console).

المنافذ المستخدمة بواسطة وحدة تحكم الويب لـ Kaspersky Security Center 14

المنفذ	رقم المنفذ	البروتوكول	غرض المنفذ	النطاق
2001	HTTPS	منفذ API مستخدم في استقبال الطلبات من خدمة KSCWebConsoleManagementService التي تعمل على نفس الجهاز.	تشغيل node.exe يعالج كل من Kaspersky Security Center 14 Web Console ومكونات الإدارة الإضافية.	
2003	HTTPS	منفذ API مستخدم في استقبال الطلبات من خدمة KSCWebConsole التي تعمل على نفس الجهاز.	تحديث مكونات Kaspersky Security Center 14 Web Console	
3333	HTTPS	منفذ نقطة نهاية مصادقة OAuth2.0	إدارة الهوية والوصول	
4004	HTTPS	منفذ موفر هوية OAuth2.0	إدارة الهوية والوصول	
4444	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 HashiCorp Vault)	تثبيت Kaspersky Security Center 14 Web	

Console وتحديث مكونات Kaspersky Security Center 14 Web Console				
التفاعل بين Kaspersky Security Center 14 Web Console ومكونات الإدارة الإضافية.	منفذ API لوسيط الرسائل المستخدم للتواصل بين Kaspersky Security Center 14 Web Console عمليات كل من Kaspersky Security Center 14 ومكونات الإدارة الإضافية.	HTTPS	4152	KSCWebConsoleMessageQueue

يسرد الجدول أدناه المنافذ التي لا يجب أن تكون مفتوحة على الجهاز حيث تم تثبيت خادم Kaspersky Security Center 14 Web Console. ومع ذلك، يستخدم Kaspersky Security Center 14 وحدة التحكم في الويب هذه المنافذ الخاصة [بإدارة الهوية والوصول](#).

المنافذ المستخدمة من قبل Kaspersky Security Center 14 لإدارة الهوية والوصول

المنفذ	البروتوكول	رقم المنفذ	اسم الخدمة	غرض المنفذ	النطاق
4445	HTTPS	خدمة Kaspersky OSMP KAS	منفذ إدارة الهوية والوصول الرئيسي الذي يتلقى التكوين من Kaspersky Security Center 14 وحدة التحكم على شبكة الإنترنت لمنفذ نقطة اتصال OAUTH2.0 (لمزيد من المعلومات حول OAUTH 2.0، راجع موقع OAuth)	إدارة الهوية والوصول	
2444	HTTPS	Kaspersky OSMP Facade Service	منفذ تكوين إدارة الهوية والوصول	إدارة الهوية والوصول	
2445	HTTPS	Kaspersky OSMP Facade Service	منفذ اتصال خدمة Kaspersky Osmk Kas لخدمة Kaspersky Osmk Facade	إدارة الهوية والوصول	

السيناريو: تثبيت وإعداد مبدئي لـ Kaspersky Security Center 14 Web Console

يصف هذا السيناريو كيفية تثبيت خادم إدارة Kaspersky Security Center 14 و Kaspersky Security Center 14 Web Console: قم بإجراء إعداد أولي لخادم الإدارة عبر استخدام معالج البدء السريع وقم بتثبيت تطبيقات Kaspersky على الأجهزة المُدارة باستخدام معالج نشر الحماية.

تثبيت وإعداد مبدئي لـ Kaspersky Security Center 14 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.

2 تثبيت خادم الإدارة، وحدة تحكم الإدارة عميل الشبكة

يتم تثبيت وحدة تحكم الإدارة وإصدار خادم عميل الشبكة مع خادم الإدارة.

أثناء تثبيت خادم الإدارة [Kaspersky Security Center 14](#)، حدد ما إذا كنت تريد تثبيت Kaspersky Security Center 14 Web Console على نفس الجهاز. إذا اخترت تثبيت كلا المكونين على الجهاز نفسه، ليس عليك أن تثبت Kaspersky Security Center 14 Web Console بشكل منفصل لأنه يتم تثبيته بشكل تلقائي. إذا كنت ترغب في تثبيت Kaspersky Security Center 14 Web Console على جهاز مختلف، فيعد تثبيت Kaspersky Security Center 14 خادم الإدارة، تابع تثبيت Kaspersky Security Center 14 Web Console.

3 تثبيت Kaspersky Security Center 14 Web Console

إذا لم تختبر تثبيت Kaspersky Security Center 14 Web Console مع خادم إدارة Kaspersky Security Center في الخطوة السابقة، فقم [بتثبيت Kaspersky Security Center 14 Web Console](#) بشكل منفصل. يمكنك تثبيت Kaspersky Security Center 14 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](#) و [المهام](#) 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 يدعم [الوظائف الأساسية لوحدة الإدارة](#) لا يتطلب أي ترخيص. أنت بحاجة إلى ترخيص تجاري إذا كنت ترغب في استخدام أحد المزايا الإضافية أو أكثر، بما في ذلك إدارة الثغرات الأمنية والتصحيحات وإدارة الأجهزة المحمولة والتكامل مع أنظمة SIEM. يمكنك إضافة ملف مفتاح أو رمز تنشيط لهذه المزايا في [الخطوة المقابلة](#) في [معالج البدء السريع](#) يدويًا.

6 اكتشاف أجهزة الشبكة

هذه الخطوة 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 هي 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 تشكل 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 للجوال (اختياري)

إذا كنت تخطط لإدارة الأجهزة المحمولة الخاصة بالشركة، فاتباع الإرشادات الواردة في تعليمات [Kaspersky Security for Mobile Help](#) للحصول على معلومات حول 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](#) و [المهام](#). لا يمكنك تطبيق المهام إلا على الأجهزة التي تلي 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:

تثبيت نظام إدارة قواعد البيانات

قم بتثبيت نظام إدارة قاعدة البيانات (DBMS) الذي سيتم استخدامه من قبل Kaspersky Security Center. يمكنك اختيار أحد الإصدارات [المدعومة](#) من خادم Microsoft SQL أو MySQL أو MariaDB.

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

لأفضل استخدام لقاعدة بيانات MariaDB، أنت بحاجة إلى [تكوين الإعدادات الموصى بها](#).

تكوين خادم MariaDB x64 للعمل مع Kaspersky Security Center 14

يدعم Kaspersky Security Center 14 الإصدار 10.3 من MariaDB (الإصدار 10.3.22 والإصدارات الأحدث).

إذا كنت تستخدم خادم MariaDB مع Kaspersky Security Center، مكن 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:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
<innodb_buffer_pool_size=< value
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

قيمة innodb_buffer_pool_size يجب أن تكون أعلى من 80 بالمائة من الحجم المتوقع لقاعدة البيانات KAV.

ننصح باستخدام قيمة المعلمة innodb_flush_log_at_trx_commit=0 لأن القيم "1" أو "2" تؤثر بالسلب على سرعة تشغيل MariaDB.

بشكل افتراضي، إضافات المحسن join_cache_incremental و join_cache_hashed و join_cache_bka تكون مفعلة. 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:

```
join_cache_incremental=on  
join_cache_hashed=on  
join_cache_bka=on
```

إذا كانت هذه السطور موجودة وكانت قيمتها مشغلة ، هذا يعني أن إضافات المحسن مفعلة.

إذا لم تكن هذه السطور موجودة أو قيمتها معطلة ، فعليك عمل التالي:

1. افتح ملف my.ini في أي محرر نصوص.

2. أضف الأسطر التالية إلى قسم [mysqld] من ملف my.ini:

```
'optimizer_switch='join_cache_incremental=on  
'optimizer_switch='join_cache_hashed=on  
'optimizer_switch='join_cache_bka=on
```

الإضافات join_cache_incremental, join_cache_hash, and join_cache_bka مفعلة.

تكوين خادم MySQL x64 للعمل مع Kaspersky Security Center 14

إذا كنت تستخدم خادم MySQL مع Kaspersky Security Center، مكن 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:

```
sort_buffer_size = 10M  
join_buffer_size = 20M  
tmp_table_size = 600M  
max_heap_table_size = 600M  
key_buffer_size = 200M
```

innodb_buffer_pool_size = يجب ألا تقل القيمة الحقيقية عن 80% من حجم قاعدة بيانات KAV المتوقع

```
innodb_thread_concurrency = 20  
innodb_flush_log_at_trx_commit = 0 (في معظم الحالات، يستخدم الخادم معاملات صغيرة)  
innodb_lock_wait_timeout = 300  
max_allowed_packet = 32M  
max_connections = 151  
max_prepared_stmt_count=12800  
table_open_cache=60000  
table_open_cache_instances=4  
table_definition_cache=60000
```

ينصح باستخدام قيمة المعلمة innodb_flush_log_at_trx_commit=0 لأن القيم "1" أو "2" تؤثر بالسلب على سرعة تشغيل MySQL.

تثبيت Kaspersky Security Center (تثبيت قياسي)

يصف هذا الإجراء كيفية تثبيت Kaspersky Security Center. يجب قبل التثبيت أن تقوم بتثبيت [نظام لإدارة قواعد البيانات](#).

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**.
بهذا سيبدأ معالج إعداد خادم إدارة Kaspersky Security Center.
 3. بدايةً من صفحة الترحيب، انتقل عبر المعالج من خلال استخدام زر **التالي**.
 4. إذا كان Microsoft .NET Framework غير مثبت، 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 14 Web Console على نفس الجهاز، فحدد خانة الاختيار **تثبيت Kaspersky Security Center 14 Web Console**.
إذا قمت بإلغاء تحديد مربع الاختيار، يمكنك بعد ذلك **تثبيت Kaspersky Security Center 14 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 التي ثبتها **قبل ذلك**.
 10. حدد معلومات الاتصال بخادم قاعدة البيانات الذي ثبته من قبل.
 11. حدد معلومات التصديق بخادم قاعدة البيانات الذي ثبته من قبل.
 12. انقر على زر **تثبيت لبدء التثبيت**.
 13. بعد اكتمال التثبيت بنجاح، اختر إذا ما كنت ترغب في بدء وحدة تحكم الإدارة مباشرةً بعد إغلاق المعالج أم لا.
إذا اخترت فتح Kaspersky Security Center 14 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 14 Web Console إلا إذا كان مثبتاً بالفعل. لا يمكنك فتح Kaspersky Security Center 14 Web Console إذا لم يتم تثبيته 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 يتم تشغيله 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 14 Web Console

يصف هذا القسم كيفية تثبيت Kaspersky Security Center 14 Web Console Server (يُشار إليه أيضًا باسم Kaspersky Security Center 14 Web Console) بشكل منفصل. يجب قبل التثبيت أن تقوم بتثبيت [نظام لإدارة قواعد البيانات](#) و خادم إدارة [Kaspersky Security Center](#). يمكنك تثبيت Kaspersky Security Center 14 Web Console على نفس الجهاز المثبت عليه Kaspersky Security Center أو على جهاز مختلف.

لتثبيت Kaspersky Security Center 14 Web Console:

1. من حساب يتمتع بامتيازات إدارية، قم بتشغيل ملف التثبيت `ksc-web-console-<version number>.<build number>.exe`. يؤدي هذا إلى تشغيل معالج الإعداد.
 2. حدد لغة لمعالج الإعداد.
 3. في نافذة الترحيب، انقر على التالي.
 4. في نافذة **اتفاقية الترخيص**، اقرأ شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل و اقبلها. يستمر التثبيت بعد قبولك اتفاقية ترخيص المستخدم النهائي، وإلا لن يكون زر التالي متاحًا.
 5. في نافذة **مجلد التثبيت**، حدد مجلدًا يتم فيه تثبيت Kaspersky Security Center 14 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 الزر **استعراض**.
 6. في نافذة **إعدادات اتصال Kaspersky Security Center 14 Web Console**، حدد المعلومات التالية:
 - عنوان Kaspersky Security Center 14 Web Console (العنوان الافتراضي هو 127.0.0.1).
 - المنفذ الذي سيستخدمه Kaspersky Security Center 14 Web Console للاتصالات الواردة، أي المنفذ الذي يتيح الوصول إلى Kaspersky Security Center 14 Web Console من مستعرض (افتراضيًا، 8080).ننصحك بأن تترك العنوان رقم المنفذ كما هما دون تغيير.
إذا كنت ترغب، يمكنك النقر على **اختبار** للتأكد أن المنفذ المحدد متاحًا.
إذا كنت ترغب في **تفعيل تسجيل أنشطة Kaspersky Security Center 14 Web Console**، حدد الخيار المناسب لذلك. إذا لم تحدد هذا الخيار، لن يتم إنشاء ملفات سجل Kaspersky Security Center 14 Web Console.
- لا يدعم Kaspersky Security Center 14 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`.
7. في نافذة **إعدادات الحساب**، حدد أسماء الحساب وكلمات المرور.
نوصي بأن تستخدم الحسابات الافتراضية.
 8. في نافذة **شهادة العميل**، حدد أحد الخيارات التالية:
 - **إنشاء شهادة جديدة**. يُنصح بهذا الخيار إذا لم يكن لديك شهادة مستعرض.
 - **اختيار الموجود**. يمكنك تحديد هذا الخيار إذا كان لديك بالفعل شهادة مستعرض، وفي هذه الحالة حدد مسارها.
 9. في نافذة **خوادم الإدارة الموثوقة**، تأكد أن خادم الإدارة لديك في القائمة ثم انقر على التالي من أجل التقدم إلى آخر نافذة للمثبت.
 10. في نافذة **Identity and Access Manager (IAM)**، حدد ما إذا كنت تريد تثبيت **إدارة الهوية والوصول** (يُشار إليها أيضًا باسم IAM). إذا اخترت تثبيت الهوية وإجراءات الوصول، فحدد أرقام المنفذ التالية:

• **منفذ مدير KAS**. يتم استخدام منفذ 4445 بشكل افتراضي لتلقي التكوين من Kaspersky Security Center 14 Web Console لمنفذ نقطة النهاية OAuth2.0.

• **منفذ مدير Facade**. يتم استخدام منفذ 2444 بشكل افتراضي لتكوين إدارة الهوية والوصول.

• **منفذ تفاعل Facade**. 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 14 Web Console.

11. في آخر نافذة للمثبت، انقر على **تثبيت** من أجل بدء التثبيت.

بعد اكتمال التثبيت بنجاح، سيظهر اختصار على سطح المكتب، ويمكنك **تسجيل الدخول** إلى Kaspersky Security Center 14 Web Console.

يبدأ **معالج البدء السريع لخدمات الإدارة** إذا لم تقم بتشغيله في وحدة تحكم الإدارة التي تعمل على Microsoft Management Console.

استكشاف الأخطاء وحلها

إذا لم يتم عرض Kaspersky Security Center 14 Web Console في مستعرضك في عنوان URL الذي كتبتَه، جَرِّب ما يلي:

1. تأكد أنك حددت اسم المضيف الصحيح أو عنوان IP للجهاز الذي تم تثبيت Kaspersky Security Center 14 Web Console عليه.

2. تأكد أن الجهاز الذي ترغب في تشغيله لديه وصول إلى الجهاز المثبت عليه Kaspersky Security Center 14 Web Console.

3. تحقق من أن إعدادات جدار الحماية على الجهاز المثبت عليه Kaspersky Security Center 14 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 14 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 14 Web Console على منصات Linux

يشرح هذا القسم كيفية تثبيت خادم Kaspersky Security Center 14 Web Console (يُشار إليه أيضًا باسم Kaspersky Security Center 14 Web Console) على الأجهزة التي تعمل بنظام التشغيل Linux (راجع **قائمة توزيعات Linux المدعومة**).

تثبيت Kaspersky Security Center 14 Web Console على منصات Linux

يصف هذا القسم كيفية تثبيت Kaspersky Security Center 14 Web Console Server (يُشار إليه أيضًا باسم Kaspersky Security Center 14 Web Console) على الأجهزة التي تعمل بنظام التشغيل Linux. يجب قبل التثبيت أن تقوم بتثبيت **نظام لإدارة قواعد البيانات** وخادم إدارة **Kaspersky Security Center**.

استخدم ملف التثبيت ksc-web-console-[version_number].deb أو ksc-web-console-[version_number].x86_64.rpm الذي يتوافق مع توزيعة Linux المثبتة على جهازك. سوف تستقبل ملف التثبيت بتنزيله من موقع Kaspersky.

لتثبيت Kaspersky Security Center 14 Web Console:

1. تأكد أن الجهاز الذي ترغب في تثبيت Kaspersky Security Center 14 Web Console عليه يعمل بإحدى [توزيعات Linux المدعومة](#).

2. اقرأ اتفاقية ترخيص المستخدم النهائي الذي قمت بتنزيله مع ملف التثبيت. في حالة عدم الموافقة على شروط اتفاقية الترخيص، يجب عدم تثبيت التطبيق.

3. أنشئ [ملف استجابة](#) يحتوي على معلومات لتوصيل Kaspersky Security Center 14 Web Console بخادم الإدارة. قم بتسمية ذلك الملف ksc-web-console-setup.json وضعه في المجلد التالي: etc/ksc-web-console-setup.json.
مثال على ملف استجابة يحتوي على أقل مجموعة من المعلومات مع العنوان والمنفذ الافتراضيين:

```
}
  "العنوان": "127.0.0.1",
  "المنفذ": "8080",
  "خادم KSC موثوق": "
  "cert/klserver.cer/|13299|127.0.0.1" |var/opt/kaspersky/klagent_srv/1093/
  "acceptEula": "حقيقي"
}
```

عند تثبيت Kaspersky Security Center 14 Web Console على نظام التشغيل Linux ALT، يجب عليك تحديد رقم منفذ بخلاف 8080، لأن المنفذ 8080 يستخدمه نظام التشغيل.

لا يمكن تحديث Kaspersky Security Center 14 Web Console باستخدام نفس ملف التثبيت بامتداد rpm. إذا كنت ترغب في تغيير بعض الإعدادات في ملف الاستجابة واستخدام ذلك الملف في إعادة تثبيت التطبيق، يجب عليك أولاً إزالة التطبيق ثم تثبيته مرة أخرى بملف الاستجابة الجديد.

4. من حساب يتمتع بالمزايا الإدارية، استخدم سطر الأوامر في تشغيل ملف الإعداد بامتداد deb. أو rpm، حسب توزيع Linux التي تستخدمها.

• لتثبيت Kaspersky Security Center 14 Web Console أو ترقيته من ملف بامتداد deb، أدخل الأمر التالي:
`sudo dpkg -i ksc-web-console-[version_number].deb $`

• لتثبيت Kaspersky Security Center 14 Web Console من ملف بامتداد rpm، أدخل الأمر التالي:
`sudo rpm -ivh --nodeps ksc-web-console-[version_number].x86_64.rpm $`

• لترقية Kaspersky Security Center Web Console من إصدار سابق، أدخل أحد الأوامر التالية:

• بالنسبة للأجهزة التي تعمل بنظام التشغيل المستند إلى RPM:
`sudo rpm -Uvh --nodeps --force ksc-web-console-[version_number].x86_64.rpm $`

• بالنسبة للأجهزة التي تعمل بنظام التشغيل المستند إلى Debian:
`sudo dpkg -i ksc-web-console-[version_number].x86_64.deb $`

يبدأ هذا حزمة ملف الإعداد. يُرجى الانتظار حتى يكتمل التثبيت. يتم تثبيت Kaspersky Security Center 14 Web Console في المسار التالي:
`var/opt/kaspersky/ksc-web-console/`

و عندما يكتمل التثبيت، يمكنك استخدام المستعرض في [فتح Kaspersky Security Center 14 Web Console وتسجيل الدخول إليه](#).

معلومات تثبيت Kaspersky Security Center 14 Web Console

من أجل [تثبيت خادم Kaspersky Security Center 14 Web Console على أجهزة تعمل بنظام Linux](#)، يجب أن تقوم بإنشاء ملف استجابة بتنسيق JSON يحتوي على معلومات لتوصيل Kaspersky Security Center 14 Web Console بخادم الإدارة.

مثال على ملف استجابة يحتوي على أقل مجموعة من المعلومات مع العنوان والمنفذ الافتراضيين:


```

    "العنوان": "127.0.0.1",
    "المنفذ": 8080,
    "defaultLangId": 1049,
    "enableLog": false,
    "خادم KSC موثوق": true,
    "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
    "webConsoleAccount": "Group1: User1",
    "managementServiceAccount": "Group2: User3"
  }

```

عند تثبيت Kaspersky Security Center 14 Web Console على نظام التشغيل Linux ALT، يجب عليك تحديد رقم منفذ بخلاف 8080، لأن المنفذ 8080 يستخدمه نظام التشغيل.

الجدول أدناه يصف المعلمات التي يمكن تحديدها في ملف استجابة.

معلومات تثبيت Kaspersky Security Center 14 Web Console على أجهزة تعمل بنظام Linux

القيم المتوفرة	الوصف	المعلمة
قيمة السلسلة.	نوان خادم Kaspersky Security Center 14 Web Console (مطلوب).	العنوان
قيمة رقمية.	رقم المنفذ الذي يستخدمه خادم Kaspersky Security Center 14 Web Console في التوصيل بخادم الإدارة (مطلوب).	المنفذ
الرمز الرقمي للغة: <ul style="list-style-type: none"> • الألمانية: 1031 • الإنجليزي: 1033 • الأسبانية: 3082 • الأسبانية (المكسيك): 2058 • الفرنسية: 1036 • اليابانية: 1041 • الكازاخستانية: 1087 • البولندية: 1045 • البرتغالية (البرازيل): 1046 • الروسية: 1049 	لغة واجهة المستخدم الافتراضي هو (1033).	defaultLangId

<ul style="list-style-type: none"> • اللغة التركية: 1055 • الصينية المبسطة: 4 • الصينية التقليدية: 31748 <p>في حال عدم تحديد قيمة، سيتم استخدام اللغة الإنجليزية.</p>		
<p>قيمة منطقية:</p> <ul style="list-style-type: none"> • true –التسجيل مفعّل (هذا هو الاختيار الافتراضي). • false –التسجيل غير مفعّل. 	<p>تفعيل تسجيل نشاط Kaspersky Security Center 14 Web Console أو لا.</p>	<p>enableLog</p>
<p>قيمة السلسلة للتنسيق التالي:</p> <p>"عنوان الخادم المنفذ مسار الشهادة اسم الخادم مثال:</p> <p>X.X.X.X 13299 /cert/server-1.cer Server" .Y.Y.Y.Y 13299 /cert/server-2.cer Server 2".1 </p>	<p>قائمة بخوادم الإدارة الموثوقة المسموح لها بالاتصال بـ Kaspersky Security Center 14 Web Console (مطلوبة). يجب تعريف كل خادم إدارة بالمعلومات التالية:</p> <ul style="list-style-type: none"> • عنوان خادم الإدارة • منفذ OpenAPI الذي يستخدمه Kaspersky Security Center 14 Web Console في الاتصال بخادم الإدارة (الافتراضي هو 13299). • مسار شهادة خادم الإدارة • اسم خادم الإدارة الذي سيتم عرضه في نافذة تسجيل الدخول 	<p>موثوق</p>

	<p>يتم الفصل بين المعلومات باستخدام أشرطة عمودية. في حال تحديد عدة خوادم إدارة، افصل بينهم باستخدام شريطين عموديين (أنبوبين).</p>	
<p>قيمة منطقية:</p> <ul style="list-style-type: none"> • صحيح – لقد قرأت شروط <u>اتفاقية ترخيص المستخدم النهائي</u> بشكل كامل واستوعقتها. • false – لا أقبل شروط اتفاقية الترخيص (الاختيار الافتراضي). 	<p>acceptEula</p> <p>سواء كنت ترغب في قبول شروط <u>اتفاقية ترخيص المستخدم النهائي</u> أو عدم قبولها. يحتوي الملف على شروط اتفاقية ترخيص المستخدم النهائي التي يتم تنزيلها مع ملف التثبيت (مطلوب).</p>	
<p>قيمة السلسلة.</p>	<p>certDomain</p> <p>إذا كنت ترغب في إنشاء شهادة جديدة، استخدم هذا المعامل في تحديد اسم النطاق الذي سيتم إنشاء شهادة جديدة له.</p>	
<p>قيمة السلسلة.</p> <p>حدد المسار</p> <p>'kaspersky/klInagent_srv/1093/cert/klserver.cer/'</p> <p>لاستخدام الشهادة الحالية. للحصول على شهادة مخصصة، حدد المسار حيث يتم تخزين الشهادة المخصصة.</p>	<p>certPath</p> <p>إذا كنت ترغب في استخدام شهادة حالية، استخدم هذا المعامل في تحديد مسار ملف الشهادة.</p>	
<p>قيمة السلسلة.</p>	<p>keyPath</p> <p>إذا كنت ترغب في استخدام شهادة حالية، استخدم هذا المعامل في تحديد مسار ملف المفتاح.</p>	
<p>قيمة السلسلة بالتنسيق التالي: "اسم المجموعة: اسم المستخدم".</p> <p>مثال: "Group1: User1".</p> <p>إذا لم يتم تحديد قيمة، سيتم إنشاء حساب جديد.</p>	<p>webConsoleAccount</p> <p>اسم الحساب الذي لا يتمتع بمزايا إدارية للعمل مع Kaspersky Security Center 14 Web Console.</p>	
<p>قيمة السلسلة بالتنسيق التالي: "اسم المجموعة: اسم المستخدم".</p> <p>مثال: "Group1: User1".</p> <p>إذا لم يتم تحديد قيمة، سيتم إنشاء حساب جديد.</p>	<p>managementServiceAccount</p> <p>اسم الحساب الذي يتمتع بمزايا إدارية للعمل مع Kaspersky Security Center 14 Web Console.</p>	

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 `ksc-web-console-<version number>.<build number>.exe`، حيث يشير `<build number>` إلى بنية Kaspersky Security Center Web Console الذي يكون رقمه أعلى 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 14 Web Console modification**، انقر على زر **Upgrade**. انتظر حتى يتم تطبيق الإعدادات الجديدة ثم انقر على **Finish** في الخطوة التالية في معالج الإعداد. يمكنك كذلك النقر على رابط **Start Kaspersky Security Center 14 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 أعلى.

يتم ترقية إصدار Kaspersky Security Center Web Console.

شهادات للعمل مع Kaspersky Security Center 14 Web Console

يصف القسم كيفية إصدار واستبدال الشهادات لوحدة تحكم ويب Kaspersky Security Center 14 وكيفية تجديد شهادة لخادم الإدارة إذا كان الخادم يتفاعل مع Kaspersky Security Center 14 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.

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**).

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 `.ksc-web-console-<version number>.<build number>.exe`.

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 14 Web Console

بشكل افتراضي، عندما تقوم بتثبيت Kaspersky Security Center 14 Web Console Server، يتم إنشاء شهادة متصفح للتطبيق تلقائيًا. يمكنك استبدال الشهادة التي تم إنشاؤها بشكل تلقائي بأخرى مخصصة.

لاستبدال شهادة Kaspersky Security Center 14 Web Console Server بأخرى مخصصة:

1. على الجهاز الذي تم تثبيت Kaspersky Security Center 14 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.

Kaspersky Security Center Web Console

Client certificate
Select how to specify the certificate.

Generate new certificate
Make sure the below domain is trusted.
Domain:

Choose existing certificate

CRT certificate file:

KEY certificate file:

< Back Next > Cancel

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 14 Web Console مع الشهادة المحددة.

تحديد الشهادات لخوادم الإدارة الموثوقة

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 14 Web Console. وإذا لم يتم فعل ذلك، لن يقدر Kaspersky Security Center 14 Web Console على الاتصال بخادم الإدارة.

في حال تثبيت Kaspersky Security Center 14 Web Console وخادم الإدارة على الجهاز نفسه، يستقبل Kaspersky Security Center 14 Web Console الشهادة الجديدة تلقائيًا. إذا كان Kaspersky Security Center 14 Web Console مثبتًا على جهاز مختلف، يجب أن تحدد المسار المحلي لشهادة خادم الإدارة الجديدة.

لتحديد شهادة جديدة لخادم الإدارة:

1. على الجهاز المثبت عليه خادم الإدارة، انسخ ملف الشهادة إلى جهاز تخزين بمساحة ضخمة مثلًا. بشكل افتراضي، يتم تخزين ملف الشهادة في المجلد التالي:

- 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 14 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 الصفحة الأولى من المعالج، حدد خيار **ترقية**.

5. في صفحة **Modification type** ، حدد خيار **تحرير إعدادات الاتصال**.

6. في صفحة **Trusted Administration Servers** ، حدد خادم الإدارة المطلوب ثم انقر على زر **تحرير**.

7. من الصفحة التي تفتح، انقر على زر **تصفح** وحدد مسار ملف الشهادة الجديدة.
 8. في الصفحة الأخيرة من المعالج، انقر على **تعديل** لتطبيق الإعدادات الجديدة.
 9. بعد اكتمال إعادة تكوين التطبيق بنجاح، انقر على زر **إنهاء**.
 10. **سجل الدخول** إلى Kaspersky Security Center 14 Web Console.
- يعمل Kaspersky Security Center 14 Web Console مع الشهادة المحددة.

تحويل شهادة PFX إلى تنسيق PEM

لاستخدام شهادة PFX في Kaspersky Security Center 14 Web Console، يجب أن تقوم أولاً بتحويلها إلى تنسيق PEM باستخدام أي أداة مساعدة عبر الأنظمة الأساسية تستند إلى 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:

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out server.crt
openssl pkcs12 -in <filename.pfx> -nocerts -nodes -out key.pem
```

نتيجة لذلك، تحصل على مفتاح عام كملف a.crt 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 الحقيقية، فاحذف هذه السمات باستخدام أي محرر نصوص مناسب، ثم احفظ الملف.

4. أعد تشغيل خدمة Windows.

5. لا يدعم Kaspersky Security Center 14 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.

ملفات crt و pem جاهزة للاستخدام، لذا يمكنك تحديد ههما في [أداة تثبيت Kaspersky Security Center 14 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:

```
openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
```

2. تأكد أن ملف الشهادة والمفتاح الخاص تم إنشاؤهما إلى الدليل نفسه الموضوع فيه الملف بامتداد pfx.

3. لا يدعم Kaspersky Security Center 14 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.

ملفات crt و pem جاهزة للاستخدام، لذا يمكنك تحديدهما في [أداة تثبيت Kaspersky Security Center 14 Web Console](#).

التحويل إلى Kaspersky Security Center Cloud Console

يمكنك إجراء التحويل 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 تحويل 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 التحويل، يمكنك إدارة الأجهزة باستخدام Kaspersky Security Center Cloud Console. في الوقت نفسه، يتم الاحتفاظ بالكائنات المنقولة وإعادة تثبيت وكيل الشبكة على جميع الأجهزة المدارة.

للحصول على معلومات حول كيفية إجراء التحويل وقائمة المتطلبات الأساسية، راجع [تعليمات Kaspersky Security Center Cloud Console](#).

تسجيل الدخول إلى Kaspersky Security Center 14 Web Console وتسجيل الخروج

يمكنك تسجيل الدخول إلى Kaspersky Security Center 14 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.

لتسجيل الدخول إلى Kaspersky Security Center 14 Web Console:

1. اذهب إلى <عنوان ويب خادم الإدارة>: <رقم المنفذ>.

سيتم عرض صفحة تسجيل الدخول.

2. إذا أضفت عدة خوادم موثوقة، حدد خادم الإدارة الذي ترغب في الاتصال به في قائمة خوادم الإدارة.

إذا لم تضاف إلا خادم إدارة واحد، لن يتم عرض إلا حقل تسجيل الدخول وكلمة المرور.

3. سجل الدخول باسم المستخدم وكلمة المرور للمدير المحلي.

يتم عرض رسالة خطأ إذا كان خادم الإدارة لا يستجيب أو إذا أدخلت بيانات تسجيل دخول غير صحيحة.

4. بعد الدخول، سيتم عرض لوحة التحكم، وتحتوي على اللغة والسمة اللذين استخدمتهما في آخر مرة.

يمكنك التنقل عبر Kaspersky Security Center 14 Web Console واستخدامه في العمل مع Kaspersky Security Center.

لتسجيل الخروج من Kaspersky Security Center 14 Web Console:

1. انقر على اسم المستخدم في أعلى الزاوية اليمين أو اليسار في الشاشة.

2. في القائمة المنسدلة، حدد تسجيل الخروج.

سيتم إغلاق Kaspersky Security Center 14 Web Console وستظهر صفحة تسجيل الدخول.

إدارة الهوية والوصول في Kaspersky Security Center 14 Web Console

يوفر هذا القسم معلومات حول إدارة الهوية والوصول (يشار إليها أيضًا باسم IAM).

حول إدارة الهوية والوصول

إدارة الهوية والوصول (يشار إليها أيضًا باسم IAM) هو مكون Kaspersky Security Center 14 Web Console يمكنك من استخدام تسجيل الدخول واحد (SSO) بين Kaspersky Security Center 14 Web Console و Kaspersky Industrial CyberSecurity for Networks و Kaspersky Security Center 14 Web Console. يستخدم IAM بروتوكول OAuth 2.0 لضمان إذن من Kaspersky Industrial CyberSecurity for Networks في Kaspersky Security Center 14 Web Console.

في هذه الحالة، يشار إلى Kaspersky Industrial CyberSecurity for Networks، والتي تحصل على الوصول إليها عبر Kaspersky Security Center 14 Web Console، باسم خادم الموارد ويشار إلى كلاً من Kaspersky Security Center 14 Web Console و Kaspersky Industrial CyberSecurity for Networks Console 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 عند تثبيت Kaspersky Security Center 14 Web Console. يمكنك تمكينه لاحقًا في أي وقت في إعدادات Kaspersky Security Center 14 Web Console. إذا تم تثبيت خادم Kaspersky Industrial CyberSecurity for Networks 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 14 Web Console. يمكنك تسجيل Kaspersky Industrial CyberSecurity for Networks واستخدام SSO لاحقًا لكل من Kaspersky Security Center 14 Web Console وواجهة ويب Kaspersky Industrial CyberSecurity for Networks.

إذا قمت بتسجيل الخروج من Kaspersky Security Center 14 Web Console، فستنتهي جلستك في واجهة ويب Kaspersky Industrial CyberSecurity for Networks وسيتم عليك تسجيل الدخول إلى Kaspersky Security Center 14 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.

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 14 Web Console. هذه المنافذ مطلوبة لاستخدام OAuth 2.0. يمكنك تغيير أرقام المنافذ الافتراضية إذا كنت تريد ذلك في نافذة إعدادات [Kaspersky Security Center 14 Web Console](#).

إلى جانب المنافذ 3333 و4004 و4444، يستخدم Kaspersky Security Center 14 Web Console أيضًا المنافذ 2445 و2444 و4445 [لأغراض مختلفة](#).

2 تثبيت إدارة الهوية والوصول

أثناء **تثبيت** Kaspersky Security Center 14 Web Console، حدد أنك تريد تثبيت إدارة الهوية والوصول. إذا لم تفعل ذلك، فقم بتشغيل معالج إعدادات Kaspersky Security Center 14 Web Console مرة أخرى.

3 تكوين إدارة الهوية والوصول

Kaspersky Security Center 14 Web Console في نافذة إعدادات [Kaspersky Security Center 14 Web Console](#)، تأكد من أنه **Identity and Access Manager (IAM)** تم تمكين زر التبديل. حدد أيضًا اسم DNS للجهاز الذي سيتم تثبيت Kaspersky Security Center 14 Web Console عليه: ستتصل تطبيقات العميل بهذا الجهاز.

4 تحديد إعدادات الرمز المميز

في نافذة إعدادات [Kaspersky Security Center 14 Web Console](#)، حدد عمر الرموز المميزة ومهلة التوثيق التي ستستخدمها إدارة 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 14 Web Console](#)، يُرجى تنزيل الشهادات الجذرية للمنافذ التي يستخدمها IAM، ثم توزيعها على محطات عمل مستخدمي Kaspersky Security Center 14 Web Console. بخلاف ذلك، ستعرض مستعرضات المستخدمين رسائل خطأ عند محاولة الاتصال بـ Kaspersky Security Center 14 Web Console.

6 تسجيل Kaspersky Industrial CyberSecurity for Networks لخوادم الشبكات و Kaspersky Industrial CyberSecurity for Networks لواجهات الويب

عند تثبيت IAM، تعرض Kaspersky Security Center 14 Web Console رسالة تفيد بأن خادم Industrial CyberSecurity للشبكات (أو خوادم عدة)، وواحدة أو أكثر من Kaspersky Industrial CyberSecurity for Networks وواجهات الويب 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 و IAM](#) لـ Kaspersky Industrial CyberSecurity for Networks و Kaspersky Security Center 14 Web Console.

تكوين إدارة الهوية والوصول في Kaspersky Security Center 14 Web Console

لتكوين Identity and Access Manager وفقاً لاحتياجاتك:

1. في Kaspersky Security Center 14 Web Console، انتقل إلى قسم إعدادات وحدة التحكم ← التكامل .
2. في قسم Identity and Access Manager تأكد من تفعيل إدارة الهوية والوصول.
3. انقر فوق الرابط إعدادات في اسم شبكة جهاز مثبت عليه Identity and Access Manager الخط.
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 إعدادات الموجود ضمن مجموعة الإعدادات ذات الصلة.

إدارة الهوية والوصول ممكنة وتعمل وفقاً لاحتياجاتك.

تسجيل واجهة ويب Kaspersky Industrial CyberSecurity for Networks في Kaspersky Security Center 14 Web Console

لبدء العمل مع واجهة ويب Kaspersky Industrial CyberSecurity for Networks عبر Kaspersky Security Center 14 Web Console ، يجب عليك أولاً تسجيله في Kaspersky Security Center 14 Web Console.

لتسجيل واجهة ويب Kaspersky Industrial CyberSecurity for Networks:

1. تأكد من القيام بما يلي:

- لقد قمت بتنزيل وتثبيت المكون الإضافي للويب [Kaspersky Industrial CyberSecurity للشبكات](#). (ومع ذلك، يمكنك القيام بذلك لاحقاً أثناء انتظار مزامنة Kaspersky Industrial CyberSecurity لخادم الشبكات 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. لمزيد من التفاصيل، يرجى الرجوع إلى [تعليمات Kaspersky Industrial CyberSecurity للشبكات عبر الإنترنت](#).
- لقد قمت بتسجيل الدخول إلى Kaspersky Security Center 14 Web Console تحت 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 [الاكتشاف والنشر](#) ← الأجهزة غير المخصصة.

b. حدد خانة الاختيار بجوار الجهاز المثبت عليه Kaspersky Industrial CyberSecurity for Networks Server.

c. انقر على زر نقل إلى مجموعة.

d. في التسلسل الهرمي لمجموعات الإدارة، حدد خانة الاختيار بجوار مجموعة الأجهزة المُدارة.

e. انقر فوق الزر نقل.

3. تابع إلى خصائص الجهاز حيث تم تثبيت Kaspersky Industrial CyberSecurity for Networks Server.

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 **مُفعل**.

قد تستغرق هذه العملية حوالي 15 دقيقة. إذا لم تقم بعد بتثبيت المكون الإضافي Kaspersky Industrial CyberSecurity for Networks على الويب، فيمكنك القيام بذلك الآن أثناء انتظارك.

8. في القائمة الرئيسية، انتقل إلى قسم **إعدادات وحدة التحكم** ← **التكامل**.

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 Kaspersky Industrial CyberSecurity for Networks لخادم الشبكات، والذي يتضمن حالة **مُعلق**، ومن ثم انقر فوق الزر **موافقة**.

إذا كنت لا ترغب في تسجيل Kaspersky Industrial CyberSecurity for Networks Server، 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. لوحة معلومات المراقبة والإبلاغ → لوحة المعلومات.

b. في لوحة المعلومات، انقر على زر **إضافة تطبيق الويب المصغر** أو **استعادته**.

c. في قائمة الأدوات التي تفتح، حدد **أخرى**.

d. حدد الأداة 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 ضمن 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 وفقاً 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

الوصف	المهلة الافتراضية (بالثواني)	الرمز المميز
رمز الهوية الذي يستخدمه عميل OAuth 2.0 (أي، إما Kaspersky Security Center 14 Web Console أو Kaspersky Industrial CyberSecurity Console). يُرسل IAM الرمز المميز للمعرف الذي يحتوي على معلومات حول المستخدم (أي ملف تعريف المستخدم) إلى العميل.	86400	رمز الهوية (id_token)
رمز الوصول المستخدم بواسطة العميل OAuth 2.0 للوصول إلى خادم المورد نيابة عن مالك المورد المحدد بواسطة IAM.	86400	رمز الوصول (access_token)
يستخدم العميل OAuth 2.0 هذا الرمز المميز لإعادة إصدار رمز الهوية ورمز الوصول.	172800	رمز التحديث (Refresh_token)

يسرد الجدول أدناه المهلات لرمز المصادقة وlogin_consent_request

إعدادات مهلة المصادقة

الوصف	المهلة الافتراضية (بالثواني)	تعيين
مهلة تبادل الرمز للرمز المميز. يرسل العميل OAuth 2.0 هذا الرمز إلى خادم المورد ويحصل على رمز الوصول في المقابل.	3600	رمز التفويض (auth_code)
انتهت مهلة تفويض حقوق المستخدم للعميل OAuth 2.0	3600	انتهت مهلة طلب الموافقة على تسجيل الدخول (login_consent_request)

لمزيد من المعلومات حول الرموز المميزة، راجع [موقع OAuth](#).

تحميل وتوزيع شهادات IAM

بشكل افتراضي، تستخدم إدارة الهوية والوصول الشهادات التي تم إنشاؤها بواسطة خادم الإدارة لمنح المستعرضات الوصول إلى Kaspersky Security Center 14 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 14 Web Console إلى Kaspersky Security Center 14 Web Console يتقنون بهذه الشهادة.

لتنزيل الشهادات وتوزيعها:

1. في Kaspersky Security Center 14 Web Console، انتقل إلى قسم إعدادات وحدة التحكم ← التكامل .

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 14 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 14 Web Console إلى Kaspersky Security Center 14 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 14 Web Console أو Kaspersky Industrial CyberSecurity Console.

تمنح الشهادات المستخدمين الوصول إلى Kaspersky Security Center 14 Web Console و Kaspersky 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 إنشاؤها من خلال مثبت Kaspersky Security Center 14 Web Console من خلال استخدام المثبت.

تعطيل إدارة الهوية والوصول

إذا كنت ترغب في ذلك، فيمكنك تعطيل Identity and Access Manager (يشار إليه أيضًا باسم IAM).

لتعطيل IAM،

في نافذة إعدادات Kaspersky Security Center 14 Web Console، قم بتبديل زر تبديل IAM إلى معطل.

يمكنك تمكين IAM في أي وقت لاحق.

إذا قمت بتحديث Kaspersky Security Center 14 Web Console عبر المثبت وحددت أنك لا تريد تثبيت IAM، فستتم ترقية Kaspersky Security Center 14 Web Console ولن يتم تثبيت IAM. ستُحذف جميع المعلومات المتعلقة بالتكامل مع Kaspersky Industrial CyberSecurity من جهاز الكمبيوتر الخاص بك، بالإضافة إلى ملفات تكوين IAM وملفات السجل.

تكوين مصادقة المجال باستخدام بروتوكولات NTLM و Kerberos

Kaspersky Security Center 14 يتيح لك استخدام مصادقة المجال في OpenAPI باستخدام بروتوكولي NTLM و Kerberos. استخدام مصادقة المجال يسمح لمستخدم Windows بتمكين المصادقة الآمنة في Kaspersky Security Center 14 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 14 Web Console باستخدام بروتوكول Kerberos. يجب أن يكون لدى المستخدم تذكارة 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 خادم Kaspersky Security Center Web Console على نفس الجهاز حيث تم تثبيت خادم الإدارة.

• يجب عليك تحديد الأسماء الأساسية للخدمة (SPN) التالية لحساب خادم الإدارة:

• "<https/<server.fqnd.name"

• "<https/<server"

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 <serverhost.find.name> أو <serverhost>.

• 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 14. إنها تدعمها في OpenAPI لـ Kaspersky Security Center Linux.

الإعداد الأولي لـ Kaspersky Security Center 14 Web Console

يرد في هذا القسم الخطوات التي يجب عليك اتخاذها بعد تثبيت Kaspersky Security Center 14 Web Console لإجراء الإعداد الأولي.

معالج البدء السريع (Kaspersky Security Center 14 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 14 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 الفيروسات ومهام تنزيل التحديثات ومهام النسخ الاحتياطي للبيانات لأعلى مستوى بالتسلسل الهرمي للأجهزة المُدارة.

معالج البدء السريع لا ينشئ سياسات إلا للتطبيقات التي لا يحتوي مجلد الأجهزة المُدارة فيها على أي سياسات. لا ينشئ معالج البدء السريع أي مهام إذا كان قد تم بالفعل إنشاء مهام بنفس الأسماء لأعلى 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 نافذة التطبيق الرئيسية، انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، قم باختيار قسم عام.

3. انقر فوق بدء معالج البدء السريع.

سيطلبك المعالج بإجراء التكوين الأولي لخادم الإدارة. اتبع إرشادات المعالج. انتقل عبر المعالج من خلال استخدام زر التالي.

الخطوة 1. تحديد إعدادات اتصال الإنترنت

تحديد إعدادات الوصول إلى الإنترنت لـ Kaspersky Security Center.

حدد خانة الاختيار استخدام الخادم الوكيل إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. إذا تم تحديد خانة الاختيار هذه، فستوفر الحقول لإدخال الإعدادات. حدد الإعدادات التالية لاتصال خادم الوكيل:

• العنوان

• رقم المنفذ

• تجاوز الخادم الوكيل للعناوين المحلية ⁵

لن يتم استخدام خادم وكيل للاتصال بالأجهزة في الشبكة المحلية.

• مصادقة الخادم الوكيل ⁶

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 ⁷ (يتوفر هذا الحقل في حالة تحديد خانة الاختيار مصادقة الخادم الوكيل)

حساب المستخدم الذي تم من خلاله إنشاء اتصال بالخادم الوكيل (يكون هذا الحقل متاحًا في حالة تحديد خانة الاختيار مصادقة الخادم الوكيل).

• كلمة المرور ⁸ (يكون هذا الحقل متاحًا في حالة تحديد مربع اختيار 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 الاختيار مصادقة الخادم الوكيل).

لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر إظهار حتى تظهر لك كلمة المرور.

الخطوة 2. جارٍ تنزيل التحديثات المطلوبة

يتم تنزيل التحديثات المطلوبة من خوادم Kaspersky تلقائيًا.

الخطوة 3. تحديد مناطق الحماية والمنصات

حدد مناطق الحماية والمنصات 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 ومخزن الملفات.** 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.
- **الظاهرية.** 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 والاحتتيال وتسليم البرامج الضارة.

• [أنظمة التشغيل](#)

يمكنك تحديد المنصات التالية:

- Microsoft Windows
- Linux
- macOS
- Android

بعد تحديد مناطق الحماية والمنصات، تبدأ مكونات الإدارة الإضافية وحزم التوزيع لتطبيقات Kaspersky في التنزيل تلقائيًا.

الخطوة 4. اختيار التشفير في الحل

لا يتم عرض نافذة التشفير ضمن الحلول إلا إذا قمت بتحديد محطات العمل كمنطقة حماية و Microsoft Windows كمنصة.

يتضمن Kaspersky Endpoint Security for Windows أداة تشفير للمعلومات المخزنة على أجهزة العملاء. التطبيق المُدار يشمل أدوات التشفير التي بها مقياس التشفير المتقدم (AES) مطبقًا مع طول 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. في النافذة **التشفير ضمن الحلول**، حدد أحد أنواع التشفير التالية:

- تشفير قوي. يستخدم هذا النوع من التشفير طول مفتاح 256 بت.
- تشفير لايت. يستخدم هذا النوع من التشفير طول مفتاح 56 بت.

الخطوة 5. تكوين تثبيت المكونات الإضافية للتطبيقات المُدارة

حدد المكونات الإضافية للتطبيقات المُدارة لتثبيتها. تُعرض 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. تتضمن قائمة المكونات الإضافية الأعمدة التالية:

• الاسم

يتم تحديد المكونات الإضافية المعتمدة على المكونات والمنصات، التي حددتها في الخطوة السابقة.

• الإصدار

تتضمن القائمة مكونات إضافية لجميع الإصدارات الموجودة على خوادم Kaspersky. حسب الإعدادات الافتراضية، يتم تحديد المكونات الإضافية لأحدث الإصدارات.

• اللغة

حسب الإعدادات الافتراضية، تُعرّف 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 **التالي** لبدء التثبيت.

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 ثم حدد خانة الاختيار **أوافق على استخدام شبكة Kaspersky Security Network** وانقر على زر **تثبيت**. 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.

تحديثات 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.

لإنهاء تنزيل بعض حزم التوزيع، يجب عليك قبول EULA. عند النقر فوق الزر **أوافق**، يُعرض 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.

الخطوة 8. تكوين Kaspersky Security Network

تحديد الإعدادات لتحميل 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 العملية بنقل تفاصيل عملياته تلقائيًا إلى [Kaspersky Security Network](#). تتضمن 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.

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. لتنشيط التطبيق باستخدام رمز تنشيط، ستحتاج إلى الوصول إلى الإنترنت لإنشاء اتصال مع خوادم تنشيط Kaspersky. إذا قمت بتحديد خيار التنشيط هذا، فيمكنك تمكين خيار **مفتاح ترخيص النشر التلقائي للأجهزة المدارة**. إذا تم تمكين هذا الخيار، فسيتم نشر مفتاح الترخيص تلقائيًا على الأجهزة المدارة. إذا تم تعطيل هذا الخيار، فيمكنك نشر مفتاح الترخيص للأجهزة المدارة 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. تتلقى ملفك الرئيسي عبر عنوان البريد الإلكتروني الذي حددته بعد شراء Kaspersky Security Center. لتنشيط التطبيق باستخدام ملف المفتاح، لا تحتاج إلى الاتصال بخوادم تنشيط Kaspersky. إذا قمت بتحديد خيار التنشيط هذا، فيمكنك تمكين خيار **مفتاح ترخيص النشر تلقائي للأجهزة المُدارة**. 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، يمكنك إضافة مفتاح ترخيص في أي وقت لاحق عن طريق تحديد **العمليات** ← **الترخيص**.

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 **إدارة الثغرات الأمنية والتصحيحات** وكانت مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة موجودة بالفعل.

لتحديثات برامج الأطراف الخارجية، حدد أحد الخيارات التالية:

• [البحث عن تحديثات مطلوبة](#)

تم إنشاء المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. 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.

هذا الخيار غير متاح إلا بموجب **ترخيص إدارة الثغرات الأمنية والتصحيحات**.

لتحديثات Windows Update، حدد أحد الخيارات التالية:

• [استخدم 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.

هذا الخيار غير متاح إلا بموجب [ترخيص إدارة الثغرات الأمنية والتصحيحات](#).

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.

الخطوة 12. تكوين إشعارات البريد الإلكتروني

قم بتكوين تسليم الإخطارات المتعلقة بالأحداث المسجلة أثناء تشغيل تطبيقات Kaspersky على الأجهزة العميلة. وستستخدم 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.

• [عنوان خادم 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. رقم المنفذ الافتراضي هو 25.

• [استخدام مصادقة ESMTP](#)

تمكين دعم مصادقة ESMTP. عند تحديد خانة الاختيار الموجودة في الحقول اسم المستخدم وكلمة المرور، يمكنك تحديد إعدادات مصادقة ESMTP. بشكل افتراضي، يتم إلغاء تحديد هذه الخانة، وتكون إعدادات مصادقة ESMTP غير متوفرة.

• [استخدام TLS](#)

يمكنك تحديد إعدادات TLS للاتصال بخادم SMTP:

• لا تستخدم TLS

يمكنك تحديد هذا الخيار إذا كنت تريد تعطيل تشفير رسائل البريد الإلكتروني.

• استخدم TLS إن 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.

• استخدم TLS دوماً وتحقق من صحة شهادة الخادم

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 للاتصال TLS.

إذا قمت بتحديد قيمة **استخدم TLS دوماً وتحقق من صحة شهادة الخادم** 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 **تحديد الشهادات** :

• 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.

○ حاوية 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**.

الخطوة 13. إجراء استطلاع على الشبكة

يجري خادم الإدارة استطلاعًا أوليًا. سيظهر شريط تقدم أثناء الاستطلاع. سيصبح رابط **عرض الأجهزة المكتشفة** متاحًا بعدما ينتهي الاستطلاع. يمكنك النقر على الرابط لعرض أجهزة الشبكة التي اكتشفها خادم الإدارة. للعودة إلى معالج البدء السريع، انقر على زر **Escape**.

الخطوة 14. إغلاق معالج البدء السريع

في صفحة إكمال معالج البدء السريع، حدد خانة الاختيار **تشغيل معالج نشر الحماية** إذا كنت ترغب في بدء **التثبيت التلقائي** لتطبيقات مكافحة الفيروسات أو عميل الشبكة على الأجهزة الموجودة في شبكتك.

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 الموصولة 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 الموصولة 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.

بشكل افتراضي، يوجد ملف التثبيت في: `<server name>\KLSHARE\PkgInst\NetAgent_<version number>`

في نافذة بوابة الاتصال لمعالج 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 فعلياً ببوابة الاتصال في منطقة الأجهزة الموصولة مباشرة بالإنترنت، اسمح بالاتصالات بمنفذ TCP 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 المدارة. المجموعة الجديدة ستحتوي على الأجهزة المدارة 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 المخصصة إلى المجموعة التي قمت بإنشائها للأجهزة الخارجية.

تم توصيل بوابة الاتصال وتكوينها.

6 **توصيل أجهزة الكمبيوتر المكتبية الخارجية بخادم الإدارة**

في العادة، لا يتم نقل أجهزة الكمبيوتر المكتبية الخارجية داخل المحيط. لذلك أنت بحاجة إلى تكوينها للاتصال بخادم الإدارة من خلال البوابة عند تثبيت عميل الشبكة.

7 **قم بإعداد تحديثات أجهزة الكمبيوتر المكتبية الخارجية**

إذا تم تكوين تحديثات تطبيقات الأمان بحيث يتم تنزيلها من خادم الإدارة، فستقوم أجهزة الكمبيوتر 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 الأسرع والأسهل أن تتلقى أجهزة الكمبيوتر الخارجية التحديثات من خوادم Kaspersky.

قم بما يلي:

1. انقل جميع أجهزة الكمبيوتر الخارجية إلى مجموعة الإدارة المنفصلة التي قمت بإنشائها مسبقًا.

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 و أوصاف موقع الشبكة. تحدد كل قاعدة خادم الإدارة الذي يلزم اتصاله بأجهزة الكمبيوتر المحمولة المتنقلة بناءً على موقعها وخادم الإدارة الذي يتطلب تلقي التحديثات منه.

حول توصيل الأجهزة خارج المكتب

دائمًا ما تقع بعض الأجهزة المدارة خارج نطاق الشبكة الرئيسية (على سبيل المثال، أجهزة الكمبيوتر في الفروع الإقليمية للشركة؛ الأكشاك وأجهزة الصراف الآلي والمحطات الطرفية المثبتة في نقاط البيع المختلفة؛ أجهزة الكمبيوتر 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 الموصولة 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 الموصولة مباشرة بالإنترنت

اطلع على نظام حركة مرور البيانات: خادم الإدارة في منطقة الأجهزة الموصولة مباشرة بالإنترنت والأجهزة المدارة على الإنترنت

بوابة اتصال في منطقة الأجهزة الموصولة مباشرة بالإنترنت

الطريقة الموصى بها لتوصيل الأجهزة الموجودة خارج المكتب بخادم الإدارة هي تنظيم منطقة الأجهزة الموصولة 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 فعلياً ولا تنشئ أي اتصالات.

ولا تتطلب بوابة الاتصال أيضاً توفر العديد من موارد الأجهزة.

ومع ذلك، فإن هذه الطريقة بها عملية تكوين أكثر تعقيداً:

- لجعل جهاز يعمل كبوابة اتصال في منطقة الأجهزة الموصولة 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 أيضاً استخدام وضع اتصال مختلف: من خلال بوابة الاتصال.
- كما يتطلب منك تحديد إعدادات اتصال مختلفة لأجهزة الكمبيوتر المحمولة في مواقع مختلفة.

خادم الإدارة في منطقة الأجهزة الموصولة مباشرة بالإنترنت

هناك طريقة أخرى وهي تثبيت خادم إدارة واحد في منطقة الأجهزة الموصولة مباشرة بالإنترنت.

هذا التكوين أقل أماناً 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، ولكن من منطقة الأجهزة الموصولة 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 الموصولة 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 معتاداً 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 100000 جهاز، بينما يمكن لبوابة الاتصال أن تدعم ما يصل إلى 10000 جهاز.

لهذا الحل أيضاً 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 الموصولة مباشرة بالإنترنت)، مما يعقد المراقبة.
- لإدارة جميع الأجهزة، يجب ضم خادم الإدارة في شكل تسلسل هرمي، مما يعقد المراقبة وكذلك الإدارة. يفرض مثل خادم الإدارة الثانوي قيوداً على الهياكل المحتملة لمجموعات الإدارة. عليك أن تقرر طريقة وماهية المهام والسياسات لتوزيعها على مثل خادم الإدارة الثانوي.
- يعد تكوين الأجهزة الخارجية لاستخدام خادم الإدارة في منطقة الأجهزة الموصولة مباشرة بالإنترنت من الخارج واستخدام خادم الإدارة الرئيسي من الداخل معقداً أكثر من مجرد تكوينها لاستخدام اتصال مشروط من خلال بوابة.
- مخاطر أمنية عالية. يُعرض مثل 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 أجهزة الكمبيوتر المكتبية الخارجية بخادم الإدارة

لا يمكن توصيل أجهزة الكمبيوتر المكتبية التي دائماً ما تكون خارج الشبكة الرئيسية (على سبيل المثال، أجهزة الكمبيوتر في الفروع الإقليمية للشركة؛ الأكتشاك وأجهزة الصراف الآلي والمحطات الطرفية المثبتة في نقاط البيع المختلفة؛ أجهزة الكمبيوتر في المكاتب المنزلية للموظفين) بخادم الإدارة مباشرة. يجب أن تكون متصلة بخادم الإدارة عبر بوابة اتصال مثبتة في منطقة الأجهزة الموصولة مباشرة بالإنترنت (DMZ). يتم إجراء هذا التكوين عند تثبيت عميل الشبكة على تلك الأجهزة.

لتوصيل أجهزة الكمبيوتر المكتبية الخارجية بخادم الإدارة:

1. قم بإنشاء حزمة تثبيت جديدة لعميل الشبكة.

2. افتح خصائص حزمة التثبيت التي تم إنشاؤها، وانتقل إلى إعدادات ← خيارات متقدمة، ومن ثم حدد الخيار 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 الحقل 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 لأجهزة الكمبيوتر المستهدفة إما إلكترونياً أو على محرك أقراص قابل للإزالة.

6. قم بتثبيت عميل الشبكة من الحزمة المستقلة.

أجهزة الكمبيوتر 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 إنترنت 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.

لقيام بذلك، أضف ملف تعريف للاتصال بخادم الإدارة من الإنترنت في خصائص سياسة عميل الشبكة (في القسم إعدادات التطبيق ← الشبكة ← ملفات تعريف الاتصال ← ملفات تعريف اتصال خادم الإدارة). في نافذة إنشاء ملف التعريف، عليك تعطيل خيار الاستخدام لاستلام التحديثات فقط، وتأكد من تحديد 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 DMZ](#))، 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 المثبت 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 **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. 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 **الأجهزة** ← **السياسات وملفات التعريف**.

b. انقر على رابط المسار الحالي.

c. في النافذة التي تفتح، حدد مجموعة الإدارة المطلوبة.

بعد ذلك، يتم تغيير المسار الحالي.

d. أضف سياسة وكيل 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 مدار معين، فقم بما يلي:

a. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **الأجهزة المدارة**.

b. انقر على اسم الجهاز المدار.

c. في نافذة خصائص الجهاز المدار التي تفتح، انتقل إلى علامة التبويب **التطبيقات**.

d. انقر فوق اسم سياسة عميل الشبكة التي تنطبق على الجهاز المدار المحدد.

3. في نافذة الخصائص التي تفتح، انتقل إلى **إعدادات التطبيق** ← **الشبكة** ← **ملفات تعريف الاتصال**.

4. من القسم **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 ذلك، الاتصال بأي خادم إدارة بينما تعمل التطبيقات المثبتة على الأجهزة العملية 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 وكيل 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 **تكوين ملف التعريف** التي تفتح، قم بتكوين ملف تعريف الاتصال:

• **تكوين ملف التعريف**

يمكنك من خلال حقل الإدخال عرض اسم ملف تعريف الاتصال وتغييره.

• **عنوان خادم الإدارة**

عنوان خادم الإدارة الذي يجب توصيل الجهاز العميل به أثناء تفعيل ملف التعريف.

• **رقم المنفذ**

رقم المنفذ المستخدم في الاتصال.

• **منفذ SSL**

رقم المنفذ الخاص بالاتصال في حالة استخدام بروتوكول SSL.

• **استخدام اتصال 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 اتصالاتك آمنًا.

• 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.

• **مصادقة الخادم الوكيل**

إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

• **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.

• **عنوان بوابة الاتصال**

عنوان البوابة التي من خلالها يتم اتصال الأجهزة العميلة بخادم الإدارة.

• **تمكين وضع الوجود خارج المكتب عندما يكون خادم الإدارة غير متاح**

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:

- **شروط عنوان خادم DHCP**—تم تغيير عنوان IP الخاص بخادم بروتوكول تكوين المضيف الديناميكي (DHCP) الخاص بالشبكة.
- **شروط عنوان بوابة الاتصال الافتراضية**—تم تغيير عنوان بوابة الشبكة الرئيسية.
- **شروط مجال نظام أسماء النطاقات (DNS)**—تم تغيير لاحقة DNS للشبكة الفرعية.
- **شروط عنوان خادم DNS**—تم تغيير عنوان IP الخاص بخادم DNS للشبكة.
- **شروط عنوان خادم WINS**—تم تغيير عنوان IP الخاص بخادم WINS للشبكة. هذا الإعداد متاح فقط للأجهزة التي تعمل بنظام Windows.

- شرط إمكانية تحليل الاسم-تم تغيير اسم DNS أو NetBIOS للجهاز العميل.
- حالة الشبكة الفرعية – تغيير عنوان الشبكة الفرعية والقناع.
- شرط إمكانية الوصول إلى مجال Windows – تغيير حالة مجال Windows الذي يتصل به الجهاز العميل. هذا الإعداد متاح فقط للأجهزة التي تعمل بنظام Windows.
- شرط 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 عميل 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 إذا 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 و macOS.

لإنشاء قاعدة لتبديل عميل الشبكة من خادم إدارة إلى آخر في حالة تغيير إعدادات الشبكة:

1. إذا أردت إنشاء قاعدة لمجموعة أجهزة مدار، فافتح سياسة عميل الشبكة لهذه المجموعة. للقيام بذلك، عليك القيام بالإجراءات التالية:

a. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **السياسات وملفات التعريف**.

b. انقر على رابط المسار الحالي.

c. في النافذة التي تفتح، حدد مجموعة الإدارة المطلوبة.

بعد ذلك، يتم تغيير المسار الحالي.

d. أضف سياسة وكيل الشبكة لمجموعة الأجهزة المدار. 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 **الأجهزة** ← **الأجهزة المُدارة**.

b. انقر على اسم الجهاز المُدار.

c. في نافذة خصائص الجهاز المُدار التي تفتح، انتقل إلى علامة التبويب **التطبيقات**.

d. انقر فوق اسم سياسة عميل الشبكة التي تنطبق على الجهاز المُدار المُحدد.

3. في نافذة الخصائص التي تفتح، انتقل إلى **إعدادات التطبيق** ← **الشبكة** ← **ملفات تعريف الاتصال**.

4. في القسم **إعدادات موقع الشبكة**، انقر على زر **إضافة**.

5. في نافذة الخصائص التي تفتح، قم بتكوين وصف موقع الشبكة وقاعدة التبدل. حدد إعدادات وصف موقع الشبكة التالية:

• **الوصف** 9

لا يمكن أن يكون اسم وصف موقع الشبكة أطول من 255 حرف أو يحتوي على رموز خاصة، مثل ("*\?/|:").

• **استخدم ملف تعريف الاتصال** 9

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 العملية إلى سياسات خارج المكتب. يتم استخدام ملف التعريف لتنزيل التحديثات فقط.

• **تم تمكين الوصف** 9

حدد خانة الاختيار هذه لتمكين استخدام وصف موقع الشبكة الجديد.

6. حدد شروط قاعدة تبديل وكيل الشبكة:

• **شرط عنوان خادم DHCP**—تم تغيير عنوان IP الخاص بخادم بروتوكول تكوين المضيف الديناميكي (DHCP) الخاص بالشبكة.

• **شرط عنوان بوابة الاتصال الافتراضية**—تم تغيير عنوان بوابة الشبكة الرئيسية.

• **شرط مجال نظام أسماء النطاقات (DNS)**—تم تغيير لاحقة DNS للشبكة الفرعية.

• **شرط عنوان خادم DNS**—تم تغيير عنوان IP الخاص بخادم DNS للشبكة.

• **شرط عنوان خادم WINS**—تم تغيير عنوان IP الخاص بخادم WINS للشبكة. هذا الإعداد متاح فقط للأجهزة التي تعمل بنظام Windows.

• **شرط إمكانية تحليل الاسم**—تم تغيير اسم DNS أو NetBIOS للجهاز العميل.

• **حالة الشبكة الفرعية**— تغيير عنوان الشبكة الفرعية والقناع.

• **شرط إمكانية الوصول إلى مجال Windows**— تغيير حالة مجال Windows الذي يتصل به الجهاز العميل. هذا الإعداد متاح فقط للأجهزة التي تعمل بنظام Windows.

• **شرط 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 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 التبدل حسب وصف موقع الشبكة، يجب استيفاء شروطها.

7. في قسم الشروط، حدد متى يجب تبديل وكيل الشبكة إلى خادم إدارة آخر. لهذا الغرض، انقر فوق الزر **"إضافة"**، ومن ثم قم بتعيين قيمة الشرط.

كما يجب تمكين الخيار **تطابق قيمة واحدة على الأقل من القائمة** 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 بالإجراءات التالية:

- تنزيل حزمة تثبيت لتثبيت التطبيق (إذا لم يتم الإنشاء مسبقاً). توجد حزمة التثبيت في **الاكتشاف والنشر ← التوزيع والتعيين ← حزم التثبيت**. 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 حديثاً في قسم **المهام**. يمكنك بدء هذه المهمة يدوياً لاحقاً. نوع المهمة هو **تثبيت التطبيق عن بُعد**.

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.

بدء معالج نشر الحماية

ليبدء معالج نشر الحماية يدوياً،

في نافذة التطبيق الرئيسية، انقر على **الاكتشاف والنشر ← التوزيع والتعيين ← معالج نشر الحماية**.

سيبدأ معالج نشر الحماية. انتقل عبر المعالج من خلال استخدام زر التالي.

الخطوة 1. تحديد حزمة التثبيت

حدد حزمة التثبيت للتطبيق الذي ترغب في تثبيته.

إذا لم تكن حزمة التثبيت للتطبيق المطلوب مدرجة، انقر على زر **إضافة** ثم حدد التطبيق من القائمة.

الخطوة 2. تحديد طريقة لتوزيع ملف المفتاح أو رمز التنشيط

حدد طريقة لتوزيع ملف المفتاح أو رمز التنشيط:

- **لا تتم بإضافة المفتاح إلى حزمة التثبيت** [5]

- يتم توزيع المفتاح تلقائيًا على كافة الأجهزة التي يتوافق معها:
- في حالة تمكين [التوزيع التلقائي](#) في خصائص المفتاح
- إذا تم إنشاء مهمة [إضافة مفتاح](#).

• [إضافة المفتاح إلى حزمة التثبيت](#) 9

يتم توزيع المفتاح على الأجهزة بالإضافة إلى حزمة التثبيت.

لا نوصي بقيامك بتوزيع المفتاح باستخدام هذه الطريقة؛ لأن وصول القراءة المشترك ممكن لمستودع الحزم.

إذا كانت حزمة التثبيت تشمل ملف مفتاح أو رمز تنشيط بالفعل، ستظهر النافذة لكن لن تحتوي إلا على تفاصيل مفتاح الترخيص.

الخطوة 3. 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 4. تحديد الأجهزة

حدد قائمة بالأجهزة التي سيتم تثبيت التطبيق عليها:

• [التثبيت على الأجهزة المُدارة](#) 9

إذا تم تحديد هذا الخيار، فسوف يتم إنشاء مهمة التثبيت عن بُعد لمجموعة أجهزة.

• [تحديد أجهزة للتثبيت](#) 9

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 5. تحديد إعدادات مهمة التثبيت عن بُعد

في صفحة 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 العملية:

• [استخدام عميل الشبكة](#) 9

إذا كان هذا الخيار مفعلاً، سيتم تسليم حزم التثبيت إلى الأجهزة العملية بواسطة عميل الشبكة المثبت على الأجهزة العملية هذه. في حال تعطيل هذا الخيار، سيتم تسليم حزم التثبيت باستخدام أدوات Microsoft Windows. ننصح بتفعيل هذا الخيار إذا تم تعيين المهمة إلى الأجهزة المثبت عليها عملاء الشبكة. يتم تمكين هذا الخيار افتراضياً.

• استخدام موارد النظام التشغيل عبر نقاط التوزيع 5

إذا تم تفعيل هذا الخيار، سيتم نقل حزم التثبيت إلى الأجهزة العملية 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 افتراضياً لمهام التثبيت عن بُعد التي تم إنشاؤها على خادم إدارة افتراضي.

• استخدام موارد نظام التشغيل من خلال خادم الإدارة 5

إذا تم تفعيل هذا الخيار، سيتم نقل الملفات إلى أجهزة الكمبيوتر العملية باستخدام أدوات Microsoft Windows عبر 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 افتراضياً.

حدد الإعدادات الإضافية:

• لا تقم بإعادة تثبيت التطبيق إذا كان مثبتاً بالفعل 5

إذا تم تفعيل هذا الخيار، لن يتم عادة تثبيت التطبيق المحدد إذا كان مثبتاً بالفعل على الجهاز العميل هذا. إذا تم تفعيل هذا الخيار، سيتم تثبيت التطبيق بأية حال. يتم تمكين هذا الخيار افتراضياً.

• تعيين تثبيت الحزمة في سياسات مجموعة Active Directory 5

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 افتراضياً.

الخطوة 6. إدارة إعادة التشغيل

حدد الإجراء الذي يجب إتمامه إذا كان يجب إعادة تشغيل نظام التشغيل عند تثبيتك للتطبيق:

• لا تقم بإعادة تشغيل الجهاز 5

لم تتم إعادة تشغيل أجهزة العميل تلقائياً بعد عملية التشغيل. لإكمال العملية، يجب عليك إعادة تشغيل الجهاز (على سبيل المثال، يدوياً 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 أمراً بالغ الأهمية.

• أعد تشغيل الجهاز 9

يتم إعادة تشغيل الأجهزة العملية 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 9

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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضيًا.

• تكرار المطالبة كل (بالدقائق) 9

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) 9

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 9

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 المستخدمون 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 7. 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 8. نقل الأجهزة إلى الأجهزة المُدارة

حدد إذا ما كان يجب نقل الأجهزة إلى مجموعة إدارة بعد تثبيت عميل الشبكة أم لا.

• عدم نقل الأجهزة ⑨

تبقى الأجهزة في المجموعات الموجودة فيها حاليًا. والأجهزة التي لم يتم وضعها في مجموعة تبقى دون تخصيص.

• نقل الأجهزة غير المخصصة إلى مجموعة ⑩

يتم نقل الأجهزة إلى مجموعة الإدارة التي تحددها.

يتم تحديد خيار **عدم نقل الأجهزة** بصورة افتراضية. ولأسباب أمنية، قد ترغب في نقل الأجهزة يدويًا.

الخطوة 9. تحديد الحسابات للوصول إلى الأجهزة

أضف الحسابات التي سيتم استخدامها لبدء مهمة التثبيت عن بُعد:

• لا يلزم وجود حساب (تم تثبيت عميل الشبكة) ⑪

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 كيل الشبكة على الأجهزة العملية، فلن يتوفر هذا الخيار.

• يلزم وجود حساب (عميل الشبكة غير مستخدم) ⑫

إذا تم تحديد هذا الخيار، فيمكنك تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. يمكنك تحديد الحساب إذا لم يتم تثبيت عميل الشبكة على الأجهزة التي تم تعيين المهمة لها. يمكنك تحديد حسابات مستخدمين متعددة، على سبيل المثال، في حالة عدم امتلاك أي منها لجميع الحقوق الموضحة على جميع الأجهزة التي تم تحديد هذه المهمة من أجلها. في هذه الحالة، يتم استخدام جميع الحسابات التي تمت إضافتها لتشغيل المهمة بترتيب متعاقب من الأعلى إلى الأسفل. في حالة عدم إضافة أي حساب، سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

الخطوة 10. بدء التثبيت

هذه الصفحة هي الخطوة الأخيرة من المعالج. في هذه الخطوة، تم إنشاء مهمة التثبيت عن بُعد وتكوينه بنجاح.

يكون خيار تشغيل المهمة بعد انتهاء المعالج غير محدد بصورة افتراضية. إذا حددت هذا الخيار، فسيبدأ مهمة التثبيت عن بُعد فورًا بعد إكمال المعالج. إذا لم تحدد هذا الخيار، لن يبدأ مهمة التثبيت عن بُعد. يمكنك بدء هذه المهمة يدويًا لاحقًا.

تكوين خادم الإدارة

يصف هذا القسم عملية التكوين وخصائص خادم إدارة Kaspersky Security Center.

تكوين اتصال Kaspersky Security Center 14 Web Console بخادم الإدارة

لتعيين منافذ التوصيل لخادم الإدارة:

1. في أعلى الشاشة، انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، حدد قسم منافذ الاتصال.

يعرض التطبيق إعدادات التوصيل الرئيسي للخادم المحدد.

في الإصدارات السابقة من Kaspersky Security Center، كان يتم توصيل وحدة تحكم الإدارة بخادم الإدارة عبر منفذ TCP 13291 SSL ومنفذ TCP 13000. وابتداءً من الحزمة Kaspersky Security Center 10 Service Pack 2، يتم استخدام منافذ SSL بواسطة التطبيق بصورة منفصلة تمامًا وأصبح من المستحيل إساءة استعمال المنافذ:

- لا يمكن استخدام منفذ طبقة مأخذ التوصيل الأمانة TCP 13291 إلا بواسطة وحدة تحكم الإدارة.
- لا يمكن استخدام منفذ SSL TCP 13000 إلا بواسطة عميل الشبكة وخادم الإدارة الثانوي وخادم الإدارة الرئيسي في منطقة DMZ.
- يمكن استخدام منفذ TCP 14000 للاتصال بوحدة تحكم الإدارة ونقاط التوزيع وخوادم الإدارة الثانوية، بالإضافة إلى تلقي البيانات من أجهزة العملاء.

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 داخل البنية الأساسية لشبكتك، ولكن أيضًا المحاولات غير المصرح بها للوصول إلى الخادم.

لتسجيل أحداث الاتصال بخادم الإدارة:

1. في نافذة التطبيق الرئيسية، انقر فوق أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، حدد قسم منافذ الاتصال.

3. قم بتفعيل خيار تسجيل أحداث الاتصال بخادم الإدارة.

سيتم حفظ جميع الأحداث الأخرى للاتصالات الواردة إلى خادم الإدارة، ونتائج المصادقة، وأخطاء SSL في ملف
ProgramData%\KasperskyLab\admindkit\logs\sc.syslog%

تعيين الحد الأقصى لعدد الأحداث في مستودع الأحداث

من القسم **مستودع الأحداث** في نافذة خصائص خادم الإدارة، يمكنك تحرير إعدادات تخزين الأحداث في قاعدة بيانات خادم الإدارة من خلال تعيين 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.

إذا وصل عدد الأحداث في قاعدة البيانات إلى الحد الأقصى المحدد من قبل المسؤول، فيقوم التطبيق بحذف الأحداث الأقدم ويعيد أحداث جديدة عليها. 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.

لتعيين عدد الأحداث التي يمكن تخزينها في مستودع الأحداث بخادم الإدارة:

1. في أعلى الشاشة، انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.
2. في علامة التبويب عام، حدد قسم **مستودع الأحداث**.
3. حدد الحد الأقصى لعدد الأحداث المخزنة في قاعدة البيانات.
4. انقر على زر **حفظ**.
يتم تعيين عدد الأحداث التي يمكن تخزينها في قاعدة البيانات إلى القيمة المحددة.

إعدادات الاتصال لأجهزة حماية UEFI

جهاز حماية UEFI هو جهاز مثبت عليه Kaspersky Anti-Virus for UEFI متكامل 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:

في نافذة التطبيق الرئيسية، انقر فوق أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

1. في علامة التبويب عام، حدد قسم **منافذ إضافية**.

2. 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.

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 14 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 خوادم الإدارة.
4. حدد خانة الاختيار الموجودة بجوار اسم مجموعات الإدارة التي ترغب في إضافة خادم الإدارة إليها.
5. في سطر القائمة، انقر على توصيل خادم الإدارة الثانوي.
يبدأ عمل معالج توصيل خادم إدارة تابع.
6. في الصفحة الأولى من المعالج، املا الحقول التالية:

• اسم عرض خادم الإدارة الثانوي ⓘ

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".

• عنوان خادم الإدارة الثانوي (اختياري) ⓘ

حدد عنوان IP أو اسم النطاق لخادم الإدارة الثانوي.

• منفذ SSL لخادم الإدارة ⓘ

حدد رقم منفذ SSL على خادم الإدارة الرئيسي. رقم المنفذ الافتراضي هو 13000.

• منفذ API لخادم الإدارة ⓘ

حدد رقم المنفذ على خادم الإدارة الرئيسي لتلقي الاتصالات عبر OpenAPI. رقم المنفذ الافتراضي هو 13299.

• توصيل خادم الإدارة الأساسي بخادم الإدارة الثانوي في DMZ ⓘ

حدد هذا الخيار إذا كان خادم الإدارة الثانوي في منطقة الأجهزة الموصولة مباشرة بالإنترنت (DMZ).

حدد هذا الخيار إذا كنت تستخدم خادم وكيل للاتصال بخادم الإدارة الثانوي. في هذه الحالة، ستحتاج كذلك إلى تحديد الإعدادات التالية للخادم الوكيل:

- العنوان
- اسم المستخدم
- كلمة المرور

7. اتبع باقي إرشادات المعالج.

بعد أن ينتهي المعالج، سيتم بناء التسلسل الهرمي "رئيسي/تابع". سيبدأ خادم الإدارة الرئيسي في تلقي الاتصال من خادم الإدارة الثانوي عبر منفذ 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 مؤقتاً مثلاً)، لا يزال بإمكانك إضافة خادم إدارة تابع.

لإضافة خادم إدارة تابع غير متوفر للتوصيل عبر Kaspersky Security Center 14 Web Console:

1. إرسال ملف الشهادة لخادم الإدارة الرئيسي المستقبلي إلى مدير النظام في المكتب الذي يوجد به خادم الإدارة الثانوي المستقبلي. (يمكنك على سبيل المثال كتابة الملف إلى جهاز خارجي مثل محرك أقراص محمول 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. تنقر على أيقونة الإعدادات (⚙️).

b. في صفحة الخصائص التي تفتح، انتقل إلى قسم التسلسل الهرمي لخوادم الإدارة من تبويب عام.

c. حدد خيار خادم الإدارة هذا ثانوي في التسلسل الهرمي

d. في حقل عنوان خادم الإدارة الأساسي، أدخل اسم شبكة خادم الإدارة الرئيسي المستقبلي.

e. حدد الملف الذي تم حفظه سابقاً والذي يحتوي على شهادة خادم الإدارة المستقبلي عن طريق النقر على استعراض.

f. حدد خانة الاختيار توصيل خادم الإدارة الأساسي بخادم الإدارة الثانوي في DMZ إذا كان ذلك ضرورياً.

g. في حال إجراء الاتصال بخادم الإدارة الثانوي المستقبلي عبر خادم وكيل، حدد خيار استخدام الخادم الوكيل وحدد إعدادات الاتصال.

h. انقر فوق حفظ.

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 نافذة التطبيق الرئيسية، انقر على اسم خادم الإدارة الذي يوجد 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 أيضاً، ولكنها تظهر باللون الرمادي وغير متوفرة في الإدارة في هذه القائمة.

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 أعلى الشاشة، انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة الرئيسي.

2. في الصفحة التي تفتح، انتقل إلى تبويب **خوادم الإدارة**.

3. حدد خادم الإدارة الثانوي في مجموعة الإدارة التي ترغب في حذف خادم الإدارة الثانوي منها.

4. في سطر القائمة، انقر فوق **حذف**.

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 خفض حجم قاعدة البيانات، وتحسين أداء التطبيق ومصادقته 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 فهرس قاعدة البيانات.
- تحديث إحصائيات قاعدة البيانات.
- تقليص قاعدة البيانات (إذا لزم الأمر).

مهمة صيانة خادم الإدارة لا تدعم MariaDB. في حالة استخدام خادم DBMS هذا في شبكتك، فسيُتعين على المسؤولين صيانة MariaDB بأنفسهم.

يتم إنشاء مهمة صيانة خادم الإدارة تلقائيًا عند تثبيت Kaspersky Security Center. إذا تم حذف مهمة صيانة خادم الإدارة، يمكنك إنشاؤها يدويًا.

لإنشاء مهمة صيانة خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

2. انقر فوق الزر **إضافة**.

يبدأ تشغيل إضافة معالج المهمة.

3. في نافذة **مهمة جديدة** من المعالج، حدد **صيانة خادم الإدارة** كنوع المهمة وانقر فوق الزر **التالي**.

4. اتبع بقية إرشادات المعالج.

يتم عرض المهمة التي يتم إنشاؤها في قائمة المهام. يمكن تشغيل مهمة صيانة خادم الإدارة واحدة فقط لخادم إدارة واحد. إذا تم بالفعل إنشاء مهمة صيانة خادم الإدارة لخادم الإدارة، فلا يمكن إنشاء مهمة صيانة خادم الإدارة الجديدة.

تكوين الواجهة

يمكنك تكوين واجهة Kaspersky Security Center 14 Web Console لعرض أقسام وعناصر الواجهة وإخفائها، حسب المزايا المستخدمة.

لتكوين واجهة Kaspersky Security Center 14 Web Console وفقًا لمجموعة المزايا المستخدمة حاليًا:

1. في نافذة التطبيق الرئيسية، انقر فوق قائمة الحساب.

2. في القائمة المنسدلة، حدد خيارات الواجهة.

3. في نافذة خيارات الواجهة التي تفتح، قم بتفعيل خيار عرض تشفير البيانات وحمايتها أو تعطيله.

4. انقر فوق حفظ.

تعرض الوحدة قسم تشفير البيانات وحمايتها.

إدارة خوادم الإدارة الافتراضية

يصف هذا القسم الإجراءات التالية لإدارة خوادم الإدارة الافتراضية:

- [إنشاء خوادم الإدارة الافتراضية](#)
- [تمكين وتعطيل خادم الإدارة الافتراضية](#)
- [حذف خوادم الإدارة الافتراضية](#)
- [تغيير خادم الإدارة للأجهزة العميلة](#)

إنشاء خادم إدارة افتراضي

يمكنك إنشاء [خوادم إدارة ظاهرية](#) وإضافتها إلى مجموعات الإدارة.

لإنشاء خادم إدارة افتراضي وإضافته:

1. في نافذة التطبيق الرئيسية، انقر فوق أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.

2. في الصفحة التي تفتح، انتقل إلى تبويب [خوادم الإدارة](#).

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).

في سطر القائمة، انقر على [خادم إدارة افتراضي جديد](#).

1. في الصفحة التي تفتح، حدد خصائص خادم الإدارة الافتراضي الجديد:

- اسم خادم الإدارة الافتراضي.
 - عنوان الاتصال بخادم الإدارة
- يمكنك تحديد اسم وعنوان IP لخادم الإدارة.

2. 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.

3. انقر فوق حفظ.

يتم إنشاء خادم الإدارة الافتراضي الجديد وإضافته إلى مجموعة الإدارة وعرضه في تبويب خوادم الإدارة.

تمكين وتعطيل خادم إدارة افتراضي

عند إنشاء خادم إدارة افتراضي جديد، يتم تمكينه افتراضياً. 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 نافذة التطبيق الرئيسية، انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.

2. في الصفحة التي تفتح، انتقل إلى تبويب خوادم الإدارة.

3. حدد خادم الإدارة الافتراضي الذي تريد تمكينه أو تعطيله.

4. في سطر القائمة، انقر على زر تمكين / تعطيل خادم الإدارة الظاهري.

يتم تغيير حالة خادم الإدارة الافتراضي إلى ممكّن أو معطل، بناءً على حالته السابقة. يتم عرض الحالة المحدثة بجوار اسم خادم الإدارة.

حذف خادم إدارة افتراضي

عند حذف خادم إدارة افتراضي، سيتم أيضاً 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 نافذة التطبيق الرئيسية، انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.

2. في الصفحة التي تفتح، انتقل إلى تبويب خوادم الإدارة.

3. حدد خادم الإدارة الافتراضي الذي تريد حذفه.

4. في سطر القائمة، انقر على زر حذف.

تم حذف خادم الإدارة الافتراضي.

تغيير خادم الإدارة للأجهزة العملية

يمكنك تغيير خادم الإدارة الذي يدير الأجهزة العملية إلى خادم مختلف باستخدام مهمة تغيير خادم الإدارة. بعد اكتمال المهمة، سيتم وضع الأجهزة العملية المحددة تحت إدارة خادم الإدارة الذي تحدده. يمكنك تبديل إدارة الجهاز بين خوادم الإدارة التالية:

- خادم الإدارة الأساسي وأحد خوادم الإدارة الافتراضية الخاصة به
- اثنين من خوادم الإدارة الافتراضية لنفس خادم الإدارة الأساسي

لتغيير خادم الإدارة الذي يدير الأجهزة العملية بخادم آخر:

1. في نافذة التطبيق الرئيسية، اذهب إلى الأجهزة ← المهام.

2. انقر فوق إضافة.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر التالي.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة تغيير خادم الإدارة.

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 خادم الإدارة الذي تريد استخدامه لإدارة الأجهزة المحددة.

7. حدد الإعدادات التالية:

• الحساب الافتراضي

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه. يتم تحديد هذا الخيار افتراضياً.

• تحديد حساب

املاً حقل الحساب وكلمة 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. إذا قمت بتفعيل خيار فتح تفاصيل المهمة عند اكتمال الإنشاء على صفحة إنهاء عملية إنشاء المهمة، يمكنك تعديل إعدادات المهمة الافتراضية. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقاً في أي وقت.

9. انقر على زر إنهاء.

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 وفقاً لاحتياجاتك.

12. انقر على زر حفظ.

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.

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 **المستخدمون والأدوار** ← **المستخدمون**.
 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 **حماية الحساب**.
 4. في تبويب **حماية الحساب**، 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.

المصادقة الثنائية

يصف هذا القسم كيفية استخدام المصادقة الثنائية لتقليل مخاطر الوصول غير المصرح به إلى Kaspersky Security Center 14 Web Console.

السيناريو: تكوين المصادقة الثنائية 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 أيضاً 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 تبدأ:

- 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 قيام المستخدمين الآخرين لخادم الإدارة بتثبيت تطبيق مصدق على أجهزتهم.

المراحل

تمكين المصادقة الثنائية لجميع المستخدمين يتم في مراحل:

1 تثبيت تطبيق مصادقة على جهاز

يمكنك تثبيت Google Authenticator أو Microsoft Authenticator أو أي تطبيق مصادقة آخر يدعم خوارزمية كلمة المرور لمرة واحدة المستندة إلى الوقت.

2 مزامنة وقت تطبيق المصادقة مع وقت الجهاز المثبت عليه خادم الإدارة.

تأكد من أن الوقت المحدد في تطبيق المصادقة متزامن مع وقت خادم الإدارة.

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 14 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 لـ Kaspersky Security Center 14 Web Console: [تمكين المصادقة الثنائية لجميع المستخدمين](#)

5 تحرير اسم مُصدر 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 مُصدر رمز الأمان](#)

○ بالنسبة لـ Kaspersky Security Center 14 Web Console: [تحرير اسم مُصدر 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 لـ Kaspersky Security Center 14 Web Console: [استثناء الحسابات من المصادقة الثنائية](#)

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

يوفر Kaspersky Security Center 14 Web Console التحقق من خطوتين لمستخدمي Kaspersky Security Center 14 Web Console. عند تمكين المصادقة الثنائية لحسابك الخاص، في كل مرة تقوم فيها بتسجيل الدخول إلى Kaspersky Security Center 14 Web Console، 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 يكون لديك تطبيق مصادقة على جهاز الكمبيوتر لديك أو على جهازك المحمول.

رمز الحماية له معرف يشار إليه باسم اسم المصدر. اسم مصدر رمز الأمان يُستخدم كـمُعرّف لخاصة الإدارة في تطبيق المصادقة. يمكنك تغيير اسم مصدر رمز الأمان. اسم مصدر رمز الأمان له قيمة افتراضية مماثلة لاسم خادم الإدارة. اسم المصدر يُستخدم كـمُعرّف لخاصة الإدارة في تطبيق المصادقة. إذا قمت بتغيير اسم مصدر رمز الأمان، يجب عليك إصدار مفتاح سري جديد وتمريضه إلى تطبيق المصادقة. رمز الحماية يُستخدم مرة واحدة وصالح لمدة تصل إلى 90 ثانية (قد يختلف الوقت المحدد).

يمكن لأي مستخدم تم تمكين المصادقة الثنائية له إعادة إصدار مفتاحه السري. عندما يقوم مستخدم بالمصادقة باستخدام المفتاح السري المعاد إصداره ويستخدمه لتسجيل الدخول، يحفظ خادم الإدارة المفتاح السري الجديد لحساب المستخدم. إذا أدخل المستخدم المفتاح السري الجديد بشكل غير صحيح، خادم الإدارة لن يحفظ المفتاح السري الجديد وسيترك المفتاح السري الحالي صالحًا للتصديق المستقبلي.

أي برنامج للمصادقة يدعم خوارزمية كلمة المرور لمرة واحدة المستندة إلى الوقت (TOTP) يمكن استخدامه كتطبيق للمصادقة، مثل Google Authenticator. لإنشاء رمز الأمان، يجب عليك مزمنة الوقت المحدد في تطبيق المصادقة مع الوقت المحدد لخادم الإدارة.

تطبيق المصادقة يُنشئ رمز الأمان على النحو التالي:

1. يقوم خادم الإدارة بإنشاء مفتاح سري خاص ورمز استجابة سريعة.
2. أنت تمرر المفتاح السري الذي تم إنشاؤه أو رمز الاستجابة السريعة إلى تطبيق المصادقة.
3. تطبيق المصادقة يُنشئ رمز أمان للاستخدام مرة واحدة تقوم بتمريره إلى نافذة المصادقة لخادم الإدارة.

نوصي بشدة بتثبيت تطبيق المصادقة على أكثر من جهاز محمول. احفظ المفتاح السري (أو رمز الاستجابة السريعة)، واحتفظ به في مكان آمن. سيساعدك هذا في استعادة الوصول إلى Kaspersky Security Center 14 Web Console في حالة فقدان الوصول إلى جهازك 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.

المصادقة الثنائية تعمل وفق القواعد التالية:

- فقط حساب المستخدم الذي يملك حق **تعديل قوائم التحكم في الوصول للكائن** مباشرةً في المجال الوظيفي الميزات العامة: **أذونات المستخدم** تمكين المصادقة الثنائية لجميع المستخدمين.
- يمكن فقط للمستخدم الذي قام بتمكين المصادقة الثنائية لحسابه الخاص أن يقوم بتمكين خيار المصادقة الثنائية لجميع المستخدمين.
- يمكن فقط للمستخدم الذي قام بتمكين المصادقة الثنائية لحسابه الخاص أن يقوم باستثناء حسابات مستخدمين آخرين من قائمة المصادقة الثنائية التي تم تمكينها لجميع المستخدمين.
- يمكن للمستخدم تمكين المصادقة الثنائية لحسابه فقط.
- يمكن لحساب المستخدم الذي لديه حق **تعديل قوائم التحكم في الوصول للكائن** مباشرةً في المجال الوظيفي الميزات العامة: **أذونات المستخدم** ومسجل الدخول إلى Kaspersky Security Center 14 Web Console باستخدام المصادقة الثنائية أن يقوم بتعطيل المصادقة الثنائية لأي مستخدم آخر فقط إذا تم تعطيل المصادقة الثنائية لجميع المستخدمين، ولمستخدم مستثنى من قائمة المصادقة الثنائية التي تم تمكينها لجميع المستخدمين.

- يمكن لأي مستخدم قام بتسجيل الدخول إلى Kaspersky Security Center 14 Web Console باستخدام المصادقة الثنائية إعادة إصدار مفتاحه السري.
- يمكنك تمكين خيار المصادقة الثنائية لجميع المستخدمين ل خادم الإدارة الذي تعمل معه حاليًا. إذا قمت بتمكين هذا الخيار على خادم الإدارة، أنت تقوم كذلك بتمكين هذا الخيار لحسابات المستخدمين لخوادم الإدارة الافتراضية الخاصة بها، ولا تقوم بتمكين المصادقة الثنائية لحسابات المستخدمين لخوادم الإدارة الثانوية.

إذا كانت المصادقة الثنائية مفعلة لحساب مستخدم على خادم إدارة Kaspersky Security Center الإصدار 13 أو أعلى، لن يقدر المستخدم على تسجيل الدخول إلى Kaspersky Security Center Web Console 12 أو 12.1 أو 12.2.

تمكين المصادقة الثنائية لحسابك الخاص

يمكنك تمكين المصادقة الثنائية لحسابك الخاص.

قبل أن تقوم بتمكين المصادقة الثنائية لحسابك، تأكد من تثبيت تطبيق مصادقة على جهازك المحمول. تأكد من 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 **المستخدمون والأدوار** ← **المستخدمون**.

2. انقر على اسم حسابك.

3. في نافذة إعدادات المستخدم التي تفتح، حدد **تبويب حماية الحساب**.

4. في **تبويب حماية الحساب**:

- حدد خيار **اطلب اسم المستخدم وكلمة المرور ورمز الحماية (التحقق المزدوج)** إذا كنت ترغب في تمكين المصادقة الثنائية لحساب مستخدم:

- في نافذة المصادقة الثنائية التي تفتح، أدخل المفتاح السري في تطبيق المصادقة أو امسح رمز الاستجابة السريعة واستلم رمز الحماية لمرة واحدة. يمكنك تحديد المفتاح السري في تطبيق المصادقة يدويًا أو مسح رمز الاستجابة السريعة ضوئيًا باستخدام جهازك المحمول.

- في نافذة المصادقة الثنائية، حدد رمز الأمان الذي أنشأه تطبيق المصادقة ثم انقر على زر **التحقق والتطبيق**.

5. انقر على زر **حفظ**.

تم تمكين المصادقة الثنائية لحسابك.

تمكين المصادقة الثنائية لجميع المستخدمين

يمكنك تمكين المصادقة الثنائية لجميع مستخدمي خادم الإدارة إذا كان حسابك لديه حقوق تعديل قوائم التحكم في الوصول للكانن للمجال الوظيفي **الميزات العامة: أدوات المستخدم** وإذا كان مصرحاً لك استخدام المصادقة الثنائية. إذا لم تقم بتمكين المصادقة الثنائية لحسابك قبل تمكينها لجميع المستخدمين، فإن التطبيق يفتح نافذة تمكين المصادقة الثنائية لحسابك الخاص أولاً.

لتمكين المصادقة الثنائية لجميع المستخدمين:

1. في نافذة التطبيق الرئيسية، انقر فوق أيقونة **الإعدادات** بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في تبويب **حماية المصادقة** في نافذة الخصائص، قم بتبديل زر التبديل لخيار **المصادقة الثنائية لجميع المستخدمين** إلى وضع التمكين.

بهذا تم تمكين المصادقة الثنائية لجميع المستخدمين. من الآن فصاعداً، 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.

تعطيل المصادقة الثنائية لحساب مستخدم

يمكنك تعطيل المصادقة الثنائية لحسابك الخاص، وكذلك لحساب أي مستخدم آخر.

يمكنك تعطيل المصادقة الثنائية لحساب مستخدم آخر فقط إذا كان لحسابك حق تعديل قوائم التحكم في الوصول للكانن مباشرة في المجال الوظيفي **الميزات العامة: أدوات المستخدم**.

لتعطيل المصادقة الثنائية لحساب مستخدم:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **المستخدمون**.

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 **حماية الحساب**.

4. في تبويب **حماية الحساب**، حدد خيار **اطلب فقط اسم المستخدم وكلمة المرور** إذا كنت ترغب في تعطيل المصادقة الثنائية لحساب مستخدم.

5. انقر على زر **حفظ**.

بهذا تم تعطيل المصادقة الثنائية لحساب المستخدم.

تعطيل المصادقة الثنائية لجميع المستخدمين

يمكنك تعطيل المصادقة الثنائية لجميع المستخدمين إذا تم تمكين المصادقة الثنائية لحسابك، وكان حسابك له حق تعديل قوائم التحكم في الوصول للكانن مباشرة في المجال الوظيفي **الميزات العامة: أدوات 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 نافذة التطبيق الرئيسية، انقر فوق أيقونة **الإعدادات** بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في تبويب **حماية المصادقة** في نافذة الخصائص، قم بتبديل زر التبديل لخيار **المصادقة الثنائية لجميع المستخدمين** إلى وضع التعطيل.

3. أدخل بيانات اعتماد حسابك في نافذة المصادقة.

بهذا تم تعطيل المصادقة الثنائية لجميع المستخدمين.

استثناء الحسابات من عملية المصادقة الثنائية

يمكنك استثناء حسابات مستخدمي 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 Active Directory من أجل تحديث قائمة مستخدمي خادم الإدارة إذا كنت ترغب في استثناء حسابات Active Directory.

2. في نافذة التطبيق الرئيسية، انقر فوق أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب. تفتح نافذة خصائص خادم الإدارة.

3. في تبويب **حماية المصادقة** في نافذة الخصائص، في جدول استثناءات المصادقة الثنائية، انقر على زر **إضافة**.

4. في النافذة التي تفتح:

a. حدد حسابات المستخدمين التي ترغب في استثناءها.

b. انقر على زر **موافق**.

بهذا تم استثناء حسابات المستخدمين المحددة من المصادقة الثنائية.

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 **المستخدمون والأدوار** ← **المستخدمون**.

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 **حماية الحساب**.

4. في تبويب **حماية الحساب**، انقر على رابط **قم بإنشاء مفتاح سري جديد**.

5. في نافذة المصادقة الثنائية التي تفتح، حدد مفتاح أمان جديدًا تم إنشاؤه بواسطة تطبيق المصادقة.

6. انقر على زر **التحقق والتطبيق**.

بهذا تم إنشاء مفتاح سري جديد للمستخدم.

إذا فقدت جهازك المحمول، يمكنك تثبيت تطبيق المصادقة على جهاز محمول آخر وإنشاء مفتاح سري جديد لاستعادة الوصول إلى Kaspersky Security Center 14 Web Console.

تحرير اسم مُصدر رمز الأمان

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 وتمريضه إلى تطبيق المصادقة.

لتحديد اسم جديد لمصدر رمز الأمان:

1. في نافذة التطبيق الرئيسية، انقر فوق أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب. تفتح نافذة خصائص خادم الإدارة.
2. في نافذة إعدادات المستخدم التي تفتح، حدد تبويب حماية الحساب.
3. في تبويب حماية الحساب، انقر على رابط تحرير. قسم تحرير مُصدر رمز الأمان سيفتح.
4. حدد اسم مُصدر رمز أمان جديد.
5. انقر على زر موافق.

بهذا تم تحديد اسم مُصدر رمز أمان جديد لخادم الإدارة.

النسخ الاحتياطي والاستعادة لبيانات خادم الإدارة

النسخ الاحتياطي للبيانات يسمح بنقل خادم الإدارة من جهاز إلى آخر دون فقدان للبيانات. باستخدام النسخ الاحتياطي، يمكنك استعادة البيانات عند نقل قاعدة بيانات خادم الإدارة إلى جهاز آخر، أو عند الترقية إلى إصدار أحدث من Kaspersky Security Center.

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 العملية.
- تخزين حزم توزيع التطبيقات للتثبيت عن بُعد.
- شهادة خادم الإدارة.

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 الأجهزة ← المهام.

2. انقر فوق الزر إضافة.

سيبدأ إضافة معالج المهمة.

3. في نافذة مهمة جديدة الخاصة بالمعالج، حدد نوع المهمة الذي يحمل الاسم النسخ الاحتياطي لبيانات خادم الإدارة.

4. اتبع بقية إرشادات المعالج.

يمكن إنشاء مهمة النسخ الاحتياطي لبيانات خادم الإدارة في نسخة مفردة فقط. إذا تم إنشاء مهمة نسخ احتياطي لبيانات خادم الإدارة بالفعل على خادم الإدارة، فلن تُعرض في نافذة اختيار نوع المهمة في "معالج إنشاء مهمة النسخ الاحتياطي".

نشر تطبيقات Kaspersky من خلال Kaspersky Security Center 14 Web Console

يصف هذا القسم تشغيل تطبيقات Kaspersky على أجهزة العميل في مؤسستك من خلال Kaspersky Security Center 14 Web Console.

السيناريو: نشر تطبيقات Kaspersky من خلال Kaspersky Security Center 14 Web Console

يشرح هذا السيناريو كيفية تشغيل تطبيقات Kaspersky من خلال Kaspersky Security Center 14 Web Console. يمكنك استخدام [معالج البدء السريع](#) ومعالج نشر الحماية، أو يمكنك إكمال جميع الخطوات الضرورية يدويًا.

المتطلبات الأساسية

[التطبيقات](#) التالية متوفرة للنشر باستخدام Kaspersky Security Center 14 Web Console:

• Kaspersky Endpoint Security for Windows

• Kaspersky Endpoint Security for Linux

يتقدم نشر تطبيقات Kaspersky في مراحل:

1 تنزيل مكون الإدارة الإضافي للتطبيق

هذه المرحلة هي 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، فاتباع الإرشادات الواردة في تعليمات [Kaspersky Security for Mobile Help](#) لتنزيل مكونات الإدارة الإضافية وتثبيتها لـ Kaspersky Endpoint Security for Android.

2 تنزيل وإنشاء حزم التثبيت

هذه المرحلة هي جزء من معالج البدء السريع.

معالج البدء السريع يتيح لك تنزيل حزمة التثبيت بمكون 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 لـ 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.

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.

4 إنشاء وتكوين المهام للتطبيق المُدار

يجب تكوين مهمة تثبيت التحديث لتطبيق Kaspersky Endpoint Security for Windows.

هذه المرحلة هي 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، تأكد أن [جدول المهمة](#) يلبي المتطلبات. (افتراضيًا، موعد البدء المحدد للمهمة مضبوط يدويًا، لكن 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، فاتباع الإرشادات الواردة في تعليمات [Kaspersky Security for Mobile Help](#) للحصول على معلومات حول نشر Kaspersky Endpoint Security for Android.

6 إنشاء السياسات

قم بإنشاء 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 المنسدلة إعدادات وحدة التحكم ، حدد المكونات الإضافية للويب.
2. في النافذة التي تفتح، انقر على زر إضافة.
3. في قائمة المكونات الإضافية المتاحة، حدد المكون الإضافي الذي ترغب في تنزيله (مثل Kaspersky Endpoint Security 11 for Windows) بالنقر على اسمه.
4. سيتم عرض صفحة بوصف المكون الإضافي.
5. في صفحة وصف المكون الإضافي، انقر على تثبيت المكون الإضافي.
5. عندما يكتمل التثبيت، انقر على موافق.

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 الدعم الفني لـ Kaspersky](#).

لتنزيل مكون إضافي من ملف أو تحديثه:

1. في القائمة المنسدلة إعدادات وحدة التحكم ، حدد المكونات الإضافية للويب.
2. حدد ملف المكون الإضافي وتوقيع الملف:
- انقر فوق إضافة من ملف لتنزيل مكون إضافي من ملف.
- انقر فوق التحديث من ملف 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:

• في القائمة الرئيسية، انتقل **الاكتشاف والنشر** ← **التوزيع والتعيين** ← **حزم التثبيت**.

• في القائمة الرئيسية، انتقل إلى **العمليات** ← **المستودعات** ← **حزم التثبيت**.

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 فوق **إضافة**.

يبدأ معالج الحزمة الجديدة. انتقل عبر المعالج باستخدام زر **التالي**.

3. في صفحة المعالج، حدد **إنشاء حزمة تثبيت لتطبيق Kaspersky**.

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 (11.0).

ستفتح نافذة بها معلومات عن حزمة التثبيت.

5. اقرأ المعلومات ثم انقر على زر **تنزيل حزمة التثبيت وإنشاؤها**.

إذا كان لا يمكن تحويل حزمة توزيع إلى حزمة تثبيت، سيظهر زر **تنزيل حزمة التوزيع** بدلاً من زر **تنزيل حزمة التثبيت وإنشاؤها**. 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 **العمليات** ← **المستودعات** ← **حزم التثبيت** ← **قيد التقدم** ().

b. تعقب تقدم العملية في عمود **تقدم التنزيل** وعمود **حالة التنزيل** للجدول.

سيتم إضافة حزمة التثبيت إلى القائمة في تويوب **تم التنزيل** عند اكتمال العملية. في حال توقف عملية التنزيل وتبديل حالة التنزيل إلى **الموافقة على اتفاقية ترخيص المستخدم النهائي**، 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 **عرض اتفاقية ترخيص المستخدم النهائي** أثناء عملية التنزيل لبعض تطبيقات Kaspersky. افعل ما يلي إذا ظهر ذلك الزر:

a. انقر على زر **عرض اتفاقية ترخيص المستخدم النهائي** لقراءة اتفاقية ترخيص المستخدم النهائي.

b. اقرأ اتفاقية ترخيص المستخدم النهائي المعروضة على الشاشة ثم انقر على **قبول**.

يستمر التنزيل بعد أن تقبل اتفاقية ترخيص المستخدم النهائي. سيتوقف التنزيل إذا نقرت على **رفض**.

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. افتح سجل النظام الخاص بجهاز خادم الإدارة (على سبيل المثال محليًا، باستخدام أمر regedit من القائمة بدء ← تشغيل).

2. انتقل إلى

KEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0\ServerFlags.hive

3. انقر بزر الماوس الأيمن فوق الخلية، ثم حدد جديد ← قيمة (32 DWORD بت).

يتم إنشاء مفتاح DWORD جديد.

4. قم بتعيين مفتاح اسم MaxArchivePkgSize.

5. انقر نقرًا مزدوجًا فوق مفتاح DWORD الجديد للتعديل.

6. قم بتعيين قيمة الحد المطلوبة:

a. حدد أي قاعدة: سداسي عشري أو عشري.

b. حدد عدد البايت المقابل للقاعدة المحددة.

على سبيل المثال، إذا كان الحد المطلوب هو 2 جيجابايت، فيمكنك تحديد القيمة العشرية 2147483648 أو القيمة السداسية العشرية 0x80000000.

7. انقر فوق موافق.

بهذا يتم تغيير حد حجم بيانات حزمة التثبيت المخصصة.

تنزيل حزم التوزيع لتطبيقات Kaspersky

يمكنك في Kaspersky Security Center 14 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. من تبويب العمليات، حدد 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 تنزيل حزمة التثبيت وإنشاؤها.

إذا كان لا يمكن تحويل حزمة توزيع إلى حزمة تثبيت، سيظهر زر تنزيل حزمة التوزيع بدلاً من زر تنزيل حزمة التثبيت وإنشاؤها.

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 نجاح Kaspersky Endpoint Security for Windows

للتأكد أنك قد قمت بنشر تطبيقات Kaspersky بشكل صحيح، مثل Kaspersky Endpoint Security:

1. باستخدام Kaspersky Security Center 14 Web Console، تأكد أنك لديك ما يلي:

- سياسة لـ Kaspersky Endpoint Security و/أو تطبيقات أمان أخرى تستخدمها.
- مهام Kaspersky Endpoint Security for Windows: مهمة فحص سريع للبحث عن الفيروسات ومهمة تثبيت التحديث (إذا كنت تستخدم Kaspersky Endpoint Security 11 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 و macOS و Linux. 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 إلى **الاكتشاف والنشر** ← **التوزيع والتعيين** ← **حزم التثبيت**.
- في القائمة الرئيسية، انتقل إلى **العمليات** ← **المستودعات** ← **حزم التثبيت**.

يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. في قائمة حزم التثبيت، حدد حزمة التثبيت، وفي أعلى القائمة انقر على زر **نشر**.

3. حدد خيار استخدام الحزمة المستقلة.

يبدأ معالج إنشاء حزمة تثبيت مستقلة. انتقل عبر المعالج باستخدام زر التالي.

4. في الصفحة الأولى من المعالج، تأكد من تمكين خيار تثبيت عميل الشبكة بالإضافة إلى هذا التطبيق إذا أردت تثبيت عميل الشبكة مع التطبيق المحدد. 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 صفحة نقل إلى قائمة الأجهزة المُدارة من المعالج، يتم تحديد خيار عدم نقل الأجهزة بشكل افتراضي. إذا كنت لا تريد نقل الجهاز العميل إلى أي مجموعة إدارية بعد تثبيت عميل الشبكة، فترك هذا الخيار ممكنًا. إذا كنت ترغب في نقل الجهاز العميل بعد تثبيت عميل الشبكة، حدد خيار نقل الأجهزة غير المخصصة إلى هذه المجموعة ثم حدد مجموعة إدارة ترغب في نقل الجهاز العميل إليها. بشكل افتراضي، يتم نقل الجهاز إلى مجموعة الأجهزة المُدارة.
6. في الصفحة التالية من المعالج، عند انتهاء عملية إنشاء حزمة التثبيت المستقلة، انقر على زر إنهاء. معالج إنشاء حزمة تثبيت مستقلة يغلُق.

يتم إنشاء حزمة التثبيت المستقلة ووضعها في المجلد الفرعي PkgInst الخاص بمجلد [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 عرض قائمة الحزم المستقلة.

في قائمة حزم التثبيت المستقلة، يتم عرض الخصائص التالية لها:

- اسم الحزمة. اسم حزمة التثبيت المستقلة الذي يتم تشكيله تلقائيًا كاسم التطبيق الموجود في الحزمة وإصدار التطبيق.
- اسم التطبيق. اسم التطبيق المذكورة في حزمة التثبيت المستقلة.
- إصدار التطبيق.
- اسم حزمة تثبيت عميل الشبكة. يتم عرض الخاصية فقط إذا تم تضمين عميل الشبكة في حزمة التثبيت المستقلة.
- إصدار عميل الشبكة. يتم عرض الخاصية فقط إذا تم تضمين عميل الشبكة في حزمة التثبيت المستقلة.
- الحجم. حجم الملف بالميجا بايت.

- **مجموعة.** اسم المجموعة التي يتم نقل الجهاز العميل إليها بعد تثبيت عميل الشبكة.
- **تم الإنشاء.** تاريخ ووقت إنشاء حزمة التثبيت المستقلة.
- **معدل.** تاريخ ووقت تعديل حزمة التثبيت المستقلة.
- **المسار.** المسار الكامل للمجلد الذي يوجد فيه حزمة التثبيت المستقلة.
- **عنوان الويب.** عنوان الويب لموقع حزمة التثبيت المستقلة.
- **تجزئة الملف.** 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 **عرض قائمة الحزم المستقلة**.

في قائمة حزم التثبيت المستقلة، يمكنك فعل ما يلي:

- نشر حزمة تثبيت مستقلة على خادم الويب بالنقر على زر **النشر**. 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 **إلغاء النشر**. حزمة تثبيت مستقلة غير منشورة ليست متوفرة للتنزيل إلا من أجلك ومن أجل المديرين الآخرين.
- تنزيل حزمة تثبيت مستقلة على جهازك بالنقر على زر **تنزيل**.
- إرسال بريد إلكتروني به رابط لحزمة التثبيت المستقلة عن طريق النقر على زر **إرسال عبر البريد الإلكتروني**.
- إزالة حزمة تثبيت مستقلة بالنقر على زر **إزالة**.

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 معلومات 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 **الاكتشاف والنشر** ← **التوزيع والتعيين** ← **حزم التثبيت**.

• في القائمة الرئيسية، انتقل إلى **العمليات** ← **المستودعات** ← **حزم التثبيت**.

يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. انقر فوق **إضافة**.

يبدأ معالج الحزمة الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. في أول صفحة في المعالج، حدد **قم بإنشاء حزمة تثبيت من ملف**.

4. في الصفحة التالية للمعالج، حدد اسم الحزمة ثم انقر على زر **استعراض**.

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 **تحويل الإعدادات إلى القيم الموصى بها للتطبيقات التي يتعرف عليها Kaspersky Security Center** بعد انتهاء المعالج محددة ثم انقر على **التالي**.

سيبدأ رفع الملف إلى خادم إدارة Kaspersky Security Center 14.

إذا قمت بتفعيل استخدام الإعدادات التثبيت الموصى بها، يتحقق Kaspersky Security Center 14 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 **إنهاء** لإغلاق المعالج.

6. في الصفحة التالية من المعالج، 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 **إنهاء** لإغلاق المعالج.

يتم تنزيل حزمة التثبيت التي قمت بإنشائها إلى مجلد الحزم الفرعي الخاص بـ **مجلد 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:

• الاسم. اسم حزمة تثبيت مخصص.

• المصدر. اسم بائع التطبيق.

• التطبيق. اسم التطبيق الموضوع في حزمة التثبيت المخصصة.

• الإصدار. إصدار التطبيق.

• اللغة. لغة التطبيق الموضوع في حزمة التثبيت المخصصة.

- الحجم (ميجابايت). حجم حزمة التثبيت.
- نظام التشغيل. نوع نظام التشغيل الذي ستعمل عليه حزمة التثبيت.
- تم الإنشاء. تاريخ إنشاء حزمة التثبيت.
- معدل. تاريخ تعديل حزمة التثبيت.
- النوع. نوع حزمة التثبيت.
- تغيير اسم الحزمة ومعلومات 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 إعدادات لخصائص حزمة التثبيت المخصصة: إعدادات وإجراء التثبيت.

يحتوي قسم إعدادات 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 تحدها معلمة التثبيت (قيمة منطقية أو مسار ملف أو رقمية أو مسار أو سلسلة).

يحتوي قسم إجراء التثبيت 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 تحده 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 المطلوبة.** يعرض ما إذا كان التحديث بحالة "إعادة التشغيل المطلوبة" 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 معرف 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.

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 **الأجهزة** ← **المهام**.
2. انقر على اسم مهمة التثبيت عن بُعد التي ترغب في تحديد إعدادات Unix الخاصة بها. سنفتح نافذة خصائص المهمة.

3. انتقل إلى إعدادات التطبيق ← الإعدادات الخاصة بـ Unix.

4. حدد الإعدادات التالية:

• **تعيين كلمة المرور لحساب الجذر (فقط للنشر من خلال SSH)** [5]

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 نيابة عن حساب الجذر باستخدام كلمة المرور المحددة.

Kaspersky Security Center لا يستخدم الحساب أو كلمة المرور المحددة لإنشاء اتصال SSH.

• **حدد المسار إلى المجلد المؤقت بأذونات التنفيذ على الجهاز الهدف (النشر من خلال SSH فقط)** [5]

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 حفظ.

بهذا تم حفظ إعدادات المهمة المحددة.

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 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 للهواتف 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 14 Web Console، يجب عليك تثبيت المكونات الإضافية التالية لإدارة الويب على الجهاز حيث تم تثبيت Kaspersky Security Center 14 Web Console:

• Kaspersky Security for Mobile Plug-in

• Kaspersky Endpoint Security for Android Plug-in

للحصول على معلومات حول نشر الحماية وإدارة الأجهزة المحمولة، راجع تعليمات [Kaspersky Security for Mobile Help](#).

تعديل إعدادات إدارة الأجهزة المحمولة في Kaspersky Security Center 14 Web Console

لتعديل إعدادات إدارة الجهاز المحمول:

1. في نافذة التطبيق الرئيسية، انقر فوق أيقونة الإعدادات [5] بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، حدد قسم منافذ إضافية.

• **فتح منفذ للأجهزة المحمولة**

في حال تفعيل هذا الخيار، سيتم فتح منفذ الأجهزة المحمولة على خادم الإدارة. لا يمكنك استخدام منفذ الأجهزة المحمولة إلا إذا كان مكون إدارة الأجهزة المحمولة مثبتًا. إذا كان هذا الخيار غير مفعل، لن يتم استخدام منفذ الأجهزة المحمولة على خادم الإدارة. يتم تعطيل هذا الخيار افتراضيًا.

• **منفذ لمزامنة الأجهزة المحمولة**

رقم المنفذ المستخدم لإتمام الاتصال بين الأجهزة المحمولة وخادم الإدارة. رقم المنفذ الافتراضي هو 13292. تم استخدام النظام العشري للسجلات.

• **المنفذ الخاص بتفعيل جهاز المحمول**

منفذ اتصال Kaspersky Endpoint Security for Android بخوادم تنشيط Kaspersky. رقم المنفذ الافتراضي هو 17100.

4. انقر على زر **حفظ**.

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 14 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: [تثبيت التطبيقات باستخدام معالج التثبيت عن بُعد](#)

• [Kaspersky Security Center 14 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 لخدم 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. عند اكتشاف جميع الأجهزة المتصلة بالشبكة، يمكنك الحصول على معلومات حولها وإدارتها من خلال السياسات. هناك حاجة لاستطلاعات شبكة منتظمة لاكتشاف وجود أي أجهزة جديدة وما إذا كانت الأجهزة التي تم اكتشافها مسبقًا لا تزال موجودة على الشبكة.

يتم اكتشاف الأجهزة المتصلة بالشبكة على المراحل التالية:

1 اكتشاف الأجهزة الأولي

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 المستقبلية

حدد **نوع (أنواع) الاكتشاف** الذي تريد استخدامه بانتظام. تأكد من أن هذا النوع ممكن وأن جدول الاستقصاء يلبي احتياجات مؤسستك. عند تكوين جدول الاستقصاء، استخدم **التوصيات لتكرار استقصاء الشبكة**.

3 إعداد القواعد لإضافة الأجهزة المكتشفة إلى مجموعات الإدارة (اختياري)

إذا ظهرت أجهزة جديدة على شبكتك، سيتم اكتشافها أثناء الاستقصاءات المنتظمة وسيتم تضمينها تلقائيًا في المجموعة **الأجهزة غير المخصصة**. إذا أردت، يمكنك إعداد القواعد **لنقل هذه الأجهزة** تلقائيًا إلى المجموعة **الأجهزة المُدارة**. يمكنك أيضًا إنشاء **قواعد الاستبقاء**.

إذا تخطيت مرحلة إعداد هذه القاعدة، فستنقل جميع الأجهزة المكتشفة حديثًا إلى المجموعة **الأجهزة غير المخصصة** وستظل هناك. 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 المطلوب النقل إليها.

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 وفقاً للجدول المحدد.
- يتم ترتيب الأجهزة المكتشفة حديثاً وفقاً للقواعد التي تم تكوينها (أو في حالة عدم تكوين أي قواعد، تظل 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.
 - **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؛ خلافاً لذلك، فلن 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.** يستقصى 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 افتراضياً. لا يوصى باستخدام هذا النوع من الاستقصاء إذا كنت تستخدم استقصاء شبكة Windows و/أو استقصاء Active Directory.
 - **استطلاع شبكة لا تتطلب تكويناً.** تقوم نقطة توزيع باستقصاء شبكة IPv6 باستخدام شيكات التكوين الصفري (كما يشار إلى Zeroconf). يتم تعطيل نوع الاستقصاء هذا افتراضياً. يمكنك استخدام استقصاء شبكة لا تتطلب تكويناً إذا كانت نقطة التوزيع تعمل بنظام Linux.
- إذا قمت بإعداد وتمكين قواعد نقل الأجهزة، فسيتم تضمين الأجهزة المكتشفة حديثاً تلقائياً في المجموعة **الأجهزة المُدارة**. في حالة عدم تمكين أي من قواعد النقل، فسيتم تضمين الأجهزة المكتشفة حديثاً تلقائياً 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 مجال Active Directory بالكامل أو فقط مجال محدد.

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، وTCP 139، وUDP 445، وTCP 445 متاحة على الشبكة.
 - 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 **الاكتشاف والنشر** ← **اكتشاف** ← **مجالات Windows**.
2. انقر على زر **خصائص**.
- تفتح نافذة خصائص مجال Windows.
3. قم بتفعيل أو تعطيل استقصاء شبكة Windows باستخدام زر **تمكين استقصاء شبكة Windows**.
4. قم بتكوين جدول الاستقصاء يجري الاستقصاء السريع كل 15 دقيقة بشكل افتراضي، ويجري الاستقصاء الكامل كل 60 دقيقة. خيارات جدول الاستقصاء:

• كل N يوماً

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.

• **حسب أيام الأسبوع**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

• **كل شهر في أيام معينة من الأسابيع المحددة**

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

• **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 تعطيل هذا الخيار افتراضيًا.

5. انقر على زر **حفظ**.

يتم حفظ الخصائص وتطبيقها إلى جميع نطاقات Windows ومجموعات عمله.

إجراء الاستطلاع يدويًا

لإجراء الاستطلاع على الفور،

انقر على **بدء الاستقصاء السريع** أو **بدء الاستقصاء بالكامل**.

عند اكتمال الاستقصاء، يمكنك عرض قائمة بالأجهزة المكتشفة على صفحة **مجالات Windows** عن طريق تحديد خانة الاختيار الموجودة بجوار اسم مجال ثم النقر على زر **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 اكتشاف هذه الأجهزة باستخدام استقصاء Active Directory.

يرسل Kaspersky Security Center طلبًا إلى وحدة التحكم بالمجال ويستقبل هيكل جهاز Active Directory. يتم إجراء استقصاء Active Directory كل ساعة.

عرض وتعديل إعدادات استقصاء Active Directory

لعرض إعدادات استقصاء Active Directory وتعديلها:

1. في القائمة الرئيسية، انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **ACTIVE DIRECTORY**.

2. انقر على زر **خصائص**.

تفتح نافذة خصائص Active Directory.

3. في نافذة خصائص Active Directory، يمكنك تحديد الإعدادات التالية:

a. قم بتشغيل استقصاء Active Directory أو إيقافه باستخدام زر التبديل.

b. قم بتغيير جدول الاستقصاء.

الفترة الافتراضية هي ساعة واحدة. يتم استبدال البيانات التي يتم تلقيها في الاستقصاء التالي بالبيانات القديمة بشكل كامل.

c. قم بتكوين الإعدادات المتقدمة لتحديد نطاق الاستقصاء:

• مجال Active Directory الذي ينتمي إليه Kaspersky Security Center:

• المجال الرئيسي الذي ينتمي إليه Kaspersky Security Center

• القائمة المحددة لمجالات Active Directory

لإضافة مجال إلى نطاق الاستقصاء، حدد خيار مجال ثم انقر على زر **إضافة**، وبعدها عنوان وحدة التحكم بالمجال واسم الحساب الذي يصل إليها وكلمة مروره.

4. لتطبيق الإعدادات الجديدة، انقر على زر **حفظ**.

يتم تطبيق الإعدادات الجديدة إلى استقصاء Active Directory.

إجراء الاستطلاع يدويًا

لإجراء الاستطلاع على الفور،

انقر على **بدء الاستقصاء**.

عرض نتائج استقصاء Active Directory.

لعرض نتائج استقصاء Active Directory:

1. في القائمة الرئيسية، انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **ACTIVE DIRECTORY**.

يتم عرض قائمة بالوحدات التنظيمية المكتشفة.

2. يمكنك إذا كنت ترغب أن تحدد وحدة تنظيمية ثم انقر على زر **الأجهزة**.

سيتم عرض قائمة بالأجهزة في الوحدة التنظيمية.

يمكنك البحث في القائمة وتصفية النتائج.

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. يستقصى Kaspersky Security Center جميع العناوين من 192.168.0.1 إلى 192.168.0.254.

لا يوصى باستخدام هذا استقصاء نطاق IP إذا كنت تستخدم استقصاء شبكة Windows و/أو استقصاء Active Directory.

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 من النطاق المحدد لاسم DNS باستخدام طلبات DNS المعتادة. وفي حال نجاح هذه العملية، يرسل الخادم طلب ICMP ECHO (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 المستخدمة 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، مدير 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 معطلًا 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 أُرجم طلب عنوان IP اسم NetBIOS، ستتم إضافة المعلومات حول هذا الجهاز إلى قاعدة بيانات Kaspersky Security Center.

عرض وتعديل إعدادات استقصاء نطاق IP

لعرض وتعديل خصائص استقصاء نطاق IP:

1. في القائمة الرئيسية، انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **نطاقات IP**.

2. انقر على زر **خصائص**.

سنتفتح نافذة خصائص استقصاء IP.

3. قم بتفعيل أو تعطيل استقصاء IP باستخدام زر **التبديل السماح بالاستقصاء**.

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:

• كل N يومًا

يعمل الاستقصاء بشكل 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 بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد.

• حسب أيام الأسبوع

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

• كل شهر في أيام معينة من الأسابيع المحددة 5

يعمل الاستقصاء بشكلٍ منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.

• تشغيل المهام الفائتة 5

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 حفظ.

يتم حفظ الخصائص وتطبيقها على جميع نطاقات IP.

إجراء الاستطلاع يدويًا

لإجراء الاستطلاع على الفور،

انقر على بدء الاستقصاء.

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. يستقصى 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 توكيلاً، فسيقوم Kaspersky Security Center باستقصاء الشبكة بالكامل.

لإضافة نطاق IP جديد:

1. في القائمة الرئيسية، انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **نطاقات IP**.

2. لإضافة نطاق IP جديد، انقر على زر **إضافة**.

3. في النافذة التي تفتح، حدد الإعدادات التالية:

• اسم نطاق IP 5

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 ④

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 **استعراض**.

• مدة بقاء عنوان IP (بالساعات) ④

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 **تمكين استقصاء نطاق IP** 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 **حفظ**.

سيتم إضافة نطاق IP الجديد إلى قائمة نطاقات IP.

يمكنك إجراء الاستقصاء لكل نطاق IP بشكل منفصل عن طريق استخدام زر **بدء الاستقصاء**. عند اكتمال الاستقصاء، يمكنك عرض قائمة بالأجهزة المكتشفة باستخدام زر **الأجهزة**. 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 **الاكتشاف والنشر** ← **اكتشاف** ← **نطاقات IP**.

2. انقر على اسم نطاق IP التي ترغب في إضافة شبكة فرعية له.

3. في النافذة التي تفتح، انقر على زر **إضافة**.

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 **استعراض**.

5. انقر على زر **حفظ**.

سيتم إضافة الشبكة الفرعية الجديدة إلى نطاق IP.

6. انقر على زر **حفظ**.

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.

1. في القائمة الرئيسية، انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **نطاقات IP**.
2. انقر على زر **خصائص**.
3. في النافذة التي تفتح، انقر على زر **التبديل** **استخدم شبكة لا تتطلب تكويناً لاستقصاء شبكات IPv6**.
بعد ذلك، تبدأ نقطة التوزيع في استقصاء شبكتك. في هذه الحالة، يتم تجاهل نطاقات IP المحددة.

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 **الاكتشاف والنشر** ← **اكتشاف** ← **مجالات Windows**. يمثل مجلد **مجالات Windows** المجموعة الرئيسية. يحتوي على مجموعات فرعية تمت تسميتها باسم المجالات ومجموعات العمل المطابقة التي تم العثور عليها أثناء إجراء الاستقصاء. قد تحتوي المجموعة الرئيسية أيضاً 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.

قم بما يلي لتكوين قواعد الاستبقاء للأجهزة غير المخصصة:

1. في القائمة الرئيسية، انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **مجالات Windows**.
2. قم بأحد الإجراءات التالية:

- لتكوين إعدادات المجموعة الأساسية، انقر على زر **خصائص**.
تفتح نافذة خصائص مجال Windows.
- لتكوين إعدادات مجموعة فرعية، انقر على اسمها.
تفتح نافذة خصائص المجموعة الفرعية.

3. حدد الإعدادات التالية:

- **إزالة الجهاز من المجموعة إذا ظل غير نشط لمدة تزيد عن (بالأيام)** 9

إذا تم تمكين هذا الخيار، فيمكنك تحديد الفترة الزمنية التي يتم بعدها إزالة الجهاز تلقائياً من المجموعة. يتم افتراضياً توزيع هذا الخيار أيضاً على المجموعات الفرعية. الفاصل الزمني الافتراضي هو 7 أيام.
يتم تمكين هذا الخيار افتراضياً.

- **توريث من المجموعة الأصلية** 9

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 افتراضياً.

- **فرض التوريث في المجموعات الفرعية** 9

سيتم توزيع قيم الإعداد إلى المجموعات الفرعية ولكن في خصائص المجموعات الفرعية يتم قفل هذه الإعدادات.
يتم تعطيل هذا الخيار افتراضياً.

تم حفظ وتطبيق التغييرات الخاصة بك.

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 المثبتة على الأجهزة المُدارة من خلال تطبيق ملف المفتاح أو رمز التنشيط على كل تطبيق من التطبيقات. يمكن نشر ملف المفتاح أو رمز التنشيط بالطرق التالية:

- النشر التلقائي
- حزمة تثبيت التطبيق المُدار
- مهمة مفتاح ترخيص بالإضافة للتطبيق المُدار
- 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 مُدارة مختلفة وكان عليك نشر ملف مفتاح محدد أو رمز تنشيط للأجهزة، فقم باختيار طرق أخرى لنشر ملف المفتاح أو رمز التنشيط 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 التنشيط إلى مستودع خادم الإدارة.

تعليمات للمساعدة:

• وحدة تحكم الإدارة:

• [إضافة مفتاح ترخيص إلى مستودع خادم الإدارة](#)

• [التوزيع التلقائي لمفتاح الترخيص](#)

أو

• Kaspersky Security Center 14 Web Console:

• [إضافة مفتاح ترخيص إلى مستودع خادم الإدارة](#)

• [التوزيع التلقائي لمفتاح الترخيص](#)

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 التنشيط المُضاف إلى حزمة التثبيت.

إذا قمت بتثبيت تطبيق مُدار 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 العملية](#)

أو

• Kaspersky Security Center 14 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 العملية](#)

أو

• [إضافة مفتاح ترخيص إلى مستودع خادم الإدارة](#)

• [نشر مفتاح ترخيص على الأجهزة العميلة](#)

إضافة رمز التنشيط أو ملف المفتاح إلى الأجهزة يدويًا

يمكنك تنشيط تطبيق Kaspersky المثبت محليًا من خلال استخدام الأدوات المتوفرة في واجهة التطبيق. يرجى الرجوع إلى وثائق التطبيق المثبت.

إضافة مفتاح ترخيص إلى مستودع خادم الإدارة

لإضافة مفتاح ترخيص إلى مستودع خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **الترخيص** ← **تراخيص KASPERSKY**.

2. انقر على زر **إضافة**.

3. اختر ما ترغب في إضافته:

• **إضافة ملف مفتاح**

انقر على زر **تحديد ملف المفتاح** واذاهب إلى ملف key الذي ترغب في إضافته.

• **إدخال رمز التنشيط**

حدد رمز التنشيط في الحقل النصي ثم انقر على زر **إرسال**

4. انقر فوق الزر **إغلاق**.

يتم إضافة مفتاح الترخيص أو عدة مفاتيح ترخيص إلى مستودع خادم الإدارة.

نشر مفتاح ترخيص على الأجهزة العميلة

تتيح لك Kaspersky Security Center 14 Web Console توزيع مفتاح ترخيص على أجهزة العميل من خلال مهمة توزيع مفتاح الترخيص.

لتوزيع مفتاح ترخيص على الأجهزة العميلة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

2. انقر فوق **إضافة**.

يبدأ تشغيل معالج إضافة مهمة.

3. حدد التطبيق الذي ترغب في إضافة مفتاح ترخيص له.

4. من قائمة **نوع المهمة**، حدد **إضافة مفتاح**.

5. اتبع تعليمات المعالج.

6. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **فتح تفاصيل المهمة عند اكتمال الإنشاء** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

7. انقر فوق الزر **إنشاء**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

8. لتشغيل المهمة، حددها في قائمة المهام ثم انقر على زر **بدء**.

يتم نشر مفتاح الترخيص إلى الأجهزة المحددة عندما تتم المهمة.

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 **العمليات** ← **الترخيص** ← **تراخيص KASPERSKY**.

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 المفاتيح تلقائيًا إلى الأجهزة التي يتم إدارتها**.

4. انقر على زر **حفظ**.

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. يتم تعيين حد الترخيص في خصائص مفتاح الترخيص. عند الوصول إلى حد الترخيص، يتوقف توزيع مفتاح الترخيص هذا على الأجهزة تلقائيًا.

إذا قمت بتحديد خانة الاختيار **توزيع المفاتيح تلقائيًا إلى الأجهزة التي يتم إدارتها** في نافذة خصائص مفتاح الترخيص، فسيتم توزيع مفتاح الترخيص على شبكتك على الفور. إذا لم تحدد هذا الخيار، فيمكنك يدويًا **توزيع مفتاح الترخيص** في وقت لاحق.

عرض معلومات حول مفاتيح التراخيص قيد الاستخدام

لعرض قائمة بمفاتيح الترخيص المضافة إلى مستودع خادم الإدارة:

في القائمة الرئيسية، انتقل إلى **العمليات** ← **الترخيص** ← **تراخيص KASPERSKY**.

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 **العمليات** ← **الترخيص** ← **تراخيص KASPERSKY**.

2. انقر على اسم مفتاح الترخيص المطلوب.

يمكنك عرض ما يلي في نافذة خصائص مفتاح الترخيص التي تفتح:

- في تبويب عام: المعلومات الأساسية عن مفتاح الترخيص
 - في تبويب الأجهزة: 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 **الأجهزة** ← **الأجهزة المُدارة**.
 2. انقر على اسم الجهاز المطلوب.
 3. في النافذة خصائص الجهاز التي تُفتح، حدد علامة التبويب **التطبيقات**.
 4. انقر على اسم التطبيق الذي ترغب في عرض معلومات عن مفتاح ترخيصه.
 5. في نافذة خصائص التطبيق التي تفتح، حدد تبويب **عام** ثم افتح قسم **ترخيص**.
- 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.

حذف مفتاح ترخيص من المستودع

عندما تحذف مفتاح الترخيص المفعّل 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 المفعّل بعد حذف مفتاح الترخيص المفعّل السابق.

عندما تحذف مفتاح الترخيص المفعّل المنشور على جهاز مُدار، سيستمر التطبيق في العمل على الجهاز المُدار.

لحذف ملف مفتاح أو رمز تنشيط من مستودع خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **الترخيص** ← **تراخيص KASPERSKY**.

2. حدد ملف المفتاح أو رمز التنشيط الذي ترغب في حذفه من المستودع.

3. انقر فوق الزر **حذف**.

4. أكد العملية عن طريق النقر على زر **موافق**.

سيتم حذف ملف المفتاح أو رمز التنشيط المحدد من المستودع.

يمكنك **إضافة** مفتاح محذوف 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 عام حدد قسم **اتفاقيات ترخيص المستخدم النهائي**.
يتم عرض قائمة باتفاقيات 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
 - المعرف الفريد (UID) لاتفاقية ترخيص المستخدم النهائي
 - النص الكامل لاتفاقية ترخيص المستخدم النهائي
 - قائمة بالكائنات (حزم التثبيت والتحديثات السلسلة 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 **إبطال اتفاقية الترخيص**.

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 **اتفاقيات ترخيص المستخدم النهائي**، ستعلق نافذة خصائص اتفاقية ترخيص المستخدم النهائي، ولن يعد التطبيق مثبتًا.

تجديد ترخيص 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 العمليات ← الترخيص ← تراخيص KASPERSKY.
 - في القائمة الرئيسية، انتقل إلى المراقبة والإبلاغ ← لوحة المعلومات ثم انقر فوق رابط عرض التراخيص المنتهية الصلاحية بجوار الإشعار.
- يتم فتح نافذة تراخيص KASPERSKY ، حيث يمكنك عرض التراخيص وتجديدها.

2. انقر على رابط تجديد الترخيص 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 14 Web Console، يتم عرض الإشعارات عندما توشك صلاحية الترخيص على الانتهاء وفقاً 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

السوق 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. يتيح لك كل صفحة ويب متابعة عملية الشراء أو تحنوي على إرشادات حول عملية الشراء.

في قسم السوق، 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 تلقائياً.

• مثالي

هذا المستوى نموذجي للمؤسسات التي لديها فريق تكنولوجيا معلومات فقط. في هذا المستوى، تحتاج الشركات إلى حلول تمكنها من مواجهة التهديدات والتهديدات السلعية التي تتحاييل 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: البيانات 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 السوق.

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 قبل 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 14 المُثبت](#)
 - [Kaspersky Security Center 14 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 14 Web Console. [يمكن تنفيذ نهج إدارة الأمان المرتكز على المستخدم من خلال](#) Kaspersky Security Center 14 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 14 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:

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 نهج 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 14 Web Console. يمكن تنفيذ نهج إدارة الأمان المرتكز على المستخدم من خلال Kaspersky Security Center 14 Web Console فقط.

تمتلك 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 في Active Directory أو مواصفات أجهزتهم.

تمتلك 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 وقلها 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 الحوادث الأمنية 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 العملية 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 نجاح تثبيت [Kaspersky Security Center 14 Web Console](#) و [Kaspersky Security Center 14 Web Console](#) (اختياري). إذا قمت بتثبيت Kaspersky Security Center 14 Web Console، فقد ترغب أيضًا في اعتبار إدارة الأمان [المرتكز 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 المثبتة على الأجهزة المُدارة من خلال إنشاء [سياسة](#) لكل تطبيق. سيتم نشر مجموعة السياسات إلى الأجهزة العملية.

عندما تقوم بتكوين حماية شبكتك في معالج البدء السريع، سينشئ Kaspersky Security Center السياسة الافتراضية لـ Kaspersky Endpoint Security for Windows. إذا قمت باستكمال عملية التكوين باستخدام هذا المعالج، فليس عليك إنشاء سياسة جديدة لهذا التطبيق. الانتقال إلى [الإعدادات اليدوي](#) [للسياسة 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 بشكل 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 14 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 [علامات](#) محددة. 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 ملف 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 14 Web Console](#):

- إنشاء ملف تعريف سياسة

- إنشاء قاعدة تفعيل ملف تعريف سياسة

3 نشر السياسات وملفات تعريف السياسة على الأجهزة المُدارة

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 الأمر [فرض المزامنة](#). عند اكتمال المزامنة يتم تسليم السياسات وملفات تعريف السياسة وتطبيقها على تطبيقات Kaspersky المثبتة.

إذا كنت تستخدم Kaspersky Security Center 14 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](#)

- [المزامنة المفروضة](#): Kaspersky Security Center 14 Web Console

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 14 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 [نهج الإدارة](#).

المعالجة

يتكون سيناريو الإدارة المرتكزة على المستخدم لتطبيقات Kaspersky من الخطوات التالية:

1 تكوين سياسات التطبيق

قم بتكوين إعدادات تطبيقات Kaspersky المثبتة على الأجهزة المُدارة من خلال إنشاء [سياسة](#) لكل تطبيق. سيتم نشر مجموعة السياسات إلى الأجهزة العملية.

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 بشكل افتراضي. يمكنك فرض الوراثة من خلال المجموعات الفرعية وخوادم الإدارة الثانوية لمنع أي تعديلات في الإعدادات المكونة في سياسة المنبع. إذا كنت لا ترغب إلا في أن يتم توريث جزء من الإعدادات بالقوة، يمكنك قفلاً 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 مهنتهم أو مناصبهم. ستحتاج بعد ذلك إلى إنشاء دور مستخدم لكل مجموعة. ضع في حسابك 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 مسبقاً. ستحتوي أدوار المستخدم على مجموعة من حقوق الوصول إلى مزايا التطبيق.

تعليمات المساعدة: إنشاء دور مستخدم

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، فقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

تعليمات المساعدة: تحديد 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 نشطاً 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 المُدارة

بشكل افتراضي، يعمل خادم الإدارة تلقائياً 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 يدوياً 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 وفقاً 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 **الأجهزة** ← **السياسات وملفات تعريف**.

2. انقر فوق اسم سياسة عميل الشبكة.

تفتح نافذة الخصائص لسياسة عميل الشبكة.

عام

في علامة التبويب هذه، يمكنك تعديل حالة السياسة وتحديد توريث إعدادات السياسة:

• **ضمن حالة السياسة**، يمكنك تحديد أحد أوضاع السياسة:

• **نشط**

إذا تم تحديد هذا الخيار، تصبح السياسة نشطة.
يتم تحديد هذا الخيار افتراضيًا.

• **غير نشط**

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 على سياسات مجموعات الإدارة المتداخلة أي على 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

يمكنك تكوين تسجيل الأحداث وإشعار الحدث في علامة التبويب هذه. يتم توزيع الأحداث وفقاً لمستوى الأهمية في الأقسام التالية في علامة التبويب تكوين الحدث:

- **خلل وظيفي**

- **تحذير**

- **معلومات**

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 **تحذير** يمكنك تكوين **وقوع حادث** 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 لتنصيب التطبيقات وتنزيل التحديثات عن بُعد). لتكوين **وقوع حادث** الحدث، انقر فوقه وحدد مكان تخزين الأحداث التي وقعت وكيفية الإخطار بها.

إذا اكتشف عميل الشبكة حادثاً، فيمكنك إدارة هذا الحادث باستخدام **إعدادات جهاز مُدار**.

إعدادات التطبيق

إعدادات

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 المدارة **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 افتراضياً.

- **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 الذي تتم إدارته
- اسم السياسة المفعلة أو خارج المكتب في لحظة تسليم السياسة إلى الجهاز الذي تتم إدارته
- الاسم والمسار الكامل لمجموعة الإدارة التي كانت تحتوي على الجهاز الذي تتم إدارته في لحظة تسليم السياسة إلى الجهاز الذي تتم إدارته
- قائمة ملفات تعريف السياسة المفعلة
- يمكنك استخدام المعلومات لضمان تطبيق السياسة الصحيحة على الجهاز ولأغراض استكشاف الأخطاء وإصلاحها. يتم تعطيل هذا الخيار افتراضياً.

• [حماية خدمة عميل الشبكة من عمليات الإزالة أو الإنهاء غير المصرح بها، ومنع إجراء تغييرات في الإعدادات](#)

بعد تثبيت عميل الشبكة على جهاز مُدار، يتعذر إزالة المكون أو إعادة تكوينه دون الامتيازات المطلوبة. يتعذر إيقاف خدمة عميل الشبكة. يتم تعطيل هذا الخيار افتراضياً.

• [استخدام كلمة مرور إلغاء التثبيت](#)

إذا تم تمكين هذا الخيار، فيمكنك تحديد كلمة المرور لإزالة تثبيت عميل الشبكة عن بُعد بالنقر فوق زر **تعديل**. يتم تعطيل هذا الخيار افتراضياً.

المستودعات

في القسم **المستودعات**، يمكنك تحديد أنواع الكائنات التي سيتم إرسال تفاصيلها من عميل الشبكة إلى خادم الإدارة. إذا كان تعديل بعض الإعدادات في هذا القسم ممنوعاً في سياسة عميل الشبكة، فلا يمكنك تعديلها.

• [تفاصيل عن التطبيقات التي تم تثبيتها](#)

• [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 افتراضياً. إنه متاح فقط لنظام التشغيل Windows.

• [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 افتراضياً. إنه متاح فقط لنظام التشغيل Windows.

• [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 وكيل الشبكة. يتم تمكين هذا الخيار افتراضياً. إنه متاح فقط لنظام التشغيل Windows. لإدارة تحديثات البرامج لبرامج Microsoft، استخدم خيار تفاصيل تحديثات Windows Update.

• تفاصيل سجل الأجهزة

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. الإعدادات الموجودة في قسم تحديثات البرنامج والثغرات الأمنية متوفرة فقط على الأجهزة التي تعمل بنظام Windows:

• [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 افتراضياً.

• يمكنك تقييد تحديثات Windows التي يمكن للمستخدمين تثبيتها على أجهزتهم يدوياً 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:

• [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 يدوياً، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلاً 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 قبلهم.

على سبيل المثال، قد ترغب أولاً 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 العمل.

عند تثبيت المستخدم لتحديثات Microsoft Windows Update يدويًا، فقد يتم تنزيل التحديثات من خوادم Microsoft بدلاً 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.

• **سليبي**

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 مجدداً، 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، فيستمر مسح الملفات التنفيذية ضوئياً للعثور على الثغرات الأمنية عند تشغيلها. يتم تمكين هذا الخيار افتراضيًا.

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. لا تتوفر الإعدادات الموجودة إلا في قسم إدارة إعادة التشغيل على الأجهزة التي تعمل بنظام التشغيل Windows:

• عدم إعادة تشغيل نظام التشغيل ④

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.

• إعادة تشغيل نظام التشغيل تلقائيًا عند الحاجة ⑤

يتم إعادة تشغيل الأجهزة العميل تلقائيًا دائمًا إذا كانت إعادة التشغيل مطلوبة لإكمال العملية. هذا الخيار مفيد للمهام على الأجهزة التي توفر عمليات إيقاف مؤقتة من منظمة في عملها (إيقاف التشغيل أو إعادة التشغيل).

• مطالبة المستخدم باتخاذ إجراء ⑥

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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضيًا.

• تكرار المطالبة كل (بالدقائق) ⑦

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.

• فرض إعادة التشغيل بعد (دقيقة) ⑧

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 ⑨

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 المستخدمون 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.

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. لا تتوفر الإعدادات الموجودة إلا في قسم مشاركة سطح المكتب لـ Windows على الأجهزة التي تعمل بنظام التشغيل Windows:

• تمكين التدقيق 9

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 افتراضياً.

• أقنعة الملفات التي ينبغي مراقبتها عند قراءتها 9

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 افتراضياً: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

• أقنعة الملفات التي ينبغي مراقبتها عند تعديلها 9

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 افتراضياً: *.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 9

إذا تم تمكين هذا الخيار، فإنه يتم تثبيت تصحيحات Kaspersky ذات حالة الموافقة غير محدد تلقائياً على الأجهزة المدارة على الفور بعد تنزيلها من خوادم التحديث. يتوفر التثبيت التلقائي للتصحيحات ذات الحالة غير المحددة للإصدار Kaspersky Security Center 10 Service Pack 2 والإصدارات اللاحقة.

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 افتراضياً.

• تنزيل التحديثات وقواعد بيانات مكافحة الفيروسات من خادم الإدارة مقدماً (مستحسن) 9

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، فإن يتصل عميل الشبكة بخادم الإدارة ولكنه سيوفر بدلاً 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 وفقاً لجدول مهمة تنزيل التحديث.

يتم تمكين هذا الخيار افتراضياً.

الشبكة

يتضمن القسم الشبكة ثلاثة أقسام فرعية:

• الاتصال

• ملفات تعريف الاتصال

• جدول الاتصال

في القسم الفرعي الاتصال، يمكنك تكوين الاتصال بخادم الإدارة وتمكين استخدام منفذ UDP وتحديد رقمه.

• في مجموعة إعدادات الاتصال بخادم الإدارة، يمكنك تكوين الاتصال بخادم الإدارة، وتحديد الفترة الزمنية للمزامنة بين أجهزة العميل وخادم الإدارة:

• الفاصل الزمني للمزامنة (بالدقائق)

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

• 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 منفذ UDP، اللازم لعمل عميل الشبكة، إلى قائمة استثناء جدار حماية Microsoft Windows. يتم تمكين هذا الخيار افتراضياً.

• استخدام اتصال SSL

في حال تمكين هذا الخيار، يتم إجراء الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL. يتم تمكين هذا الخيار افتراضياً.

• 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 افتراضياً.

• استخدام منفذ UDP

إذا احتجت أن تكون الأجهزة المُدارة متصلة بخادم وكيل KSN عبر منفذ UDP، فقم بتمكين خيار استخدام منفذ UDP وحدد رقم منفذ UDP. يتم تمكين هذا الخيار افتراضياً. والمنفذ الافتراضي لـ UDP للاتصال بخادم وكيل KSN هو 15111.

• 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 يدوياً.

• استخدم نقطة التوزيع لفرض الاتصال بخادم الإدارة

حدد هذا الخيار إذا كنت قد حددت خيار استخدام نقطة التوزيع هذه كخادم إرسال في نافذة إعدادات نقطة التوزيع. بخلاف ذلك، لن تعمل نقطة التوزيع كخادم إرسال.

في القسم الفرعي ملفات تعريف الاتصال بالقسم الشبكة، يمكنك تحديد إعدادات موقع الشبكة وتمكين وضع الوجود خارج المكتب عندما لا يكون خادم الإدارة متاح. لا تتوفر الإعدادات الموجودة في القسم ملفات تعريف الاتصال إلا على الأجهزة التي تعمل بنظام التشغيل Windows و macOS:

• 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 أيضاً 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 افتراضياً.

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 افتراضياً.

• **الاتصال في فواصل زمنية محددة**

إذا حددت هذا الخيار، يقوم عميل الشبكة بالاتصال بخادم الإدارة في فترات محددة. ويمكنك إضافة فترات زمنية متعددة للاتصال.

استقصاء الشبكة من خلال نقاط التوزيع

في قسم **استقصاء الشبكة من خلال نقاط التوزيع**، يمكنك تكوين الاستقصاء التلقائي للشبكة. تتوفر إعدادات الاستقصاء فقط على الأجهزة التي تعمل بنظام التشغيل Windows. يمكنك استخدام الخيارات التالية لتمكين الاستقصاء وتعيين تردده:

• **شبكة Windows**

إذا تم تمكين الخيار، فإن خادم الإدارة يجري استقصاء الشبكة تلقائياً وفقاً للجدول المُكوّن عن طريق النقر فوق الروابط **تعيين جدول استقصاء سريع** و**تعيين جدول استقصاء كامل**.

إذا تم تعطيل هذا الخيار، فلن يجري خادم الإدارة استقصاء الشبكة.

يمكن تكوين الفاصل الزمني لاكتشاف الجهاز لإصدارات عميل الشبكة السابقة لـ 10.2 في الحقول **معدل الاستقصاءات من مجالات Windows (دقيقة)** و**معدل استقصاءات الشبكة (بالدقائق)**. تتوفر الحقول إذا تم تمكين الخيار.

يتم تعطيل هذا الخيار افتراضياً.

• **شبكة لا تتطلب تكويناً**

إذا تم تمكين هذا الخيار، فتقوم نقطة التوزيع تلقائياً باستقصاء الشبكة باستخدام أجهزة IPv6 عن طريق **شيكات التكوين الصفري** (كما يشار إلى شبكة لا تتطلب تكويناً). في هذه الحالة، يتم تجاهل استقصاء نطاق IP الذي تم تمكينه، لأن نقطة التوزيع تستقصي الشبكة بالكامل.

لبدء استخدام شبكة لا تتطلب تكويناً، 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 افتراضياً.

• **نطاقات IP**

إذا تم تمكين الخيار، فإن خادم الإدارة يجري استقصاء نطاقات IP تلقائيًا وفقًا للجدول المُكوّن عن طريق النقر فوق الرابط **تعيين جدول الاستقصاء**. إذا تم تعطيل هذا الخيار، فلن يجري خادم الإدارة 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.

• [Active Directory](#) ⑤

إذا تم تمكين الخيار، فإن خادم الإدارة يجري 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.

إعدادات الشبكة لنقاط التوزيع

في قسم **إعدادات الشبكة لنقاط التوزيع**، يمكنك تحديد إعدادات الوصول إلى الإنترنت:

- استخدام الخادم الوكيل
- العنوان
- رقم المنفذ

• [تجاوز الخادم الوكيل للعناوين المحلية](#) ⑤

إذا تم تمكين هذا الخيار، فلن يتم استخدام خادم الوكيل للاتصال بالأجهزة على الشبكة المحلية. يتم تعطيل هذا الخيار افتراضيًا.

• [مصادقة الخادم الوكيل](#) ⑤

إذا تم تحديد خانة الاختيار تلك، فيمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال. يتم تعطيل خانة الاختيار هذه بشكل افتراضي.

- اسم المستخدم
- كلمة المرور

وكيل KSN (نقاط التوزيع)

في قسم **وكيل KSN (نقاط التوزيع)**، يمكنك تكوين التطبيق لاستخدام نقطة التوزيع لإعادة توجيه طلبات KSN من الأجهزة المدارة:

• [تمكين وكيل KSN من جانب نقطة التوزيع](#) ⑤

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. يوجد بيان KSN افتراضيًا في ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula%. يتم تعطيل هذا الخيار افتراضيًا. يسري تمكين هذا الخيار فقط في حالة **تمكين** الخيارين استخدام خادم الإدارة كخادم وكيل وأوافق على استخدام Kaspersky Security Network في نافذة خصائص خادم الإدارة. يمكنك تعيين عقدة مجموعة نشط-خامل إلى نقطة توزيع، وتمكين وكيل 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 / شبكة KSN الخاصة مباشرة عبر الإنترنت**

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المدارة إلى KSN Cloud أو شبكة KSN الخاصة. يتم أيضًا إرسال طلبات KSN – التي تم إنشاؤها على نقطة التوزيع نفسها – مباشرة إلى KSN Cloud أو KSN Private.

لا يمكن لنقاط التوزيع التي لديها الإصدار 11 المثبت لعملاء الشبكة (أو الأقدم)، الوصول إلى شبكة KSN الخاصة مباشرة. إذا كنت ترغب في إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KSN الخاصة، 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 شبكة KSN الخاصة مباشرة.

• **المنفذ**

رقم منفذ TCP الذي ستستخدمه الأجهزة المدارة للاتصال بخادم وكيل KSN. رقم المنفذ الافتراضي هو 13111.

• **منفذ UDP**

إذا احتجت أن تكون الأجهزة المدارة متصلة بخادم وكيل KSN عبر منفذ UDP، فقم بتمكين خيار **استخدام منفذ UDP** وحدد رقم منفذ UDP. يتم تمكين هذا الخيار افتراضيًا. والمنفذ الافتراضي لـ UDP للاتصال بخادم وكيل KSN هو 15111.

التحديثات (نقاط التوزيع)

في هذا القسم **التحديثات (نقاط التوزيع)** يمكنك تمكين **ميزة تنزيل الملفات المختلفة**، بحيث تأخذ نقاط التوزيع التحديثات في شكل ملفات مختلفة من خوادم تحديث Kaspersky.

سجل المراجعة

في علامة التبويب هذه، يمكنك عرض قائمة مراجعات السياسة و **الرجوع إلى التغييرات السابقة** التي تم إجراؤها على السياسة إذا لزم الأمر.

مقارنة الميزات من خلال أنظمة تشغيل عميل الشبكة

يوضح الجدول أدناه إعدادات سياسة عميل الشبكة التي يمكنك استخدامها لتكوين وكيل الشبكة مع نظام تشغيل محدد.

إعدادات نهج عميل الشبكة: المقارنة حسب أنظمة التشغيل

Linux	Mac	Windows	قسم السياسة
-------	-----	---------	-------------

✓	✓	✓	عام
✓	✓	✓	تكوين الحدث
✓ خيارات الحجم الأقصى لقائمة انتظار الحدث، بالميجابايت و يُسمح للتطبيق باسترداد بيانات السياسة الموسعة على الجهاز المتاحة فقط.	✓	✓	إعدادات
✓ تتوفر فقط خيارات تفاصيل عن التطبيقات التي تم تثبيتها وتفصيل سجلات الأجهزة .	—	✓	المستودعات
—	—	✓	تحديثات البرنامج والثغرات الأمنية
—	—	✓	إدارة إعادة التشغيل
—	—	✓	مشاركة سطح المكتب لـ Windows
—	—	✓	إدارة التصحيحات والتحديثات
✓ فيما عدا خيار فتح منافذ عميل الشبكة في جدار حماية Microsoft Windows .	✓	✓	الشبكة ← الاتصال
—	✓	✓	الشبكة ← ملفات تعريف الاتصال
✓	✓	✓	الشبكة ← جدول الاتصال
✓ لا تتوفر سوى خيارات شبكة لا تتطلب تكويناً ونطاقات IP.	—	✓ خيارات شبكة Windows ، نطاقات IP، و Active Directory المتاحة فقط.	استقصاء الشبكة من خلال نقاط التوزيع
✓	✓	✓	إعدادات الشبكة لنقاط التوزيع
—	—	✓	وكيل KSN (نقاط التوزيع)
—	—	✓	التحديثات (نقاط التوزيع)
✓	✓	✓	سجل المراجعة

الإعداد اليدوي لسياسة Kaspersky Endpoint Security

يقدم هذا القسم توصيات حول كيفية تكوين سياسة Kaspersky Endpoint Security التي يتم إنشاؤها بواسطة معالج البدء السريع لـ Kaspersky Security Center 14 Web Console. يتم إجراء الإعداد في نافذة خصائص السياسة.

عند تحرير إعداد ما، الرجاء مراعاة أنه يجب عليك النقر على أيقونة القفل فوق الإعداد ذي الصلة للسماح باستخدام القيمة الخاصة به على محطة العمل.

تكوين السياسة في قسم الحماية من التهديدات المتقدمة

يصف هذا القسم إجراءات إعداد إضافية نوصيك بإجرائها في نافذة خصائص السياسة في Kaspersky Endpoint Security for Windows، في قسم **الحماية من التهديدات المتقدمة**.

للحصول على وصف كامل للإعدادات الموجودة في هذا القسم، فبرجاء الرجوع إلى وثائق Kaspersky Endpoint Security for Windows.

لتحديد إعدادات KSN الموصى بها:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.
 2. انقر على سياسة Kaspersky Endpoint Security for Windows. سيتم فتح نافذة خصائص السياسة المحددة.
 3. في نافذة خصائص السياسة، اذهب إلى إعدادات التطبيق ← الحماية من التهديدات المتقدمة ← Kaspersky Security Network.
 4. تأكد أن خيار استخدام وكيل KSN مفعلاً. يساعد استخدام هذا الخيار في إعادة توزيع وتحسين حركة المرور على الشبكة.
 5. [اختياري] قم بتمكين استخدام خوادم KSN إذا لم يكن خدمة وكيل KSN متوفرة. قد تتواجد خوادم KSN إما على جانب Kaspersky (عند استخدام شبكة KSN العالمية) أو على جانب أطراف خارجية (عند استخدام شبكة KSN الخاصة).
 6. انقر على موافق.
- إعدادات KSN الموصى بها محددة.

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.

موضح أدناه إجراءات الإعداد الإضافية، والتي ننصحك بإجرائها في نافذة خصائص السياسة الخاصة بـ Kaspersky Endpoint Security for Windows، في قسم **الحماية من التهديدات الأساسية**.

قسم الحماية من التهديدات الأساسية، القسم الفرعي "جدار الحماية"

تحقق من قائمة الشبكات الموجودة في خصائص السياسة. قد لا تحتوي القائمة على كل الشبكات.

للتحقق من قائمة الشبكات:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.
2. انقر على سياسة Kaspersky Endpoint Security for Windows. سيتم فتح نافذة خصائص السياسة المحددة.

3. في نافذة خصائص السياسة، اذهب إلى إعدادات التطبيق ← الحماية من التهديدات الأساسية ← الجدار الناري.

4. ضمن الشبكات المتاحة، انقر فوق رابط إعدادات الشبكة.

ستفتح النافذة اتصالات الشبكة. تعرض هذه النافذة قائمة بالشبكات.

قسم الحماية من التهديدات الأساسية، القسم الفرعي الحماية من تهديدات الملفات

يمكن أن يؤدي تمكين 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 القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.

2. انقر على سياسة Kaspersky Endpoint Security for Windows.

سيتم فتح نافذة خصائص السياسة المحددة.

3. في نافذة خصائص السياسة، اذهب إلى إعدادات التطبيق ← الحماية من التهديدات الأساسية ← الحماية من تهديدات الملفات.

4. في نطاق الحماية، قم بتعطيل خيار كل محركات أقراص الشبكة.

5. انقر على موافق.

فحص محركات أقراص الشبكة معطل.

تكوين السياسة في قسم الإعدادات العامة

للحصول على وصف كامل للإعدادات الموجودة في هذا القسم، فارجع إلى وثائق Kaspersky Endpoint Security for Windows.

موضح أدناه إجراءات الإعداد المتقدمة، والتي ننصحك بإجرائها في نافذة خصائص السياسة الخاصة بـ Kaspersky Endpoint Security for Windows، في قسم الإعدادات العامة.

قسم الإعدادات العامة، القسم الفرعي التقارير وعمليات التخزين

لتعطيل حفظ المعلومات عن الوحدات النمطية للبرامج المثبتة:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.

2. انقر على سياسة Kaspersky Endpoint Security for Windows.

سيتم فتح نافذة خصائص السياسة المحددة.

3. في خصائص السياسة، اذهب إلى إعدادات التطبيق ← الإعدادات العامة ← التقارير والتخزين.

4. ضمن تحويل البيانات إلى خادم الإدارة، الغ تحديد خانة الاختيار حول التطبيقات التي تم بدؤها إذا كانت لا تزال ممكنة في سياسة المستوى الأعلى.

في حالة تمكين خانة الاختيار هذه، تقوم قاعدة بيانات خادم الإدارة بحفظ 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).

لن يتم حفظ المعلومات عن الوحدات النمطية للبرامج المثبتة بعد اللحظة في قاعدة بيانات خادم الإدارة.

قسم الإعدادات العامة، القسم الفرعي الواجهة

إذا كان يجب إدارة الحماية ضد الفيروسات على شبكة المنظمة في وضع مركزي من خلال وحدة تحكم الإدارة، حدد إعدادات الواجهة كما هو موصوف أدناه.

لتحديد إعدادات الواجهة الموصى بها:

1. في علامة التبويب **الأجهزة**، حدد **السياسات وملفات التعريف**.
 2. انقر على سياسة **Kaspersky Endpoint Security for Windows**. سيتم فتح نافذة خصائص السياسة المحددة.
 3. في خصائص السياسة، اذهب إلى **إعدادات التطبيق** ← **الإعدادات العامة** ← **الواجهة**.
 4. تحت **التفاعل مع المستخدم**، حدد خيار **لا توجد واجهة**. يقوم هذا بتعطيل عرض واجهة مستخدم Kaspersky Endpoint Security for Windows على محطات العمل.
 5. تحت **حماية كلمة المرور**، قم بتفعيل زر التبديل. يقلل هذا من خطر التغييرات غير المصرح بها أو غير المقصودة في إعدادات Kaspersky Endpoint Security for Windows على محطات العمل.
- الإعدادات الموصى بها لواجهة Kaspersky Endpoint Security for Windows محددة.

تكوين السياسة في القسم تكوين الحدث

لتجنب تجاوز سعة قاعدة بيانات خادم الإدارة، ننصح بالأحداث المهمة في قاعدة البيانات.

لتكوين تسجيل الأحداث المهمة في قاعدة بيانات خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **السياسات وملفات التعريف**.
2. انقر على سياسة **Kaspersky Endpoint Security for Windows**. سيتم فتح نافذة خصائص السياسة المحددة.
3. في خصائص السياسة، افتح علامة التبويب **تكوين الحدث**.
4. في قسم **حرج**، انقر على **إضافة حدث** وحدد خانة الاختيار الموجودة بجوار الأحداث التالية فقط:

- انتهاك اتفاقية الترخيص
- تم تعطيل التشغيل التلقائي للتطبيق
- خطأ في التفعيل
- تم اكتشاف تهديد نشط. بدء التنظيف المتقدم
- التنظيف غير ممكن

- تم اكتشاف رابط خطير تم فتحه مسبقاً
- تم إنهاء العملية
- تم حظر نشاط الشبكة
- تم اكتشاف هجوم على الشبكة
- تم حظر بدء التطبيق
- تم رفض الوصول (القواعد المحلية)
- تم رفض الوصول (KSN)
- خطأ في التحديث المحلي
- يتعذر تشغيل مهمتين في الوقت نفسه
- خطأ في التفاعل مع Kaspersky Security Center
- لم يتم تحديث كل المكونات
- خطأ في تطبيق قواعد تشفير / فك تشفير الملف
- خطأ في تمكين الوضع المحمول
- خطأ في تعطيل الوضع المحمول
- تعذر تحميل الوحدة النمطية للتشفير
- يتعذر تطبيق السياسة
- خطأ في تغيير مكونات التطبيق

5. انقر على موافق.

6. في قسم خلل وظيفي، انقر على إضافة حدث وحدد خانة الاختيار الموجودة بجوار الحدث "إعدادات المهمة غير الصالحة. لم يتم تطبيق الإعدادات" فقط.

7. انقر على موافق.

8. في قسم تحذير، انقر على إضافة حدث وحدد خانة الاختيار الموجودة بجوار الأحداث التالية فقط:

- تم تعطيل الدفاع الذاتي
- تم تعطيل مكونات الحماية
- مفتاح حجز غير صحيح
- برامج قانونية يمكن استخدامها في الإضرار بجهاز الكمبيوتر لديك أو تم اكتشاف بيانات شخصية (قواعد محلية)
- برامج قانونية يمكن استخدامها في الإضرار بجهاز الكمبيوتر لديك أو تم اكتشاف بيانات شخصية (KSN)
- تم حذف كائن
- تم تنظيف كائن

• قام المستخدم بإلغاء اشتراكه في سياسة التشفير

• تم استعادة ملف KATA من العزل

• تم نقل ملف KATA إلى العزل

• رسالة حظر بدء تشغيل التطبيق إلى المدير

• رسالة حظر وصول جهاز إلى المدير

• رسالة حظر وصول صفحة ويب إلى المدير

9. انقر على موافق.

10. في قسم معلومات، انقر على إضافة حدث وحدد خانة الاختيار الموجودة بجوار الأحداث التالية فقط:

• تم إنشاء نسخة احتياطية من الكائن

• تم حظر بدء التطبيق في وضع الاختبار

11. انقر على موافق.

تم تكوين تسجيل الأحداث المهمة في قاعدة بيانات خادم الإدارة.

الإعداد اليدوي لمهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security

إن خيار الجدولة الأمثل والموصى به لإصدار Kaspersky Endpoint Security هو عند تنزيل تحديثات جديدة إلى المستودع عندما تكون خانة الاختيار استخدام التأخير العشوائي لبدء المهام تلقائياً محددة.

منح الوصول دون اتصال إلى الجهاز الخارجي المحظور بواسطة التحكم في الجهاز

فيكون التحكم في الجهاز لسياسة Kaspersky Endpoint Security for Windows، يمكنك إدارة وصول المستخدم إلى الأجهزة الخارجية المثبتة على الجهاز العميل أو مرتبطة به (مثل محركات الأقراص الثابتة والكاميرات والوحدات النمطية لشبكات Wi-Fi). يتيح هذا لك حماية الجهاز العميل من التفاعل مع تلك الأجهزة الخارجية المتصلة ويمنع فقدان البيانات أو تسربها.

إذا كنت بحاجة إلى منع وصول مؤقت إلى الجهاز الخارجي المحظور عن طريق التحكم في الجهاز لكن ليس من الممكن إضافة الجهاز إلى قائمة الأجهزة الموثوقة، لا يزال بإمكانك منح وصول دون اتصال مؤقت إلى الجهاز الخارجي. الوصول دون اتصال يعني أن الجهاز العميل لا يملك وصولاً إلى الشبكة.

لا يمكنك منح وصول دون اتصال إلى الجهاز الخارجي المحظور بواسطة التحكم في الجهاز إلا إذا كان خيار السماح بطلب الوصول المؤقت مفعلاً في إعدادات سياسة Kaspersky Endpoint Security for Windows في قسم التحكم في الجهاز.

منح الوصول دون اتصال إلى الجهاز الخارجي المحظور بواسطة التحكم في الجهاز يشمل المراحل التالية:

1. في نافذة مربع الحوار في Kaspersky Endpoint Security for Windows، مستخدم الجهاز الذي يرغب في الوصول إلى الجهاز الخارجي المحظور يقوم بإنشاء ملف طلب وصول ويرسله إلى مدير Kaspersky Security Center.

2. بالحصول على هذا الطلب، يقوم مدير Kaspersky Security Center بإنشاء ملف مفتاح وصول ويرسله إلى مستخدم الجهاز.

3. في نافذة مربع الحوار في Kaspersky Endpoint Security for Windows، يقوم مستخدم الجهاز بتنشيط ملف مفتاح الوصول والحصول على وصول مؤقت إلى الجهاز الخارجي.

لمنح الوصول مؤقت إلى الجهاز الخارجي المحظور بواسطة التحكم في الجهاز:

1. حدد الأجهزة ← الأجهزة المُدارة.

يتم عرض قائمة الأجهزة المُدارة.

2. في قائمة بالأجهزة المُدارة، حدد جهاز المستخدم الذي يطلب الوصول إلى الجهاز الخارجي المحظور بواسطة التحكم في الجهاز.

لا يمكنك تحديد إلا جهاز واحد.

3. أعلى قائمة الأجهزة المُدارة، انقر على زر منح الوصول إلى الجهاز في وضع عدم الاتصال.

ستفتح نافذة منح الوصول في وضع عدم الاتصال.

4. في نافذة منح الوصول في وضع عدم الاتصال، من تبويب التحكم في الجهاز، انقر على زر استعراض.

ستفتح نافذة تحديد ملف طلب الوصول القياسية لنظام Microsoft Windows.

5. في نافذة تحديد ملف طلب الوصول، حدد ملف طلب الوصول الذي استلمته من المستخدم ثم انقر على زر فتح.

سيتم عرض تفاصيل الجهاز المقبول الذي طلب المستخدم الوصول إليه.

6. حدد قيمة إعداد مدة الوصول.

يحدد هذا الإعداد المدة التي ترغب في منح المستخدم الوصول إلى الجهاز المقبول خلالها. القيمة الافتراضية هي القيمة التي حددها المستخدم عند إنشاء ملف طلب الوصول.

7. حدد قيمة إعداد فترة التنشيط.

يحدد هذا الإعداد الفترة التي يمكن للمستخدم خلالها تنشيط الوصول إلى الجهاز المقبول باستخدام مفتاح الوصول المتوفر.

8. انقر على زر حفظ.

يفتح هذا نافذة حفظ مفتاح الوصول القياسية لنظام Microsoft Windows.

9. حدد المجلد الوجهة الذي ترغب أن تحفظ فيه الملف الذي يحتوي على مفتاح الوصول إلى الجهاز المقبول.

10. انقر على زر حفظ.

ونتيجةً لذلك، عندما ترسل إلى المستخدم ملف مفتاح الوصول ويقوم المستخدم بتنشيطه في النافذة الحوارية في Kaspersky Endpoint Security for Windows، عندها يملك المستخدم وصولاً مؤقتاً إلى الجهاز المقبول طوال الفترة المحددة.

إزالة تحديثات تطبيقات أو برامج عن بُعد

لإزالة تطبيقات أو تحديثات برامج عن بُعد من الأجهزة المحددة:

1. في نافذة التطبيق الرئيسية، اذهب إلى الأجهزة ← المهام.

2. انقر فوق إضافة.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام الزر التالي.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة إلغاء تثبيت التطبيق عن بُعد.

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:

• **قم بإلغاء تثبيت التطبيق المدار**

سيتم عرض قائمة بتطبيقات Kaspersky. حدد التطبيق الذي ترغب في إزالته.

• **إلغاء تثبيت التطبيق غير المتوافق**

ستظهر قائمة من التطبيقات غير المتوافقة مع تطبيقات أمان Kaspersky أو Kaspersky Security Center. حدد خانة الاختيار الموجودة بجوار التطبيقات التي ترغب في إزالتها.

• **إلغاء تثبيت التطبيق من سجل التطبيقات**

افتراضياً، 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 **التطبيق المراد إلغاء تثبيته** ثم حدد التطبيق الذي ترغب في إزالته.

b. حدد خيارات **إلغاء التثبيت**:

• **وضع إلغاء التثبيت**

حدد الطريقة التي ترغب في إزالة التطبيق بها:

• **تعريف أمر إلغاء التثبيت تلقائياً**

إذا كان للبرنامج أمر إلغاء تثبيت حدده بائع التطبيق، سيستخدم Kaspersky Security Center هذا الأمر. ننصح بتحديد هذا الخيار.

• **تحديد أمر إلغاء التثبيت**

حدد هذا الخيار إذا كنت ترغب في تحديد أمرك الخاص لإلغاء تثبيت التطبيق.

ننصح بأن تحاول أولاً إزالة التطبيق باستخدام خيار **تعريف أمر إلغاء التثبيت تلقائياً**. إذا تعذر إلغاء التثبيت من خلال الأمر المحدد تلقائياً، عندها استخدم أمرك الخاص.

اكتب أمر تثبيت في الحقل ثم حدد الخيار التالي:

استخدام هذا الأمر لإلغاء التثبيت فقط إذا لم يتم اكتشاف الأمر الافتراضي تلقائياً

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 **أمر إلغاء تثبيت التطبيق**.

ننصح بأن تقوم بتفعيل هذا الخيار.

• **إجراء إعادة التشغيل بعد إلغاء تثبيت التطبيق بنجاح**

إذا طلب التطبيق إعادة تشغيل نظام التشغيل على الجهاز المدار بعد إلغاء التثبيت بنجاح، سيتم إعادة تشغيل نظام التشغيل تلقائياً.

• إزالة تحديث لتطبيق محدد أو التصحيح الخاص به أو التطبيق التابع لجهة خارجية 5

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 الأجهزة.

يمكنك كذلك عرض قائمة بالتطبيقات والتحديثات المثبتة في نافذة خصائص الجهاز.

7. حدد كيف ستقوم أجهزة العميل بتنزيل أداة إلغاء التثبيت:

• استخدام عميل الشبكة 5

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.

• استخدام موارد النظام التشغيل من خلال خادم الإدارة 5

سيتم نقل الملفات إلى أجهزة العميل باستخدام أدوات Microsoft Windows عبر 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.

• استخدام موارد نظام التشغيل عبر نقاط التوزيع 5

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 استخدام عميل الشبكة مفعلاً، يتم تسليم الملفات باستخدام أدوات نظام التشغيل فقط في حالة عدم توفر أدوات عميل الشبكة.

• أقصى عدد من عمليات التنزيل المتزامنة 5

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.

• الحد الأقصى لعدد محاولات إلغاء التثبيت 5

عند تشغيل مهمة إلغاء تثبيت التطبيق عن بُعد، 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 الحد الأقصى لعدد محاولات إلغاء التثبيت 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 الحد الأقصى لعدد محاولات إلغاء التثبيت وبدء تشغيل المهمة لإلغاء تثبيت التطبيق. وكحل بديل، يمكنك إنشاء مهمة إلغاء تثبيت التطبيق عن بُعد جديدة.

• تحقق من نوع نظام التشغيل قبل التنزيل 8

قبل نقل الملفات إلى أجهزة العميل، يتحقق Kaspersky Security Center مما إذا كانت إعدادات أداة إلغاء التثبيت قابلة للتطبيق على نظام تشغيل الجهاز العميل أم لا. إذا لم تكن الإعدادات قابلة للتطبيق، لا ينقل Kaspersky Security Center الملفات ولا يحاول إلغاء تثبيت التطبيق. على سبيل المثال: لإلغاء تثبيت تطبيق على نظام Windows من أجهزة في مجموعة إدارة تشمل أجهزة تعمل بعدة أنظمة تشغيل مختلفة، يمكنك تعيين مهمة إلغاء التثبيت إلى مجموعة الإدارة ثم تفعيل هذا الخيار من أجل تخطي الأجهزة التي تعمل بنظام تشغيل غير نظام Windows.

8. حدد إعدادات إعادة تشغيل نظام التشغيل:

• لا تقم بإعادة تشغيل الجهاز 9

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.

• إعادة تشغيل الجهاز 9

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 9

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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضيًا.

• تكرار المطالبة كل (بالدقائق) 9

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) 9

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد. يتم تمكين هذا الخيار افتراضياً. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

• **فرض إغلاق التطبيقات في الجلسات المحظورة** 9

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 المستخدم 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 يدوياً وإعادة تشغيل هذه الأجهزة. يتم تعطيل هذا الخيار افتراضياً.

9. أضف الحسابات التي سيتم استخدامها لبدء مهمة إلغاء التثبيت عن بُعد إذا كان ذلك ضرورياً:

• **لا يلزم وجود حساب (تم تثبيت عميل الشبكة)** 9

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 كيل الشبكة على الأجهزة العميلة، فلن يتوفر هذا الخيار.

• **يلزم وجود حساب (عميل الشبكة غير مستخدم)** 9

إذا تم تحديد هذا الخيار، فيمكنك تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. يمكنك تحديد الحساب إذا لم يتم تثبيت عميل الشبكة على الأجهزة التي تم تعيين المهمة لها. يمكنك تحديد حسابات مستخدمين متعددة، على سبيل المثال، في حالة عدم امتلاك أي منها لجميع الحقوق الموضحة على جميع الأجهزة التي تم تحديد هذه المهمة من أجلها. في هذه الحالة، يتم استخدام جميع الحسابات التي تمت إضافتها لتشغيل المهمة بترتيب متعاقب من الأعلى إلى الأسفل. في حالة عدم إضافة أي حساب، سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

10. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **فتح تفاصيل المهمة عند اكتمال الإنشاء** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقاً في أي وقت.

11. انقر على زر **إنهاء**.

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 **حفظ**.

15. قم بتشغيل المهمة يدوياً أو انتظر إلى أن يتم البدء وفقاً للجدول الذي حددته أنت في إعدادات المهمة.

بمجرد إكمال مهمة إلغاء التثبيت عن بُعد، ستتم إزالة التطبيق المحدد من الأجهزة المحددة

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 **سجل المراجعة**.

2. في قائمة مراجعات الكائنات، حدد المراجعة التي ترغب في التراجع عن تغييراتها.

3. انقر على زر **التراجع**.

4. انقر على **موافق 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.

تغيير أولوية قواعد نقل الجهاز

كل قواعد نقل الأجهزة **تحتوي على أولويات**:

لزيادة أو تقليل أولوية قاعدة متحركة:

حرك القاعدة لأعلى أو لأسفل في القائمة، على التوالي، باستخدام الماوس.

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.

يمكن إنشاء مهام لتطبيق محدد باستخدام Kaspersky Security Center 14 Web Console فقط في حالة تثبيت مكونات الإدارة لهذا التطبيق على خادم Kaspersky Security Center 14 Web Console.

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 أي 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، و عرض 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 بتغيير 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 دائماً وفق جدول بواسطة خادم الإدارة. لا يمكن أن تعمل هذه المهام على أجهزة غير متصلة بخادم الإدارة. إن المهام التي تم تحديدها 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 تحديدها باستخدام وسائل أخرى يتم تنفيذها في الوقت المحلي لجهاز ما.

إنشاء مهمة

لإنشاء مهمة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

2. انقر فوق **إضافة**.

يبدأ تشغيل معالج إضافة مهمة. اتبع تعليماته.

3. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **فتح تفاصيل المهمة عند اكتمال الإنشاء** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقاً في أي وقت.

4. انقر على زر **إنهاء**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

بدء مهمة يدوياً

يبدأ التطبيق المهام وفق إعدادات الجدول المحددة في خصائص كل مهمة. يمكنك بدء مهمة يدوياً في أي وقت.

لبدء مهمة يدوياً:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

2. في قائمة المهمة، حدد خانة الاختيار الموجودة بجوار المهمة التي ترغب في بدنها.

3. انقر فوق الزر **بدء**.

تبدأ المهمة. يمكنك التحقق من حالة المهمة في عمود **الحالة** أو بالنقر على زر **النتيجة**.

عرض قائمة المهام

يمكنك عرض قائمة المهام التي تم إنشاؤها في Kaspersky Security Center.

لعرض قائمة المهام،

في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

يتم عرض قائمة المهام. يتم تجميع المهام بأسماء التطبيقات التي ترتبط بها. على سبيل المثال: مهمة إلغاء تثبيت التطبيق عن بُعد متعلقة بخادم الإدارة، ومهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة 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 **نوع المهمة** في تبويب عام، ويتم عرض جدول المهمة في تبويب الجدول.

إعدادات المهمة العامة

يذكر هذا القسم الإعدادات التي يمكنك عرضها وتحديدتها للمهام.

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.

• إعادة 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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة 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 افتراضياً. 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 المستخدم 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 يدوياً وإعادة تشغيل هذه الأجهزة. يتم تعطيل هذا الخيار افتراضياً.

• إعدادات جدولة المهام:

• البدء المُجدول

حدد الجدول الذي تعمل المهمة وفقاً 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 ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• كل N يوماً

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 أسبوعاً

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.

• يومياً (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. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 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 تمكين 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، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• [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 المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• 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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تمكين 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 المترامنة 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 المترامنة 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 المحاسيبين 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.

• إعدادات الحساب:

• **الحساب الافتراضي**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه. يتم تحديد هذا الخيار افتراضيًا.

• **تعيين حساب**

املاً حقلي الحساب وكلمة 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:

• التوزيع للمجموعات الفرعية ٩

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 افتراضياً.

• توزيع إلى خوادم الإدارة الثانوية والافتراضية ٩

عند تمكين هذا الخيار، يتم أيضاً 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 افتراضياً.

• إعدادات الجدولة المتقدمة:

• تفعيل الجهاز قبل بدء المهمة عبر Wake On LAN (بالدقائق) ٩

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 العملية من نطاق المهام، بما في ذلك تلك الأجهزة التي تم إيقاف تشغيلها عندما تكون المهمة على وشك البدء.
إذا كنت تريد إيقاف تشغيل الجهاز تلقائياً بعد اكتمال المهمة، فقم بتمكين خيار أغلق الأجهزة بعد الانتهاء من المهمة. يمكن العثور على هذا الخيار في النافذة نفسها.
يتم تعطيل هذا الخيار افتراضياً.

• قم بإيقاف تشغيل الجهاز بعد اكتمال المهمة ٩

على سبيل المثال، قد ترغب في تمكين هذا الخيار لمهمة تحديث تثبيت والتي تقوم بتثبيت التحديثات على الأجهزة العملية كل يوم جمعة بعد ساعات العمل، ثم تقوم بإيقاف تشغيل هذه الأجهزة لعطلة نهاية الأسبوع.
يتم تعطيل هذا الخيار افتراضياً.

• أوقف المهمة إذا كانت تعمل لمدة أطول من (دقيقة) ٩

بعد انتهاء الفترة الزمنية المحددة، يتم إيقاف المهمة تلقائياً، سواء أكانت مكتملة أم لا.
قم بتمكين هذا الخيار إذا كنت تريد مقاطعة (أو إيقاف) المهام التي تستغرق وقتاً طويلاً للتنفيذ.
يتم تعطيل هذا الخيار افتراضياً. وقت تنفيذ المهمة الافتراضي هو 120 دقيقة.

• إعدادات الإخطار:

• الكتلة تخزين محفوظات المهمة

• **تخزين في قاعدة البيانات الخاصة بخادم الإدارة لمدة (بالأيام) 9**

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 افتراضياً.

• **تخزين في سجل أحداث نظام التشغيل (OS) على جهاز 9**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة محلياً في سجل أحداث Windows لكل جهاز عميل.
يتم تعطيل هذا الخيار افتراضياً.

• **تخزين في سجل أحداث نظام التشغيل (OS) على خادم إدارة 9**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة على جميع الأجهزة العميلة من نطاق المهام مركزياً في سجل أحداث Windows لنظام تشغيل خادم الإدارة (OS).
يتم تعطيل هذا الخيار افتراضياً.

• **حفظ كل الأحداث 9**

إذا تم تحديد هذا الخيار، فسيتم حفظ جميع الأحداث المتعلقة بالمهمة في سجلات الأحداث.

• **حفظ الأحداث المتعلقة بتقدم المهمة 9**

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بتنفيذ المهمة في سجلات الأحداث.

• **حفظ نتائج تنفيذ المهمة فقط 9**

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بنتائج المهمة في سجلات الأحداث.

• **قم بإخطار المسؤول بنتائج تنفيذ المهمة 9**

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 9**

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 افتراضياً.

• إعدادات الأمن

• إعدادات نطاق المهمة

اعتماداً على كيفية تحديد نطاق المهام، تكون الإعدادات التالية موجودة:

• الأجهزة ④

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 ④

يمكنك تغيير تحديد الجهاز الذي يتم تطبيق المهمة عليه.

• الاستثناءات من نطاق المهمة ④

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

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 وفقاً 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.

يمكنك "معالج تغيير كلمة مرور المهام" من استبدال كلمة المرور القديمة تلقائياً بكلمة مرور جديدة في جميع المهام التي يتم فيها تحديد الحساب. بدلاً من ذلك، يمكنك تغيير كلمة المرور هذه يدوياً في خصائص كل مهمة.

لبدء تشغيل معالج تغيير كلمة مرور المهام:

1. في علامة التبويب الأجهزة، حدد المهام.

2. انقر على إدارة بيانات اعتماد الحسابات لبدء المهام.

اتبع إرشادات المعالج.

الخطوة 1. تحديد بيانات الاعتماد

حدد بيانات اعتماد جديدة صالحة حالياً في نظامك (في Active Directory مثلاً). عندما تقوم بالتبديل إلى الخطوة التالية من المعالج، يتحقق Kaspersky Security Center ما إذا كان اسم الحساب المحدد مطابقاً لاسم الحساب في خصائص كل مهمة غير محلية. في حالة تطابق أسماء الحساب، يتم استبدال كلمة المرور في خصائص المهمة تلقائياً بكلمة المرور الجديدة.

لتحديد الحساب الجديد، حدد خياراً:

• استخدام الحساب الحالي ④

يستخدم المعالج اسم الحساب الذي قمت بتسجيل الدخول من خلاله حاليًا إلى Kaspersky Security Center 14 Web Console. بعدها حدد كلمة مرور الحساب يدويًا في حقل كلمة المرور الحالية المستخدمة في المهام.

• تحديد حساب مختلف

حدد اسم الحساب التي يجب بدء المهام من خلاله. بعدها حدد كلمة مرور الحساب في حقل كلمة المرور الحالية المستخدمة في المهام.

إذا كنت تملأ حقل كلمة المرور السابقة (اختيارية، إذا كنت تريد استبدالها بكلمة المرور الحالية)، 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 لاتخاذها في الخطوة التالية من المعالج.

الخطوة 2. اختيار إجراء لاتخاذها

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 لاتخاذها للمهام التي تم العثور عليها.

لاختيار إجراء المهمة:

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 حذف بيانات الاعتماد.
- ستتحوّل المهمة إلى العمل عبر الحساب الافتراضي.
- لاستبدال كلمة المرور بأخرى جديدة، انقر على فرض تغيير كلمة المرور حتى إذا كانت كلمة المرور القديمة خاطئة أو لم يتم توفيرها.
- لإلغاء تغيير كلمة المرور، انقر على لم يتم تحديد الإجراء.

سيتم تطبيق الإجراءات التي تم اختيارها بعد أن تنتقل إلى الخطوة التالية من المعالج.

الخطوة 3. عرض النتائج

في الخطوة الأخيرة من المعالج، قم بعرض النتائج لكل المهام التي تم العثور عليها. لإكمال المعالج، انقر فوق الزر إنهاء.

إدارة الأجهزة العميلة

يصف هذا القسم كيفية إدارة الأجهزة في مجموعات الإدارة.

إعدادات جهاز مدار

لعرض إعدادات جهاز مدار:

1. حدد الأجهزة ← الأجهزة المُدارة.

يتم عرض قائمة الأجهزة المُدارة.

2. في قائمة بالأجهزة المُدارة، انقر على الرابط الذي يحمل اسم الجهاز المطلوب.

يتم عرض نافذة خصائص الجهاز المحدد.

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.

• **المجموعة**

مجموعة الإدارة التي تتضمن الجهاز العميل.

• **تاريخ آخر تحديث**

تحديد تاريخ آخر تحديث لقواعد البيانات 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، فسيتم فصل 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 ممكنًا حتى إذا حاولت تعطيله.

الشبكة

يعرض قسم الشبكة 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.

النظام

يوفر قسم النظام معلومات عن نظام التشغيل المثبت على الجهاز العميل.

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 للفيروسات أُجري على الجهاز العميل.

• **إجمالي عدد التهديدات المكتشفة**

العدد الإجمالي للتهديدات المكتشفة على الجهاز العميل منذ تثبيت تطبيق مكافحة الفيروسات (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.

حالة الجهاز المحددة من خلال التطبيق

يوفر القسم حالة الجهاز المحددة بواسطة التطبيق المعلومات المتعلقة بحالة الجهاز التي حددها التطبيق المُدار المُثبت على الجهاز. يمكن لحالة الجهاز هذه أن تختلف عن الحالة المحددة في Kaspersky Security Center.

التطبيقات

يدرج قسم **التطبيقات** جميع تطبيقات Kaspersky المثبتة على الجهاز العميل. يمكنك النقر على اسم التطبيق لعرض معلومات عامة عن التطبيق وقائمة بالأحداث التي حدثت على الجهاز وإعدادات التطبيق.

السياسات النشطة وملفات تعريف السياسة

قسم **السياسات المفعلة وملفات تعريف السياسات** يدرج السياسات وملفات تعريف السياسة المفعلة حاليًا على الجهاز المُدار.

المهام

في القسم **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. إذا لم يتم إنشاء الاتصال، فلا يتم عرض الحالة.

أحداث

يعرض القسم **الأحداث** المسجلة على خادم الإدارة للجهاز العميل المحدد.

الحوادث

في القسم **الحوادث**، يمكنك عرض الحوادث وتحريرها وإنشاؤها للجهاز العميل. يمكن إنشاء الحوادث 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 حادث. يمكن للمسؤول توفير وصف مختصر للحالة والإجراءات الموصى بها (مثل الإجراءات التأديبية التي سيتم اتخاذها ضد المستخدم) في نص الحادث، ويمكنه إضافة رابط للمستخدم أو المستخدمين.

يُطلق على حادث تم اتخاذ جميع الإجراءات المطلوبة بشأنه اسم تمت المعالجة. قد يتم اختيار وجود حوادث غير معالجة كشرط لتغيير حالة الجهاز إلى حرج أو تحذير.

يحتوي هذا القسم على قائمة بالحوادث التي تم إنشاؤها للجهاز. يتم تصنيف الحوادث بحسب مستوى الخطورة وبحسب النوع. يتم تحديد نوع الحادث بواسطة تطبيق Kaspersky، الذي يقوم بإنشاء الحادث. يمكنك تمييز الحوادث التي تمت معالجتها في القائمة عن طريق تحديد خانة الاختيار الموجودة في العمود **تمت المعالجة**.

العلامات

في القسم **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.

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**. يتم توفير معلومات حول التطبيقات المثبتة للأجهزة التي تعمل بنظام تشغيل Windows فقط.

يوفر عميل الشبكة معلومات حول التطبيقات اعتمادًا على البيانات التي يتم استلامها من سجل النظام.

النقر على اسم التطبيق يفتح نافذة تحتوي على تفاصيل التطبيق وقائمة بحزم التثبيت المثبتة للتطبيق.

الملفات التنفيذية

يعرض القسم **الملفات التنفيذية** الملفات التنفيذية التي تم العثور عليها على الجهاز العميل.

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.

سجل الأجهزة

في القسم **سجل الأجهزة**، يمكنك عرض معلومات عن الأجهزة المثبتة على الجهاز العميل. يمكنك عرض هذه المعلومات لأجهزة Windows وأجهزة Linux.

التحديثات المتوفرة

يعرض هذا القسم تحديثات البرامج التي تم العثور عليها على هذا الجهاز والتي لم يتم تثبيتها بعد.

• [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 افتراضياً.

الثغرات الأمنية بالبرامج

يوفر القسم الثغرات الأمنية بالبرنامج معلومات حول الثغرات الأمنية في تطبيقات الجهة الخارجية المثبتة على أجهزة العميل.

لحفظ الثغرات الأمنية في ملف، حدد خانة الاختيار الموجودة بجوار الثغرات الأمنية التي ترغب في حفظها ثم انقر على زر تصدير الصفوف إلى ملف CSV أو زر تصدير الصفوف إلى ملف TXT.

يحتوي قسم الثغرات الأمنية بالبرنامج 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 افتراضياً.

• [خصائص الثغرة الأمنية](#)

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 وحدة تحكم الويب الخاصة بـ [Kaspersky Security Center 14](#)).
- عرض قائمة الإصلاحات الموصى بها للثغرة الأمنية.
- حدد تحديثات البرامج يدوياً لإصلاح الثغرات الأمنية (في وحدة تحكم الإدارة أو في [Kaspersky Security Center 14 Web Console](#)).
- عرض مثيلات الثغرات الأمنية.
- عرض قائمة المهام الحالية لإصلاح الثغرات الأمنية وإنشاء مهام جديدة لإصلاح الثغرات الأمنية.

إنشاء مجموعات إدارة

فوراً بعد تثبيت Kaspersky Security Center، الترتيب الهرمي لمجموعات الإدارة لا يحتوي إلا على مجموعة إدارة واحدة اسمها الأجهزة المُدارة. عند إنشاء ترتيب هرمي لمجموعات الإدارة، يمكنك إضافة أجهزة، بما في ذلك الأجهزة الظاهرية، إلى مجموعة الأجهزة المُدارة وكذلك إضافة المجموعات المتداخلة (انظر الشكل أدناه).

<input type="checkbox"/>	Administration group
▼ <input type="checkbox"/>	Managed devices
▼ <input type="checkbox"/>	klst-group-0
<input type="checkbox"/>	klst-group-0-0
<input type="checkbox"/>	klst-group-1
<input type="checkbox"/>	klst-group-2

عرض الترتيب الهرمي لمجموعات الإدارة

لإنشاء مجموعة إدارة:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← التسلسل الهرمي للمجموعات.

2. في هيكل مجموعة الإدارة، حدد مجموعة الإدارة التي ستشمل مجموعة الإدارة الجديدة.

3. انقر على زر إضافة.

4. في نافذة اسم مجموعة الإدارة الجديدة التي تفتح، أدخل اسمًا للمجموعة، ثم انقر على زر إضافة.

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 الأجهزة ← التسلسل الهرمي للمجموعات.

2. انقر فوق زر استيراد.

بدء 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 الأجهزة ← الأجهزة المُدارة.

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 إضافة جهاز.

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 **إضافة جهاز** ثم حدد الأجهزة بإحدى الطرق التالية:
- حدد أجهزة من قائمة الأجهزة التي اكتشفها خادم الإدارة.
- حدد عنوان IP لجهاز أو نطاق IP.
- حدد اسم NetBIOS أو اسم DNS لجهاز.

يجب ألا يحتوي حقل اسم الجهاز على مسافات بين الأحرف أو الأحرف المحظورة التالية: \ / * ; : ~ ! @ # \$ % ^ & () = + [] { } | . < > %

- انقر على زر **استيراد الأجهزة من ملف** 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 **التالي**.

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 إلى مجموعة إدارة يدويًا

يمكنك نقل أجهزة من مجموعة إدارة إلى أخرى أو من مجموعة الأجهزة غير المخصصة إلى مجموعة إدارة.

لنقل جهاز أو عدة أجهزة إلى مجموعة إدارة محددة:

1. افتح مجموعة الإدارة التي ترغب في نقل أجهزة منها. لفعل هذا، قد بأحد الإجراءات التالية:

- لفتح مجموعة إدارة، انتقل إلى **الأجهزة** ← **المجموعات** ← **اسم المجموعة** ← **الأجهزة المُدارة**.
- لفتح مجموعة الأجهزة غير المخصصة، انتقل إلى **الاكتشاف والنشر** ← **الأجهزة غير المخصصة**.

2. حدد خانة الاختيار الموجودة بجوار الأجهزة التي ترغب في نقلها إلى مجموعة أخرى.

3. انقر على زر **نقل إلى مجموعة**.

4. في التسلسل الهرمي لمجموعات الإدارة، حدد خانة الاختيار الموجودة بجوار مجموعة الإدارة التي ترغب في نقل الأجهزة المحددة إليها.

5. انقر فوق الزر **نقل**.

يتم نقل الأجهزة المحددة إلى مجموعة الإدارة المحددة.

إنشاء قواعد نقل الجهاز

يمكنك تعيين قواعد نقل الجهاز التي تقوم تلقائيًا بتخصيص الأجهزة لمجموعات الإدارة.

لإنشاء قاعدة نقل:

1. في القائمة الرئيسية، انتقل إلى تبويب الأجهزة ← قواعد النقل.

2. انقر فوق إضافة.

3. في النافذة التي تفتح، حدد المعلومات التالية في تبويب عام:

• اسم القاعدة

أدخل اسمًا للقاعدة الجديدة.

إذا كنت تنسخ قاعدة، ستحصل القاعدة الجديدة على نفس اسم قاعدة المصدر، ولكن يُضاف فهرس بتنسيق () إلى الاسم، مثل: (1).

• مجموعة الإدارة

حدد مجموعة الإدارة التي سيتم نقل الأجهزة إليها تلقائيًا.

• تطبيق قاعدة

يمكنك تحديد أي من الخيارات التالية:

- قم بالتشغيل مرة واحدة لكل جهاز.
يتم تطبيق القاعدة مرة واحدة لكل جهاز يتوافق مع معاييرك.
- قم بالتشغيل مرة واحدة لكل جهاز ثم عند كل إعادة تثبيت لعميل الشبكة.
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.
- تنطبق القاعدة بشكل مستمر.
يتم تطبيق القاعدة وفقًا للجدول الزمني الذي يقوم خادم الإدارة بإعداده تلقائيًا (كل عدة ساعات في العادة).

• نقل الأجهزة فقط التي لا تنتمي لمجموعة إدارة

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.

• تمكين القاعدة

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.

4. يمكنك إذا كنت ترغب أن تحدد معايير الأجهزة التي ترغب في نقلها تلقائيًا، وذلك في تبويب حالات القاعدة.

يتم إنشاء قاعدة النقل. يتم عرضها في قائمة قواعد النقل. كلما كان الموضع أعلى في القائمة، كانت أولوية القاعدة أعلى: 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. في القائمة الرئيسية، انتقل إلى تبويب الأجهزة ← قواعد النقل. يمكنك كذلك تحديد الاكتشاف والنشر ← التوزيع والتعيين، ثم من القائمة حدد قواعد النقل. يتم عرض قائمة قواعد النقل.
2. حدد خانة الاختيار الموجودة بجوار القاعدة التي ترغب في نسخها.
3. انقر على نسخ.
4. في النافذة التي تفتح، قم بتغيير المعلومات التالية في تبويب عام أو لا تقم بأي تغييرات إذا كنت لا ترغب إلا في نسخ القاعدة دون تغيير إعداداتها:

• اسم القاعدة

أدخل اسمًا للقاعدة الجديدة.

إذا كنت تنسخ قاعدة، ستحصل القاعدة الجديدة على نفس اسم قاعدة المصدر، ولكن يُضاف فهرس بتنسيق () إلى الاسم، مثل: (1).

• مجموعة الإدارة

حدد مجموعة الإدارة التي سيتم نقل الأجهزة إليها تلقائيًا.

• تطبيق قاعدة

يمكنك تحديد أي من الخيارات التالية:

- قم بالتشغيل مرة واحدة لكل جهاز. يتم تطبيق القاعدة مرة واحدة لكل جهاز يتوافق مع معاييرك.
- قم بالتشغيل مرة واحدة لكل جهاز ثم عند كل إعادة تثبيت لعميل الشبكة. 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.
- تنطبق القاعدة بشكل مستمر. يتم تطبيق القاعدة وفقًا للجدول الزمني الذي يقوم خادم الإدارة بإعداده تلقائيًا (كل عدة ساعات في العادة).

• نقل الأجهزة فقط التي لا تنتمي لمجموعة إدارة

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.

• **تمكين القاعدة** ⑤

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.

5. يمكنك إذا كنت ترغب أن تحدد معايير الأجهزة التي ترغب في نقلها تلقائيًا، وذلك في تبويب **حالات القاعدة**.

6. انقر على **حفظ**.

تم إنشاء قاعدة النقل الجديدة. يتم عرضها في قائمة قواعد النقل.

عرض وتكوين الإجراءات عندما تكون حالة الأجهزة غير نشطة

إذا كانت الأجهزة العملية 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 **الأجهزة** ← **التسلسل الهرمي للمجموعات**.

2. انقر على اسم مجموعات الإدارة المطلوبة.

سنتفتح نافذة خصائص مجموعة الإدارة.

3. في نافذة الخصائص، انتقل إلى تبويب **إعدادات**.

4. قم بتفعيل الخيارات التالية أو تعطيلها في قسم **اكتساب خصائص**:

• **توريث من المجموعة الأصلية** ⑤

سيتم توريث الإعدادات الموجودة في هذا القسم من المجموعة الرئيسية التي تم تضمين الجهاز العميل بها. إذا تم تمكين هذا الخيار، فسيتم نقل 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 توريث الإعدادات في السياسات الفرعية** ⑤

سيتم توزيع قيم الإعدادات إلى المجموعات الفرعية ولكن في خصائص المجموعات الفرعية يتم نقل هذه الإعدادات.
يتم تعطيل هذا الخيار افتراضيًا.

5. قم بتفعيل الخيارات التالية أو تعطيلها في قسم **نشاط الجهاز**:

• **إخطار المسؤول إذا ظل الجهاز غير نشط لمدة تزيد عن (بالأيام) 7**

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 افتراضياً.

• **إزالة الجهاز من المجموعة إذا ظل غير نشط لمدة تزيد عن (بالأيام) 7**

إذا تم تمكين هذا الخيار، فيمكنك تحديد الفترة الزمنية التي يتم بعدها إزالة الجهاز تلقائياً من المجموعة. الفاصل الزمني الافتراضي هو 60 أيام. يتم تمكين هذا الخيار افتراضياً.

6. انقر فوق حفظ.

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 لجهاز ما، يأخذ Kaspersky Security Center في الاعتبار علامة رؤية الجهاز على الشبكة (انظر الجدول أدناه). 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

القيم المتوفرة	وصف الشرط	الشرط
<ul style="list-style-type: none"> • زر التبديل قيد التشغيل. • زر التبديل متوقف. 	عميل الشبكة مثبت على الجهاز، إلا أن تطبيق الأمان غير مثبت.	تطبيق الأمان غير مثبت
أكثر من 0.	تم العثور على بعض الفيروسات على الجهاز عن طريق تنفيذ إحدى مهام اكتشاف الفيروسات، على سبيل المثال مهمة فحص الفيروسات، ويتجاوز عدد الفيروسات التي تم العثور عليها القيمة المحددة.	تم اكتشاف العديد من الفيروسات
<ul style="list-style-type: none"> • متوقف. • متوقف مؤقتاً. • قيد التشغيل. 	الجهاز مرئي على الشبكة، إلا أن مستوى الحماية في الوقت الحقيقي يختلف عن المستوى الذي حدده المسؤول (في الشرط) لحالة الجهاز.	يختلف مستوى الحماية في الوقت الحقيقي عن المستوى الذي تم تعيينه من قبل المسؤول

أكثر من يوم واحد.	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز ، إلا أنه لم يتم تشغيل مهمة فحص الفيروسات خلال الفاصل الزمني المحدد. لا ينطبق الشرط إلا على الأجهزة التي تمت إضافتها إلى قاعدة بيانات خادم الإدارة قبل 7 أيام أو أكثر.	لم يتم إجراء فحص الفيروسات منذ وقت طويل
أكثر من يوم واحد.	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.	قواعد البيانات قديمة
أكثر من يوم واحد.	يتم تثبيت عميل الشبكة على الجهاز ، ولكن لم يتم اتصال الجهاز بخادم الإدارة خلال الفاصل الزمني المحدد نظرًا لإيقاف تشغيل الجهاز.	لم يتم الاتصال منذ فترة طويلة
أكثر من 0 عناصر.	يتجاوز عدد الكائنات التي لم تتم معالجتها في المجلد تهديدات نشطة القيمة المحددة.	تم اكتشاف تهديدات نشطة
أكثر من 0 دقائق.	الجهاز مرئي على الشبكة، إلا إن أحد التطبيقات يتطلب إعادة تشغيل الجهاز لمدة أطول من الفاصل الزمني المحدد ولأحد الأسباب المحددة.	إعادة التشغيل مطلوبة
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	الجهاز مرئي على الشبكة، إلا إن مخزون البرنامج المنفذ عبر عميل الشبكة قد اكتشف تطبيقات غير متوافقة مثبتة على الجهاز.	تم تثبيت تطبيقات غير متوافقة
<ul style="list-style-type: none"> حرج. مرتفع. متوسط. تجاهل إذا تعذر إصلاح الثغرات الأمنية. تجاهل إذا تم تعيين تحديث للتثبيت. 	الجهاز مرئي على الشبكة و عميل الشبكة مثبت على الجهاز ، إلا أن مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة قد اكتشفت وجود ثغرات أمنية بمستوى الخطورة المحدد في التطبيقات المثبتة على الجهاز.	تم اكتشاف ثغرات أمنية بالبرنامج
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	الجهاز مرئي على الشبكة، إلا إن الترخيص قد انتهى.	انتهت صلاحية الترخيص
أكثر من 0 أيام.	الجهاز مرئي على الشبكة، إلا أن الترخيص سينتهي على الجهاز خلال فترة أقل من عدد الأيام المحدد.	سنتتهي فترة صلاحية الترخيص قريباً
أكثر من يوم واحد.	الجهاز مرئي على الشبكة، إلا أنه لم يتم تشغيل مهمة إجراء مزامنة Windows Update خلال الفاصل الزمني المحدد.	لم يتم إجراء البحث عن تحديثات تحديث Windows منذ وقت طويل
<ul style="list-style-type: none"> لا تتفق مع السياسة بسبب رفض المستخدم (بالنسبة للأجهزة الخارجية فقط). لا تتوافق مع السياسة بسبب وجود خطأ. 	عميل الشبكة مثبت على الجهاز ، إلا إن نتيجة تشفير الجهاز مساوية للقيمة المحددة.	حالة تشفير غير صالحة

<ul style="list-style-type: none"> إعادة التشغيل مطلوبة عند تطبيق السياسة. لم يتم تحديد سياسة تشفير. غير مدعوم عند تطبيق السياسة. 		
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	إعدادات الجهاز المحمول تختلف عن الإعدادات المحددة في سياسة Kaspersky Endpoint Security for Android أثناء التحقق من قواعد الامتثال.	لا تتوافق إعدادات الجهاز المحمول مع السياسة
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	تم العثور على بعض الأحداث التي لم تتم معالجتها على الجهاز. يمكن إنشاء الحوادث إما تلقائيًا من خلال تطبيقات Kaspersky المُدارة المثبتة على الجهاز العميل أو يدويًا من قبل المسؤول.	تم اكتشاف حوادث لم تتم معالجتها
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	تم تحديد حالة الجهاز بواسطة التطبيق المدار.	حالة الجهاز المحددة بواسطة التطبيق
أكثر من 0 ميجابايت	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.	نفدت مساحة قرص الجهاز
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	أثناء اكتشاف الأجهزة، تم التعرف على الجهاز بأنه مرئي على الشبكة، لكن فشلت أكثر من ثلاث محاولات للمزامنة مع خادم الإدارة.	أصبح الجهاز غير مُدار
أكثر من 0 دقائق.	الجهاز مرئي على الشبكة، إلا إنه قد تم تعطيل تطبيق الأمان على الجهاز لمدة أطول من الفاصل الزمني المحدد.	تم تعطيل الحماية
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لا يعمل.	تطبيق الأمان ليس 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 قواعد البيانات قديمة 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 قواعد البيانات قديمة لتخصيص الحالة تتغير إلى حرجة أو تحذير أو لا تتغير.

عندما يقوم Kaspersky Security Center بتعيين حالة إلى جهاز، يتم أخذ علامة الرؤية في الاعتبار بالنسبة لبعض الشروط (راجع عمود وصف الحالة). على سبيل المثال: إذا تم تعيين الحالة حرج إلى جهاز مُدار بسبب عدم استيفاء شرط قواعد البيانات قديمة ثم بعد ذلك تم تعيين علامة الرؤية للجهاز، يتم تعيين حالة موافق إلى الجهاز.

تكوين تبديل حالات الجهاز

يمكنك تغيير الشروط لتعيين الحالة حرجة أو تحذير لجهاز 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 النافذة خصائص التي تفتح في الجزء 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. حدد القيمة المطلوبة للحالة المحددة.

يمكنك تعيين قيم لبعض الشروط، ولكن ليس جميعها.

5. انقر على موافق.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار على 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. من النافذة خصائص المهمة التي تفتح، في الجزء 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. حدد القيمة المطلوبة للحالة المحددة.

يمكنك تعيين قيم لبعض الشروط، ولكن ليس جميعها.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار على 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 و UDP بالجهاز العميل.

عند إنشاء اتصال مع الجهاز، يكون للمسؤول حق الوصول الكامل للمعلومات المخزنة 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 أدواتان:

- أداة كاسبيرسكي تسمى klsctunnel. يجب تخزين هذه الأداة على محطة عمل المسؤول. يمكنك استخدام هذه الأداة المساعدة لربط الاتصال بين جهاز عميل و خادم 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 مثبت 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 و خادم 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 بسطح المكتب عن بُعد عبر أداة Windows القياسية mstsc.exe وفقًا لإعدادات الأداة.
- تم إنشاء اتصال بجلسة سطح المكتب البعيد للحالية 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 14 Web Console، انتقل إلى الأجهزة ← الأجهزة المُدارة ← المجموعات، ثم حدد مجموعة الإدارة التي تحتوي على الجهاز الذي تريد الوصول إليه.
5. حدد خانة الاختيار بجوار اسم الجهاز الذي تريد الوصول إليه.

6. انقر على زر الاتصال بسطح المكتب البعيد.

يتم فتح النافذة سطح المكتب البعيد (نظام Windows فقط).

7. 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.

8. انقر على زر تنزيل لتنزيل الأداة المساعدة klsctunnel.

9. انقر على زر نسخ إلى الحافظة 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 سطح المكتب البعيد (نظام Windows فقط) لإنشاء BLOB جديد.

10. قم بتشغيل الأداة المساعدة klsctunnel.

يتم فتح نافذة الأداة.

11. قم بلصق النص المنسوخ في حقل النص.

12. إذا كنت تستخدم الخادم الوكيل، فحدد خانة الاختيار استخدام الخادم الوكيل، ثم حدد إعدادات اتصال الخادم الوكيل.

13. انقر فوق زر فتح المنفذ.

يتم فتح نافذة تسجيل دخول اتصال سطح المكتب عن بُعد.

14. حدد بيانات اعتماد الحساب الذي قمت بتسجيل الدخول من خلاله حاليًا إلى وحدة تحكم الويب Kaspersky Security Center 14.

15. 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 و UDP 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 مثبت عليه وحدة تحكم الإدارة إلى منفذ TCP على جهاز مُدار—في حالة عدم إمكانية الاتصال المباشر بين وحدة تحكم الإدارة والجهاز المستهدف.

نق 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. للتحقق مما إذا كانت ميزة مشاركة سطح المكتب لـ Windows مضمنة في إصدار Windows، تأكد من تضمين -32BE5ED2-5C86-CLSID {480F-A914-OFF8885A1B3F} في التسجيل 32 بت.

- يتم تثبيت Microsoft Windows Vista أو إصدار أحدث على الجهاز العميل.

- يستخدم Kaspersky Security Center ترخيصًا لإدارة الثغرات الأمنية والتصحیحات.

للاتصال بسطح مكتب جهاز عميل من خلال مشاركة سطح المكتب لـ Windows:

1. في وحدة تحكم الإدارة المعتمدة على MMC، في قائمة السياق ل خادم 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** ممكن.
4. في Kaspersky Security Center 14 Web Console، انتقل إلى **الأجهزة** ← **الأجهزة المُدارة** ← **المجموعات**، ثم حدد مجموعة الإدارة التي تحتوي على الجهاز الذي تريد الوصول إليه.

5. حدد خانة الاختيار بجوار اسم الجهاز الذي تريد الوصول إليه.

6. انقر على زر **مشاركة سطح المكتب لـ Windows**.

يتم فتح معالج مشاركة سطح المكتب لـ Windows.

7. انقر على زر **تنزيل** لتنزيل أداة klsctunnel المساعدة، وانتظر اكتمال عملية التنزيل.

إذا كان لديك بالفعل أداة klsctunnel المساعدة، فتخط هذه الخطوة.

8. انقر فوق زر **التالي**.

9. حدد الجلسة على الجهاز الذي تريد الاتصال به، ثم انقر فوق زر **التالي**.

10. 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.

11. انقر على زر **نسخ إلى الحافظة** 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.

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.

يتم بدء مشاركة سطح المكتب في نافذة جديدة. إذا كنت ترغب في التفاعل مع الجهاز، فانقر فوق رمز القائمة () في الزاوية العلوية اليسرى من النافذة، ثم حدد الوضع التفاعلي.

تحديدات الأجهزة

تحديدات الأجهزة هي أداة لتصنيف 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 مسبقاً) (مثل الأجهزة بحالة "حرجة"، تم تعطيل الحماية، تم اكتشاف تهديدات نشطة). لا يمكن حذف التحديدات المحددة مسبقاً. يمكنك كذلك إنشاء وتكوين تحديدات من تعريف المستخدم إضافية.

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.

لعرض تحديد الجهاز:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← تحديدات الأجهزة أو قسم الاكتشاف والنشر ← تحديدات الأجهزة.

2. في قائمة التحديد، انقر على اسم التحديد ذي الصلة.

سيتم عرض نتيجة تحديد الجهاز.

إنشاء تحديد جهاز

لإنشاء تحديد جهاز:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← تحديدات الأجهزة.

سيتم عرض صفحة بقائمة تحديدات الأجهزة.

2. انقر على زر إضافة.

ستفتح نافذة إعدادات تحديد الجهاز.

3. أدخل اسم التحديد الجديد.

4. حدد نوع الأجهزة التي ترغب في إدراجها في تحديد الجهاز.

5. انقر على زر إضافة.

6. في النافذة التي تفتح، حدد الشروط التي يجب تحقيقها لتضمين الأجهزة في هذا التحديد ثم انقر على زر موافق.

7. انقر على زر حفظ.

يتم إنشاء تحديد الجهاز وإضافته إلى قائمة تحديدات الأجهزة.

تكوين تحديد جهاز

لتكوين تحديد جهاز:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← تحديدات الأجهزة.

سيتم عرض صفحة بقائمة تحديدات الأجهزة.

2. انقر على تحديد الجهاز الذي حدده المستخدم ذو الصلة.

سنفتح نافذة إعدادات تحديد الجهاز.

3. في تبويب عام، حدد الشروط التي يجب تحقيقها لتضمين الأجهزة في هذا التحديد.

4. انقر على زر حفظ.

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

إذا تم تمكين هذا الخيار، فسيتم عكس حالة التحديد المحددة. سيتضمن التحديد جميع الأجهزة التي لا تتوافق مع الحالة. يتم تعطيل هذا الخيار افتراضياً.

الشبكة

في القسم الشبكة، يمكنك تحديد المعايير التي ستستخدم لتضمين الأجهزة في التحديد وفقاً لبيانات الشبكة الخاصة بهم:

• اسم الجهاز أو عنوان IP

اسم الجهاز الموجود في شبكة Windows (اسم NetBIOS)

• 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 وظاهري، 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 موجوداً في النص.

مثال:

للبحث عن عبارة تحتوي على الكلمة المركبة الخادم التابع، أدخل "الخادم التابع" في الاستعلام.

• نطاق IP ٩

إذا تم تمكين هذا الخيار، فيمكنك إدخال عناوين IP الأولية والنهائية لنطاق IP الذي يجب تضمين الأجهزة ذات الصلة فيه.
يتم تعطيل هذا الخيار افتراضياً.

العلامات

في القسم العلامات، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على الكلمات المفتاحية (العلامات) التي تمت إضافتها سابقاً إلى أوصاف الأجهزة المدارة:

• تطبيق في حالة مطابقة علامة محددة واحدة على الأقل ٩

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 افتراضياً.

• **يجب تضمين العلامة** ④

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 افتراضياً.

• **يجب استثناء العلامة** ④

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** ④

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من وحدة Active Directory المحددة في حقل الإدخال.
يتم تعطيل هذا الخيار افتراضياً.

• **تضمين وحدات تنظيمية تابعة** ④

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من الوحدات التنظيمية التابعة للوحدة التنظيمية المحددة Active Directory.
يتم تعطيل هذا الخيار افتراضياً.

• **هذا الجهاز عضو في مجموعة Active Directory** ④

إذا تم تمكين هذا الخيار، فسوف يتضمن التحديد أجهزة من مجموعة Active Directory المحددة في حقل الإدخال.
يتم تعطيل هذا الخيار افتراضياً.

نشاط الشبكة

في القسم **نشاط الشبكة** يمكنك تحديد المعايير التي ستستخدم لتضمين الأجهزة في التحديد وفقاً لنشاط الشبكة الخاص بهم:

• **هذا الجهاز هو عبارة عن نقطة توزيع** ④

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 ⑤

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- مُمكن. 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 ⑤

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 ⑤

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 ⑤

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 ⑤

- في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختبار عند إجراء البحث:
- نعم. يشمل التطبيق في الاختيار الأجهزة المرئية في الوقت الحالي على الشبكة.
- لا. يشمل التطبيق في الاختيار 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 ④

- 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 ④

- 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 ④

- في حقل الإدخال، يمكنك تحديد معيار للأجهزة المشمولة في التحديد عند إجراء بحث باسم التطبيق أو برقم حزمة التحديث. إذا تم ترك الحقل فارغاً، لن يتم تطبيق المعيار.

آخر تحديث للوحدات ④

- 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 14 ④

- 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 ⑨

- 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 ستستخدم لتضمين الأجهزة في التحديد وفقاً لنوع نظام التشغيل الخاص بهم.

• إصدار نظام التشغيل ⑨

إذا تم تحديد خانة الاختبار، فيمكنك تحديد نظام تشغيل من القائمة. يتم تضمين الأجهزة المثبت عليها أنظمة التشغيل المحددة في نتائج البحث.

• حجم نظام التشغيل بالبت ⑨

في القائمة المنسدلة، يمكنك تحديد بنية نظام التشغيل والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز (غير معروف، AMD64، x86 أو IA64). وبشكل افتراضي، لا يتم تحديد أي خيار في القائمة ومن ثم لا يتم تحديد بنية نظام التشغيل.

• إصدار حزمة خدمة نظام التشغيل ⑨

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 ⑨

لا يكون هذا الإعداد قابلاً 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 أيضاً تكوين البحث عن جميع أرقام النسخة باستثناء الرقم المحدد.

• معرف تحرير نظام التشغيل ⑨

لا يكون هذا الإعداد قابلاً 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 أيضاً 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 خانة 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 افتراضياً.

• عدد سجلات قاعدة البيانات

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 افتراضياً.

• عملية الفحص الأخيرة

إذا تم تمكين هذا الخيار، فيمكنك البحث عن أجهزة العميل حسب وقت آخر فحص للفيروسات. في حقول الإدخال، يمكنك تحديد الفترة الزمنية التي تم فيها آخر فحص للفيروسات. يتم تعطيل هذا الخيار افتراضياً.

• 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 افتراضياً.

سجل التطبيقات

في القسم سجل التطبيقات، يمكنك إعداد معايير البحث عن الأجهزة وفقاً للتطبيقات المثبتة عليها:

• اسم التطبيق ④

القائمة المنسدلة التي يمكنك فيها تحديد أي تطبيق. يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

• إصدار التطبيق ④

يمكنك في حقل الإدخال تحديد إصدار التطبيق المحدد.

• المورد ④

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة لأي تطبيق مثبت على الجهاز.

• حالة التطبيق ④

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 ④

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 وإصدار التطبيق وحالة التطبيق إلى اسم التحديث وإصدار التحديث والحالة على التوالي. يتم تعطيل هذا الخيار افتراضياً.

• اسم تطبيق الأمان غير المتوافق ④

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 ④

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 ④

إذا تم تمكين هذا الخيار، فسيتم تضمين تحديد أجهزة أوصافها لا تحتوي على أي من العلامات المحددة.

إذا تم تعطيل هذا الخيار، فلن يتم تطبيق المعيار.

يتم تعطيل هذا الخيار افتراضياً.

سجل الأجهزة

في القسم سجل الأجهزة، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناء على الأجهزة المثبتة:

• الجهاز ④

يمكنك في القائمة المنسدلة تحديد نوع الوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث. يدعم الحقل البحث بالنص الكامل.

• [المورد](#)

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 ⑤

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 ⑤

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 ⑤

نطاق القيم لحجم ذاكرة الوصول العشوائي للجهاز. سيتم تضمين الأجهزة التي تحتوي على ذاكرة الوصول العشوائي، والتي تطابق النطاق في حقوق الإدخال هذه (ضمنياً) في التحديد.

الأجهزة الظاهرية

في القسم الأجهزة الظاهرية، يمكنك إعداد المعايير لتضمين الأجهزة في التحديد بناءً على ما إذا كانت تعد أجهزة ظاهرية أو جزءاً من البنية الأساسية لسطح المكتب الافتراضي (VDI):

• هذا جهاز ظاهري ⑤

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- ليس هاماً.
- لا. البحث عن الأجهزة التي لا تعد أجهزة ظاهرية.
- نعم. البحث عن الأجهزة التي تعد أجهزة ظاهرية.

• نوع الجهاز الظاهري ⑤

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة للجهاز الظاهري.

هذه القائمة المنسدلة متاحة إذا تم تحديد القيمة نعم أو ليس هاماً تم تحديد القيمة هذا جهاز ظاهري في القائمة المنسدلة.

• جزء من البنية الأساسية لسطح المكتب الافتراضي ⑤

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- ليس هاماً.
- لا. البحث عن الأجهزة التي لا تعد جزءاً من البنية الأساسية لسطح المكتب الافتراضي.
- نعم. البحث عن الأجهزة التي تعد جزءاً من البنية الأساسية لسطح المكتب الافتراضي (VDI).

الثغرات الأمنية والتحديثات

في القسم الثغرات الأمنية والتحديثات، يمكنك تحديد المعايير التي ستستخدم لتضمين الأجهزة في التحديد وفقاً لمصدر Windows Update الخاص بها:

• تم تبديل WUA إلى خادم الإدارة ④

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، فستشتمل النتائج على 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 ④

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 ④

إذا تم تمكين هذا الخيار، فانقر فوق زر استعراض لتحديد حساب مستخدم. ستضمن 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 ستستخدم لتضمين الأجهزة في التحديد وفقاً 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 تلقائياً.

• وصف حالة الجهاز ④

يمكنك تحديد خانة 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 تلقائياً.

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 ④

البحث عن الأجهزة حسب حالة منع تسريب البيانات (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتاً، قيد التشغيل، فشل).

• حالة الحماية الخاصة بتعاون الخوادم ④

البحث عن الأجهزة حسب حالة حماية تعاون الخادم (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتاً، قيد التشغيل، فشل).

• حالة الحماية ضد الفيروسات الخاصة بخوادم البريد ④

البحث عن الأجهزة حسب حالة حماية خادم البريد (لا توجد بيانات من الجهاز، متوقف، يجري البدء، متوقف مؤقتًا، قيد التشغيل، فشل).

• [حالة أداة استشعار نقطة النهاية](#)

البحث عن الأجهزة حسب حالة المكون أداة استشعار نقطة النهاية (لا توجد بيانات من الجهاز، 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: AES56 وAES128 وAES192 وAES256.

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.

• [يتم 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 يمكن اكتشاف الجهاز باستخدام AWS API أو Azure API أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة ولكن لا يمكن اكتشافه باستخدام API لسبب ما.
- دون قيمة. يتعذر تطبيق هذا المعيار.

مكونات التطبيق

يحتوي هذا القسم على قائمة المكونات لهذه التطبيقات التي لديها مكونات إدارة إضافية مطابقة مثبتة في وحدة تحكم الإدارة.

في القسم مكونات التطبيق، يمكنك تحديد معايير لتضمين الأجهزة في تحديد وفقاً للحالات ولأرقام الإصدار المكونات التي تشير للتطبيق الذي حددته:

• الحالة ⑤

البحث عن الأجهزة وفقاً لحالة المكون المرسله بواسطة تطبيق إلى خادم الإدارة. يمكنك تحديد أحد الحالات التالية: لا بيانات من الجهاز، أو متوقف، أو بدء التشغيل، أو تم إيقاف مؤقتاً، أو قيد التشغيل، أو اختلال تشغيل أو غير مثبت. إذا كان للمكون المحدد للتطبيق المثبت على جهاز مُدار حالة محددة، فإنه يتم تضمين الجهاز في تحديد الجهاز.

الحالات المرسله بواسطة التطبيقات:

- بدء تشغيل—يكون المكون في عملية التهيئة في الوقت الحالي.
- قيد التشغيل—يكون المكون ممكناً ويعمل على النحو الصحيح.
- تم إيقاف مؤقتاً—تم تعليق المكون، على سبيل المثال، بعد إيقاف المستخدم للحماية مؤقتاً في التطبيق المُدار.
- اختلال التشغيل—حدث خطأ أثناء تشغيل المكون.
- متوقف—تم تعطيل المكون وهو لا يعمل في الوقت الحالي.
- غير مثبت—لم يتم 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 ⑤

البحث عن الأجهزة وفقاً لرقم الإصدار للمكون الذي حددته في القائمة. يمكنك كتابة رقم الإصدار، على سبيل المثال 0.1.4.3، ثم تحديد ما إذا كان المكون المحدد يجب أن يمتلك إصداراً مماثلاً أو إصداراً سابقاً أو إصداراً أحدث. يمكنك أيضاً تكوين البحث عن جميع الإصدارات عدا الإصدار المحدد.

علامات الجهاز

يصف هذا القسم علامات الجهاز ويوفر تعليمات لإنشائها وتعديلها وكذلك لوضع علامات على الأجهزة يدوياً أو تلقائياً.

حول 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 يدوياً أو تلقائياً. يمكنك استخدام وضع العلامات يدوياً عندما ترغب في وضع علامة على جهاز محدد. يتم إجراء وضع العلامات التلقائي بواسطة Kaspersky Security Center وفقاً لقواعد وضع العلامات المحددة.

يتم وضع العلامات على الأجهزة تلقائياً 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: 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. سيساعدك هذا في ترتيب جميع الأجهزة الظاهرية من Microsoft Azure وتعيين مهمة لها.

يتم إزالة علامة تلقائياً 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 الأجهزة ← العلامات ← علامات الجهاز.

2. انقر فوق إضافة.

ستفتح نافذة علامة جديدة.

3. في حقل علامة، أدخل اسم العلامة.

4. انقر على حفظ لحفظ التغييرات.

تظهر العلامة الجديدة في قائمة علامات الجهاز.

إعادة تسمية علامة جهاز

لإعادة تسمية علامة جهاز:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← العلامات ← علامات الجهاز.

2. انقر على اسم العلامة التي ترغب في إعادة تسميتها.

ستفتح نافذة الخصائص.

3. في حقل علامة، قم بتغيير اسم العلامة.

4. انقر على حفظ لحفظ التغييرات.

تظهر العلامة المحدثة في قائمة علامات الجهاز.

حذف علامة جهاز

لحذف علامة جهاز:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← العلامات ← علامات الجهاز.

2. حدد زر الراديو بجوار علامة الجهاز التي ترغب في حذفها.

3. انقر فوق الزر حذف.

4. في النافذة التي تفتح، انقر على نعم.

سيتم حذف علامة الجهاز. يتم إزالة العلامة المحذوفة بشكل تلقائي من جميع الأجهزة التي تخصصها إليها.

لا يتم إزالة العلامة التي حذفها بشكل تلقائي من قواعد وضع العلامات تلقائيًا. بعد حذف العلامة، لا يتم تخصيصها إلى جهاز جديد إلا عندما يفى الجهاز بمتطلبات قاعدة تخصص العلامة.

عرض الأجهزة التي تم تعيين علامة لها

لعرض الأجهزة التي تم تعيين علامة لها:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **العلامات** ← **علامات الجهاز**.
 2. انقر على رابط **عرض الأجهزة** بجوار العلامة التي ترغب في عرض الأجهزة المخصصة لها. إذا لم تر رابط **عرض الأجهزة** بجوار علامة، هذا يعني عدم تخصيص العلامة لأي أجهزة. قائمة الأجهزة التي تظهر لا تعرض إلا تلك الأجهزة التي تم تخصيص العلامة لها.
- للعودة إلى قائمة علامات الجهاز، انقر على زر **العودة** لمستعرضك.

عرض العلامات المعينة إلى جهاز

لعرض العلامات المعينة إلى جهاز:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **الأجهزة المُدارة**.
 2. انقر على اسم الجهاز الذي ترغب في عرض علاماته.
 3. في النافذة خصائص الجهاز التي تُفتح، حدد علامة التبيويب **العلامات**.
- يتم عرض قائمة العلامات المعينة للجهاز المحدد.
- يمكنك **تخصيص علامة أخرى** إلى الجهاز أو **إزالة علامة مخصصة بالفعل**. يمكنك كذلك رؤية جميع علامات الجهاز الموجودة على خادم الإدارة.

وضع علامة على جهاز يدويًا

لتخصيص علامة إلى جهاز يدويًا:

1. اعرض العلامات المخصصة للجهاز الذي ترغب في تخصيص علامة أخرى له.
 2. انقر فوق **إضافة**.
 3. في النافذة التي تفتح، قم بأحد الإجراءات التالية:
- لإنشاء علامة جديدة وتخصيصها، حدد **إنشاء علامة جديدة** ثم حدد اسم العلامة الجديدة.
 - لتحديد علامة موجودة، حدد **تعيين علامة موجودة** ثم حدد العلامة الضرورية في القائمة المنسدلة.

4. انقر على موافق لتطبيق التغييرات.

5. انقر على حفظ لحفظ التغييرات.

يتم تخصيص العلامة المحددة إلى الجهاز.

إزالة علامة معينة من جهاز

لإزالة علامة من جهاز:

1. اعرض العلامات المخصصة للجهاز الذي ترغب في إزالة علامة منه.

2. حدد خانة الاختيار الموجودة بجوار العلامة التي ترغب في إزالتها.

3. انقر على زر إلغاء تعيين العلامة.

4. في النافذة التي تفتح، انقر على نعم.

يتم إزالة العلامة من الجهاز.

لا يتم حذف علامة الجهاز غير المخصصة. يمكنك، إذا كنت ترغب، حذفها يدويًا.

عرض قواعد وضع العلامات على الأجهزة تلقائيًا

لعرض قواعد وضع العلامات على الأجهزة تلقائيًا،

قم بأحد الإجراءات التالية:

- في القائمة الرئيسية، انتقل إلى الأجهزة ← العلامات ← قواعد وضع العلامات تلقائيًا.
 - في القائمة الرئيسية، انتقل إلى الأجهزة ← العلامات، ثم انقر فوق رابط إعداد قواعد وضع العلامات تلقائيًا.
 - اعرض العلامات المخصصة لجهاز ثم انقر على زر إعدادات.
- 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 اسم القاعدة.

يتعذر أن يكون الاسم أكثر من 256 حرفاً.

b. قم بأحد الإجراءات التالية:

• قم بتمكين القاعدة عن طريق تبديل زر التبديل إلى تم تمكين القاعدة.

• قم بتعطيل القاعدة عن طريق تبديل زر التبديل إلى تم تعطيل القاعدة.

4. قم بأحد الإجراءات التالية:

• إذا كنت ترغب في إضافة شرط جديد، انقر على زر **إضافة** 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 **حذف**.

5. انقر على **موافق** في نافذة إعدادات الشروط.

6. انقر على **حفظ** لحفظ التغييرات.

تظهر القاعدة التي تم تحريرها في القائمة.

إنشاء قاعدة لوضع علامات على الأجهزة تلقائياً

لإنشاء قاعدة لوضع علامات على الأجهزة تلقائياً:

1. **اعرض قواعد وضع العلامات على الأجهزة تلقائياً.**

2. انقر فوق **إضافة**.

سنفتح نافذة إعدادات قاعدة جديدة.

3. قم بتكوين الخصائص العامة للقاعدة:

a. أدخل اسم القاعدة في حقل اسم القاعدة.

يتعذر أن يكون الاسم أكثر من 256 حرفاً.

b. قم بأحد الإجراءات التالية:

• قم بتمكين القاعدة عن طريق تبديل زر التبديل إلى تم تمكين القاعدة.

• قم بتعطيل القاعدة عن طريق تبديل زر التبديل إلى تم تعطيل القاعدة.

c. أدخل اسم علامة الجهاز الجديدة في حقل **علامة** أو حدد واحدة من علامات الجهاز الموجودة من القائمة.

يتعذر أن يكون الاسم أكثر من 256 حرفاً.

4. انقر على زر **إضافة** في قسم الشروط من أجل إضافة شرط جديد.

سنفتح نافذة إعدادات شرط جديد.

5. أدخل اسم الشرط.

يتعذر أن يكون الاسم أكثر من 256 حرفاً. يجب أن يكون الاسم فريداً داخل القاعدة.

6. قم بإعداد بدء تشغيل القاعدة حسب الشروط التالية. يمكنك تحديد العديد من الشروط.

- **الشبكة:** خصائص الشبكة للجهاز، مثل اسم الجهاز في شبكة Windows، أو تضمين الجهاز في مجال أو شبكة IP فرعية.
- **التطبيقات** – وجود عميل الشبكة على الجهاز ونوع نظام التشغيل والإصدار والبنية.
- **الأجهزة الظاهرية:** الأجهزة التي تنتمي إلى نوع معين من الأجهزة الظاهرية.
- **Active Directory** – وجود الجهاز في الوحدة التنظيمية لـ Active Directory، وعضوية الجهاز في مجموعة Active Directory.
- **سجل التطبيقات** – وجود تطبيقات لبايعين مختلفين على الجهاز.

7. انقر فوق **موافق** لحفظ التغييرات.

يمكنك إعداد العديد من الشروط لقاعدة واحدة إن لزم الأمر. في هذه الحالة، سيتم تعيين العلامة إلى الجهاز عند استيفائه لشروط واحد على الأقل.

8. انقر على **حفظ** لحفظ التغييرات.

يتم فرض تطبيق القاعدة التي تم إنشاؤها حديثاً 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 يدوياً**

• بعد أن يكتشف خادم الإدارة تغييراً في إعدادات جهاز يفرض شروط 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 تلقائياً

عند تشغيل قاعدة، العلامة المحددة في خصائص هذه القاعدة يتم تخصيصها إلى الأجهزة التي تلي القواعد المحددة في خصائص القاعدة نفسها. يمكنك لا يمكنك تشغيل إلا القواعد المفعلة.

لتنشغيل قواعد وضع العلامات على الأجهزة تلقائياً:

1. **عرض قواعد وضع العلامات على الأجهزة تلقائياً.**

2. حدد خانة الاختيار الموجودة بجوار القواعد المفعلة التي ترغب في تشغيلها.

3. انقر على زر **تشغيل القاعدة.**

سيتم تشغيل القواعد المحددة.

حذف قاعدة لوضع علامات على الأجهزة تلقائياً

لحذف قاعدة لوضع علامات على الأجهزة تلقائياً:

1. إعرض قواعد وضع العلامات على الأجهزة تلقائيًا.

2. حدد خانة الاختيار الموجودة بجوار القاعدة التي ترغب في حذفها.

3. انقر على **حذف**.

4. في النافذة التي تفتح، انقر على **حذف** 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.

السياسات وملفات تعريف السياسة

يمكنك في Kaspersky Security Center 14 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

الوصف	الحالة
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.	نشطة
سياسة غير مطبقة حاليًا على جهاز.	غير نشطة
إذا تم تحديد هذا الخيار، تصبح السياسة نشطة عندما يغادر الجهاز شبكة الشركة.	خارج المكتب

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 الحماية ضد 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 الإعدادات والسياسة وإعدادات ملفات تعريف السياسة وإعدادات التطبيق المحلية المطبقة حالياً للجهاز.

تعمل ملفات التعريفية للسياسة وفقاً 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 <input type="checkbox"/>	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 <input checked="" type="checkbox"/>	في حال عرض قفل مقفول بجوار إعداد وكان زر التبديل مفعلاً، هذا الإعداد مطبق على الأجهزة التي تسيّر 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 المؤمنة من خلال إعدادات تطبيق Kaspersky على جهاز مُدار.

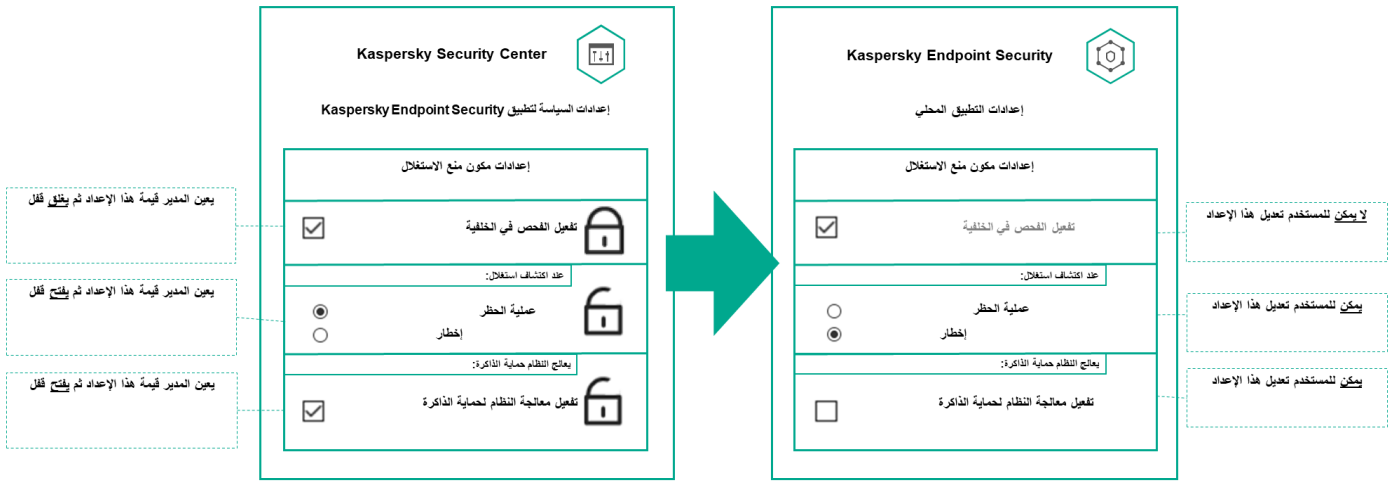
يمكنك استخدام زر قفل لإجراء الإجراءات التالية:

- 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.

السياسة وتطبيق Kaspersky المحلي يحتويان على نفس مجموعة الإعدادات. عندما تقوم بتكوين إعدادات السياسة، إعدادات تطبيق Kaspersky تغير 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

يوفر هذا القسم معلومات عن التسلسل الهرمي للسياسات وملفات تعريف السياسة وتوريثها.

التسلسل الهرمي للسياسات

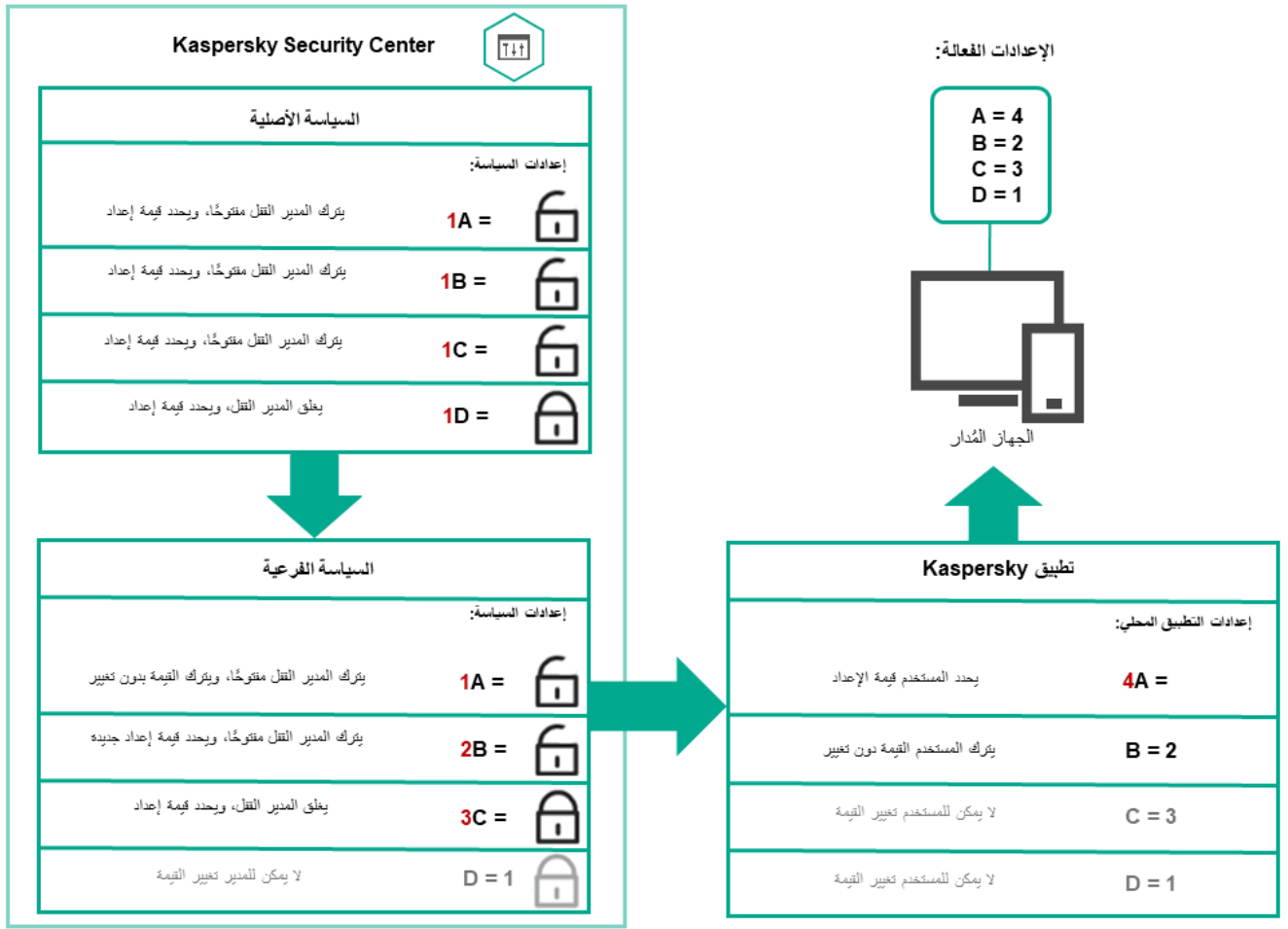
في حال وجود أجهزة مختلفة بحاجة إلى إعدادات مختلفة، يمكنك تنظيم الأجهزة في مجموعات إدارة.

يمكنك تحديد سياسة **لمجموعة إدارة** واحدة. يمكن أن يتم توريث 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.

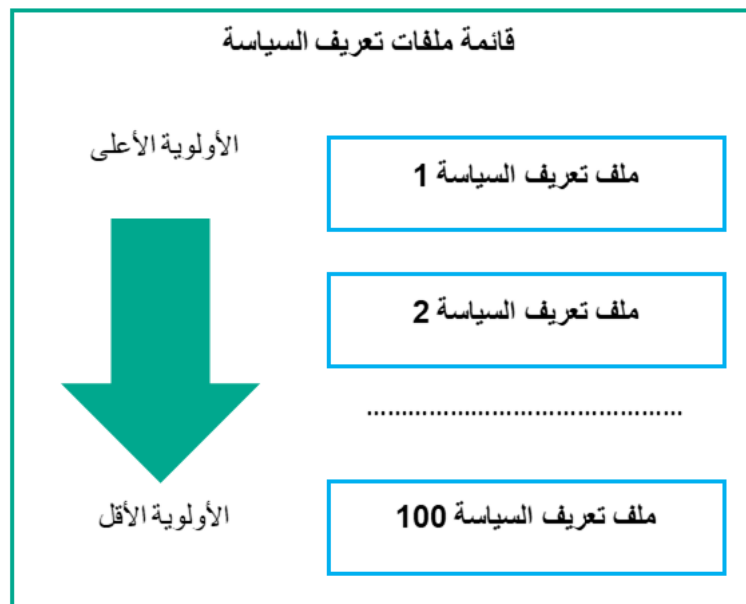
سياسات التطبيق نفسه تتصرف على بعضها وفق تسلسل هرمي لمجموعات الإدارة. الإعدادات المقولة من سياسة مجموعة إدارة مستوى أعلى (أصلية) سوف تعيد تعيين قيم إعدادات السياسة لمجموعة فرعية (انظر الشكل أدناه).



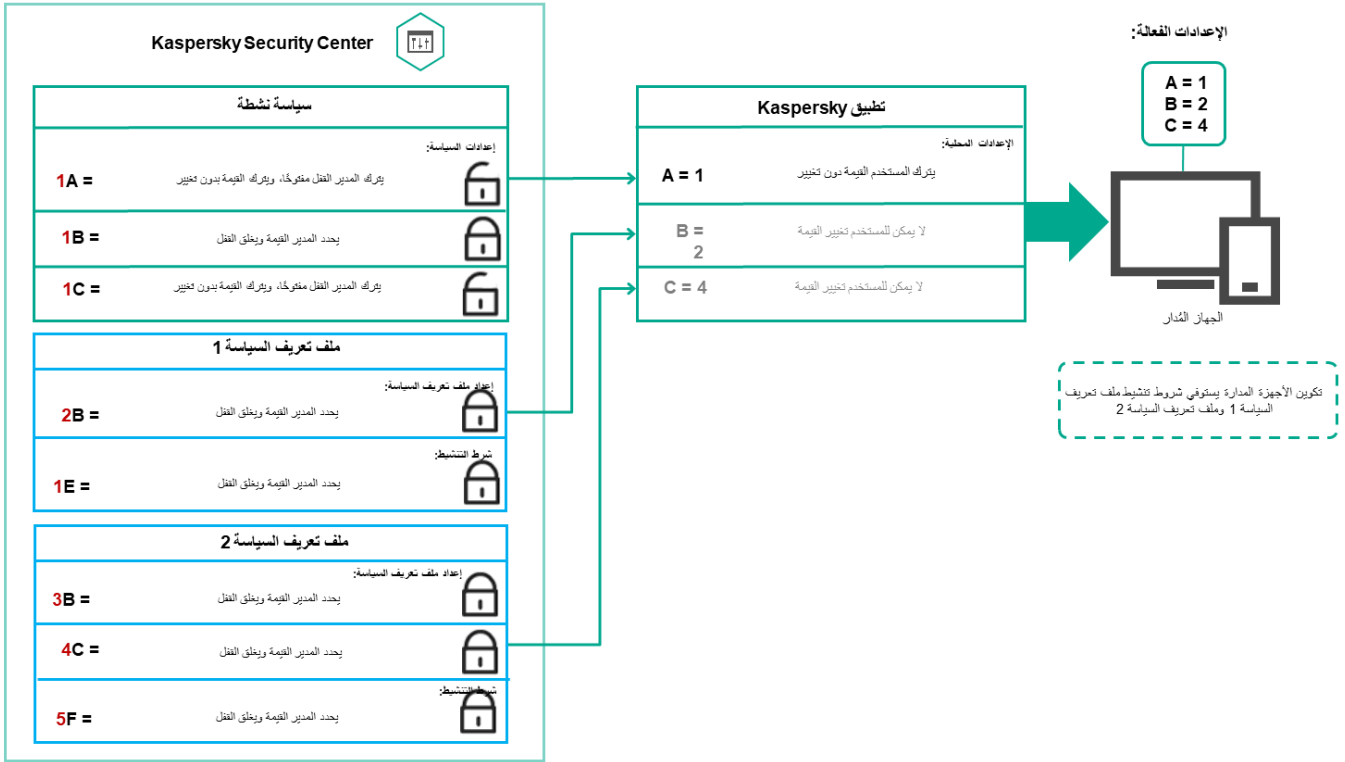
ملفات تعريف السياسة في التسلسل الهرمي للسياسات

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).



- 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 الإعدادات نفسها، يأخذ الجهاز قيمة الإعداد من ملف تعريف السياسة صاحب أعلى أولوية (انظر الشكل أدناه).

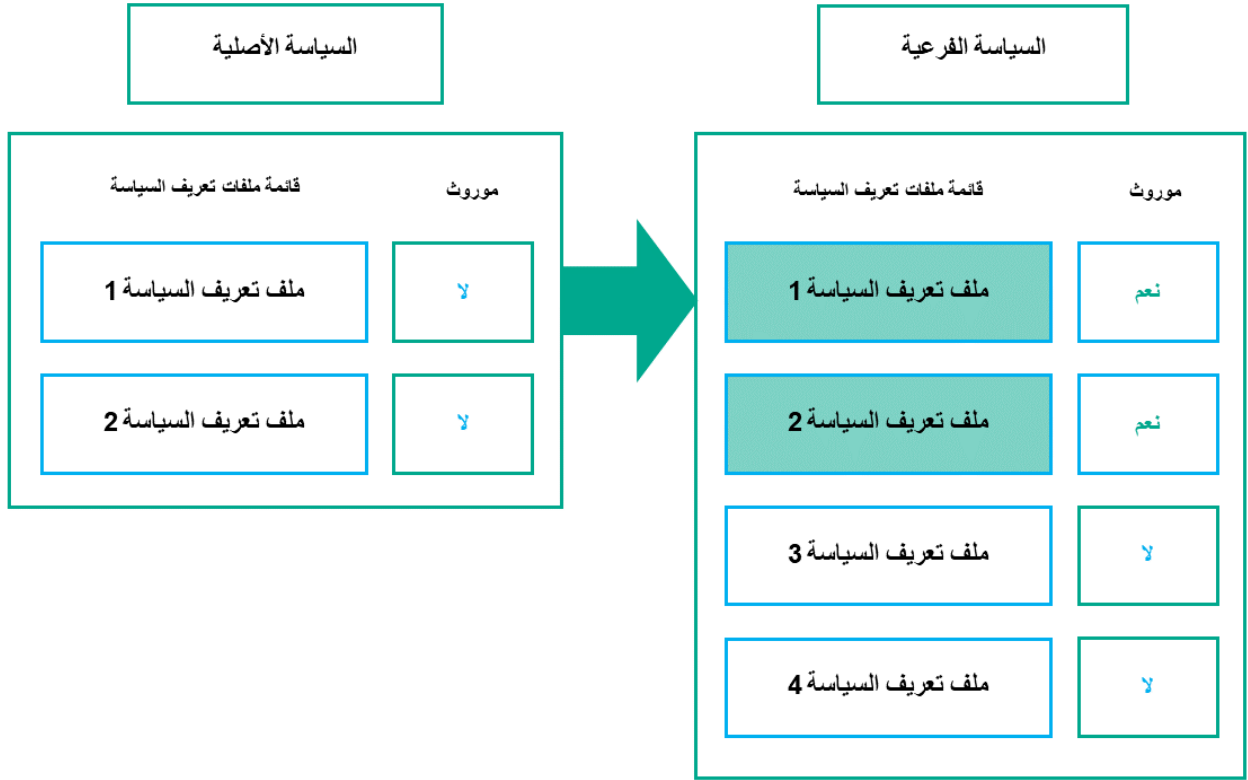


تكوين الجهاز المُدار يفي بشروط التنشيط لعدة ملفات تعريف سياسة

ملفات تعريف السياسة في التسلسل الهرمي للتوريث

ملفات تعريف السياسة من سياسات مستوى تسلسل هرمي مختلف تمثل 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).

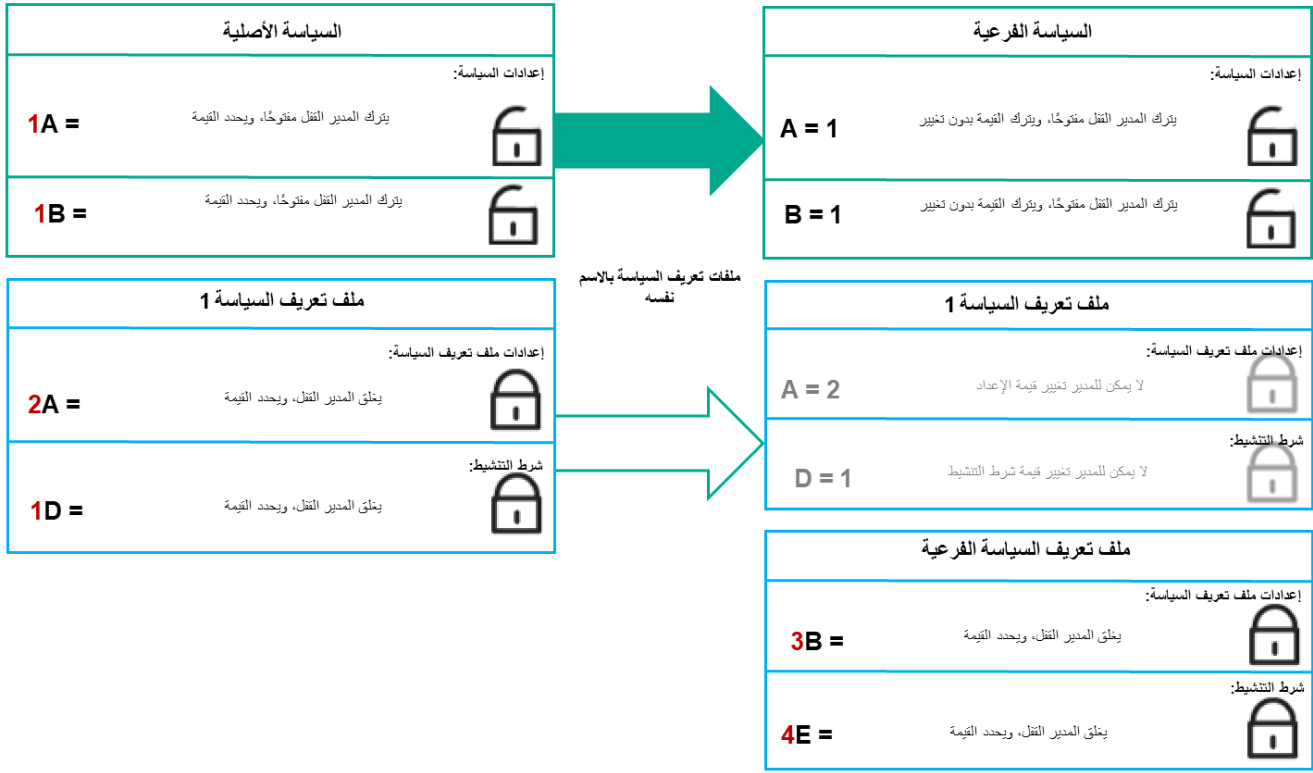


توريث ملفات تعريف السياسة

ملفات تعريف السياسة بالاسم نفسه

في حال وجود سياستين بالاسم نفسه في مستويين مختلفين في التسلسل الهرمي، تعمل هاتان السياستان وفق القواعد التالية:

- الإعدادات المقفولة وشرط تنشيط ملف التعريف لملف تعريف سياسة مستوى أعلى تغير إعدادات وشرط تنشيط ملف التعريف لملف تعريف سياسة مستوى أقل (انظر الشكل أدناه).



الملف التعريفي التابع يرث قيم الإعدادات من الملف التعريفي لسياسة أصلية

- الإعدادات غير المقفولة وشرط تنشيط ملف التعريف لملف تعريف سياسة مستوى أعلى لا تغيّر إعدادات وشرط تنشيط ملف التعريف لملف تعريف سياسة 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 تغيّر قيم الإعدادات الفعالة غير المقفولة.

إدارة السياسات

يصف هذا القسم إدارة السياسات ويوفّر 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 الأجهزة ← التسلسل الهرمي للمجموعات.

2. في هيكل مجموعة الإدارة، حدد مجموعة الإدارة التي ترغب في عرض قائمة السياسات لها.

تظهر قائمة السياسات في تنسيق جدولي. يكون الجدول فارغاً في حال عدم وجود سياسات. يمكنك عرض عواميد الجدول أو إخفائها أو تغيير ترتيبها أو عرض السطور التي تحتوي على قيمة تحدها أو استخدام البحث.

إنشاء سياسة

يمكنك إنشاء سياسات، ويمكنك كذلك تعديل السياسات الموجودة وحذفها.

لإنشاء سياسة:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.

2. انقر فوق إضافة.

تفتح النافذة تحديد تطبيق.

3. حدد التطبيق الذي ترغب في إنشاء سياسة له.

4. انقر فوق التالي.

تفتح نافذة إعدادات السياسة الجديدة مع وجود تبويب عام محدد.

5. يمكنك إذا كنت ترغب تغيير الاسم الافتراضي والحالة الافتراضية وإعدادات التوارث الافتراضية للسياسة.

6. حدد تبويب إعدادات التطبيق.

أو يمكنك النقر على حفظ والخروج. ستظهر السياسة في قائمة السياسات، ويمكنك تحرير إعداداتها لاحقاً.

7. في تبويب إعدادات التطبيق، حدد في الجزء الأيسر الفئة التي تريدها، وفي الجزء الأيمن 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 إلغاء لإلغاء العملية الأخيرة.

8. انقر على حفظ لحفظ السياسة.

ستظهر السياسة في قائمة السياسات.

تعديل سياسة.

لتعديل سياسة:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.

2. انقر على السياسة التي ترغب في تعديلها.

ستفتح نافذة إعدادات السياسة.

3. حدد الإعدادات 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 فوق **حفظ**.

سيتم حفظ التغييرات التي تم إجراؤها على السياسة في خصائص السياسة، وسيتم عرضها في قسم **سجل المراجعة**.

إعدادات السياسة العامة

عام

في تبويب **عام**، يمكنك تعديل حالة السياسة وتحديد توريث إعدادات السياسة:

• في **الكتلة حالة السياسة**، يمكنك تحديد أحد أوضاع السياسة:

• **نشط** 

إذا تم تحديد هذا الخيار، تصبح السياسة نشطة.

يتم تحديد هذا الخيار افتراضياً.

• **خارج المكتب** 

إذا تم تحديد هذا الخيار، تصبح السياسة نشطة عندما يغادر الجهاز شبكة الشركة.

• **غير نشط** 

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 افتراضياً.

• فرض توريث الإعدادات في السياسات الفرعية ④

إذا تم تمكين هذا الخيار، يتم تنفيذ الإجراءات التالية بعد تطبيق تغييرات السياسة:

- سيتم توزيع قيم إعدادات السياسة على سياسات مجموعات الإدارة المتداخلة أي على 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 تبويب تكوين الحدث تكوين تسجيل الحدث وإخطار الحدث. يتم توزيع الأحداث حسب مستوى الأهمية على علامات التبويب التالية:

• حرج

لا يتم عرض قسم حرج في خصائص سياسة عميل الشبكة.

• خلل وظيفي

• تحذير

• معلومات

في قسم البحث، تعرض القائمة أنواع الأحداث ومدة تخزين الحدث الافتراضية على خادم الإدارة (بالأيام). انقر على نوع حدث يتيح لك تحديد الإعدادات التالية:

• تسجيل الحدث

يمكنك تحديد عدد أيام تخزين الحدث، وكذلك تحديد مكان تخزين الحدث:

• تصدير إلى نظام SIEM باستخدام Syslog

• تخزين في سجل أحداث نظام التشغيل (OS) على جهاز

• تخزين في سجل أحداث نظام التشغيل (OS) على خادم إدارة

• الإخطارات بالأحداث

يمكنك تحديد ما إذا كنت ترغب في أن يتم إخطارك بالحدث أم لا بإحدى الطرق التالية:

• إخطار عبر البريد الإلكتروني

• إخطار عبر رسالة SMS

• إخطار عن طريق تشغيل ملف تنفيذي أو برنامج نصي

• الإخطار بواسطة SNMP

يتم بشكل افتراضي استخدام إعدادات الإخطار المحددة في تبويب خصائص خادم الإدارة (مثل عنوان المستلم). يمكنك إذا كنت ترغب تغيير هذه الإعدادات في تبويب البريد الإلكتروني، رسالة SMS والملف التنفيذي المراد تشغيله.

سجل المراجعة

تبويب سجل المراجعة يتيح لك عرض قائمة بمراجعات السياسة والتراجع عن التغييرات 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 عام.

3. تمكين توريث سياسة أو تعطيله:

- في حالة تمكين توريث الإعدادات من السياسة الأصلية في سياسة فرعية ويقوم بدير بفتح بعض الإعدادات في السياسة الأصلية، بهذا لا يمكنك تغيير هذه الإعدادات في السياسة التابعة.
- في حالة تعطيل توريث الإعدادات من السياسة الأصلية في سياسة تابعة، يمكنك إذاً تغيير كل الإعدادات في السياسة التابعة حتى في حالة قفل بعض الإعدادات في السياسة الأصلية.
- في حالة تفعيل فرض توريث الإعدادات في السياسات الفرعية في المجموعة الأصلية، يقوم هذا بتفعيل خيار توريث الإعدادات من السياسة الأصلية 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 **حفظ** لحفظ التغييرات، أو انقر على زر **إلغاء** لرفض التغييرات.

يتم افتراضياً تمكين خيار توريث الإعدادات من السياسة الأصلية 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 الأجهزة ← السياسات وملفات التعريف.

2. حدد خانة الاختيار الموجودة بجوار السياسة (أو السياسات) التي ترغب في نسخها.

3. انقر فوق الزر **نسخ**.

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 فوق الزر **نسخ** الموجود في أسفل الشاشة.

6. انقر على **موافق** لتأكيد العملية.

سيتم نسخ السياسة (أو السياسات) إلى المجموعة المستهدفة بجميع ملفات تعريفها. حالة كل سياسة منسوخة في المجموعة المستهدفة ستكون **غير نشط**. يمكنك تغيير الحالة إلى **نشط** في أي وقت.

في حالة وجود سياسة باسم مطابق لاسم السياسة المنقولة حديثاً في المجموعة المستهدفة بالفعل، سيتم الإضافة إلى اسم السياسة المنقولة حديثاً 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.

لنقل سياسة إلى مجموعة إدارة أخرى:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.

2. حدد خانة الاختيار الموجودة بجوار السياسة (أو السياسات) التي ترغب في نقلها.

3. انقر فوق الزر **نقل**.

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 فوق الزر **نقل** الموجود في أسفل الشاشة.

6. انقر على **موافق** لتأكيد العملية.

إذا كانت سياسة غير موروثه من المجموعة المصدر، سيتم نقلها إلى المجموعة المستهدفة بجميع ملفات تعريفها. حالة السياسة في المجموعة المستهدفة هي **غير نشط**. يمكنك تغيير الحالة إلى **نشط** في أي وقت.

إذا كانت سياسة موروثه من المجموعة المصدر، سوف تبقى في المجموعة المصدر. سيتم نسخها إلى المجموعة المستهدفة بجميع ملفات تعريفها. حالة السياسة في المجموعة المستهدفة هي **غير نشط**. يمكنك تغيير الحالة إلى **نشط** في أي وقت.

في حالة وجود سياسة باسم مطابق لاسم السياسة المنقولة حديثاً في المجموعة المستهدفة بالفعل، سيتم الإضافة إلى اسم السياسة المنقولة حديثاً بوضع المؤشر (رقم التسلسل التالي) في آخر الاسم، مثل (1).

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 الأجهزة ← السياسات وملفات التعريف.

2. حدد خانة الاختيار الموجودة بجوار اسم السياسة التي ترغب في عرض حالة توزيعها على الأجهزة.

3. حدد رابط **توزيع** 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 100000.

لتغيير عدد الأجهزة المعروضة في قائمة نتائج توزيع السياسة:

1. في القائمة الرئيسية ، انتقل إلى قسم خيارات الواجهة في شريط الأدوات.
2. في حد الأجهزة المعروضة في نتائج توزيع السياسة، أدخل عدد الأجهزة (بحد أقصى 100000).
العدد الافتراضي هو 5000.
3. انقر فوق حفظ.
يتم حفظ الإعدادات وتطبيقها.

تنشيط سياسة تلقائيًا بعد حدث انتشار الفيروسات

لجعل السياسة تقوم بعملية التنشيط تلقائيًا عند حدوث حدث انتشار الفيروسات:

1. في أعلى الشاشة، انقر على أيقونة الإعدادات (⚙) بجوار اسم خادم الإدارة المطلوب.
سنتفتح نافذة خصائص خادم الإدارة مع تحديد تبويب عام.
2. حدد قسم انتشار الفيروسات.
3. انقر على رابط تكوين السياسات ليتم تفعيلها عند وقوع حدث انتشار الفيروسات في الجزء الأيمن.
يتم فتح نافذة تنشيط السياسة.
4. في القسم المتعلق بالمكون الذي يكتشف انتشار الفيروسات (مكافحة الفيروسات لمحطات العمل وخوادم الملفات أو مكافحة الفيروسات لخوادم البريد أو مكافحة الفيروسات للدفاع المحيطي)، حدد زر الخيار الموجود بجوار المدخل الذي تريده ثم انقر على إضافة.
سنتفتح نافذة مجموعة الإدارة الأجهزة المُدارة.
5. انقر على أيقونة الرتبة العسكرية (>) الموجود بجوار الأجهزة المُدارة.
يتم عرض تسلسل هرمي لمجموعات الإدارة وسياساتها.
6. في التسلسل الهرمي لمجموعات الإدارة وسياساتها، انقر على اسم سياسة أو سياسات مفعلة عندما يتم اكتشاف انتشار فيروس.
لتحديد جميع السياسات في القائمة أو في مجموعة، حدد خانة الاختيار الموجودة بجوار الاسم المطلوب.
7. انقر على زر حفظ.
يتم غلق نافذة التسلسل الهرمي لمجموعات الإدارة وسياساتها.
يتم إضافة السياسات المحددة إلى قائمة السياسات المفعلة عند اكتشاف انتشار فيروس. يتم تفعيل السياسات المحددة عند انتشار الفيروس، سواء كانت نشطة أو غير نشطة.

إذا تم تنشيط سياسة عند حدوث انتشار فيروسات، لا يمكنك العودة إلى السياسة السابقة إلا باستخدام الوضع اليدوي.

حذف سياسة

يمكنك حذف سياسة إذا كنت لم تعد بحاجة إليها. لا يمكنك حذف سياسة إلا إذا لم تكن موروثه في مجموعة الإدارة المحددة. إذا كانت سياسة موروثه، لا يمكنك حذفها إلا في مجموعة المستوى الأعلى التي تم إنشاؤها لها.

لحذف سياسة:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.

2. حدد خانة الاختيار الموجودة بجوار السياسة التي ترغب في حذفها ثم انقر على **حذف**.

يصبح زر **حذف** غير متوفر (أي باهتًا) إذا حدد سياسة موروثية.

3. انقر على **موافق** لتأكيد العملية.

يتم حذف السياسة مع جميع ملفات تعريفها.

إدارة ملفات تعريف السياسة

يصف هذا القسم إدارة ملفات تعريف السياسة ويوفّر 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 **الأجهزة** ← **السياسات وملفات التعريف**.

2. انقر على اسم السياسة التي ترغب في عرض ملفات تعريفها.

ستفتح نافذة خصائص السياسة مع تحديد تبويب **عام**.

3. افتح تبويب **ملفات تعريف السياسة**.

تظهر قائمة ملفات تعريف السياسة في تنسيق جدولي. إذا لم يكن للسياسة ملفات تعريف، سيظهر الجدول الفارغ.

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 **ملفات تعريف السياسة**، 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 **تحديد الأولويات** أو **التقليل من الأهمية**.

كلما ارتفع موقع ملف تعريف السياسة في القائمة، ارتفعت أولويته.

4. انقر على زر **حفظ**.

يتم تغيير أولوية ملف تعريف السياسة المحدد وتطبيقه.

إنشاء ملف تعريف سياسة

يمكنك إنشاء ملفات تعريف السياسة لسياسة.

لإنشاء 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. انقر فوق **إضافة**.

3. يمكنك إذا كنت ترغب تغيير الاسم الافتراضي وإعدادات التوارث الافتراضية للسياسة.

4. حدد **تبويب إعدادات التطبيق**.

أو يمكنك النقر على **حفظ والخروج**. سيظهر الملف الذي أنشأته في قائمة ملفات تعريف السياسة، ويمكنك تحرير إعداداته لاحقًا.

5. في **تبويب إعدادات التطبيق**، حدد في الجزء الأيسر الفئة التي تريدها، وفي الجزء الأيمن قم بتحرير إعدادات ملف التعريف. يمكنك تحرير إعدادات ملف تعريف السياسة في كل فئة (قسم).

عند تحرير الإعدادات، يمكنك النقر على **إلغاء** لإلغاء العملية الأخيرة.

6. انقر على **حفظ** 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 ملفات تعريف السياسة**، 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 عام** 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 فوق **حفظ**.

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 **ملفات تعريف السياسة**، حدد ملف تعريف السياسة الذي ترغب في نسخه.

3. انقر على **نسخ**.

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 تحددتها.

5. انقر على **نسخ**.

يتم نسخ ملف تعريف السياسة إلى السياسة التي حددتها. يحصل ملف التعريف المنسوخ حديثاً على أقل أولوية. إذا نسخت ملف التعريف إلى السياسة نفسها، سيتم تديد اسم ملف التعريف المنسوخ حديثاً بإضافة مؤشر (). على سبيل المثال: (1)، (2).

يمكنك لاحقاً تغيير إعدادات ملف التعريف، ويشمل ذلك اسمه وألويته، 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 **ملفات تعريف السياسة**، 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 تبويب **قواعد التفعيل** ثم انقر على زر **إضافة**.

ستفتح نافذة بها قواعد تفعيل ملف تعريف السياسة.

4. حدد اسماً للقاعدة.

5. حدد خانة 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.

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

• حالة الجهاز

يحدد شرط ظهور الجهاز على الشبكة:

- عبر الإنترنت: الجهاز موجود على الشبكة، لذا يتوفر خادم الإدارة.
- غير متصل: الجهاز موجود على شبكة خارجية، وهذا يعني أن خادم الإدارة غير متاح.
- N/A: لن يتم تطبيق المعيار.

• قاعدة اتصال خادم الإدارة مفعلة على هذا الجهاز 9

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.

• قواعد مالك جهاز معين

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

• مالك الجهاز 9

ممكن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف وتمكينها على الجهاز وفقاً للمالكه. 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 وفقاً 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 افتراضياً.

• تم تضمين مالك الجهاز في مجموعة الأمان الداخلية 9

ممكن 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 وفقاً 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 افتراضياً.

• قواعد مواصفات الأجهزة 9

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:

• حجم ذاكرة الوصول العشوائي RAM، بالميجابايت 9

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 وفقاً 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 افتراضياً.

• عدد المعالجات المنطقية ٩

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 (علامة ">").

• عدد المعالجات المنطقية على الجهاز أكبر من أو يساوي القيمة المحددة (علامة "<").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقاً 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 افتراضياً.

• قواعد تعيين الدور

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

تفعيل ملف تعريف السياسة من خلال دور محدد لمالك الجهاز ٩

حدد هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز بناءً على دور المالك. قم بإضافة الدور يدوياً من قائمة الأدوار الموجودة.

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقاً للمعيار الذي تم تكوينه.

• قواعد استخدام العلامة ٩

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:

• علامة ٩

في قائمة العلامات، حدد قاعدة لتضمين الجهاز في ملف تعريف السياسة عن طريق تحديد خانة 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 خانة الاختيار، لن يتم تطبيق المعيار. بشكل افتراضي، خانة الاختيار هذه غير محددة.

• التطبيق على الأجهزة بدون العلامات المحددة ٩

مكّن هذا الخيار إذا كان يتعين عليك عكس تحديد علامتك.

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 افتراضياً.

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:

• **عضوية مالك الجهاز في مجموعة أمن Active Directory** 6

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 أمن Active Directory** 6

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** 6

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 إنشاء.

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 **قواعد التفعيل**. 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.**

سنظهر قائمة ملفات تعريف السياسة.

2. في تبويب **ملفات تعريف السياسة**، حدد خانة الاختيار الموجودة بجوار ملف تعريف السياسة الذي ترغب في حذفه ثم انقر على **حذف**.

3. في النافذة التي تفتح، انقر على **حذف** مرة أخرى.

سيتم حذف ملف تعريف السياسة. إذا ورث السياسة مجموعة مستوى أقل، يبقى ملف التعريف في تلك المجموعة لكنه يصبح ملف تعريف سياسة 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 دفتر الملاحظات أو محرك الأقراص الثابتة، أو في حالة فقدانه أو الوصول غير المصرح به من قِبَل 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](#).

تشفير البيانات في Kaspersky Endpoint Security for Windows

يمكنك إدارة تشفير BitLocker على الأجهزة التي تدار عبر Kaspersky Endpoint Security for Windows: تفعيل التشفير أو تعطيله وعرض قائمة ببرامج التشغيل المشفرة وإنشاء تقارير عن التشفير وعرضها.

يمكنك تكوين التشفير عن طريق تحديد سياسة Kaspersky Endpoint Security for Windows في Kaspersky Security Center Cloud Console. يجري Kaspersky Endpoint Security for Windows التشفير وفق السياسة المفعلة للحصول على إرشادات مفصلة حول كيفية تكوين القواعد ووصف لمزايا التشفير، يرجى الرجوع إلى [التعليمات عبر الإنترنت 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 وفق السياسة المفعلة للحصول على وصف تفصيلي حول مزايا التشفير، يرجى الرجوع إلى [التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Mac](#).

عرض قائمة ببرامج التشغيل المشفرة

يتم عرض عناصر الواجهة المتعلقة بميزة إدارة التشفير أو إخفاؤها بناءً على [إعدادات واجهة المستخدم](#).

لعرض قائمة ببرامج التشغيل المشفرة،

حدد **العمليات** ← **تشفير البيانات وحمايتها**، ومن القائمة المنسدلة حدد **برامج التشغيل المشفرة**.

ستظهر قائمة ببرامج التشغيل المشفرة.

تعرض النافذة معلومات حول برامج التشغيل المشفرة، وحول الأجهزة المشفرة على مستوى محركات الأقراص. بعد فك تشفير المعلومات على محرك أقراص، يتم إزالة محرك الأقراص تلقائيًا من القائمة.

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.

يتم عرض عناصر الواجهة المتعلقة بميزة إدارة التشفير أو إخفاؤها بناءً على [إعدادات واجهة المستخدم](#).

لعرض قائمة بالأحداث التي وقعت أثناء تشفير البيانات على الأجهزة،

حدد **العمليات** ← **تشفير البيانات وحمايتها**، ومن القائمة المنسدلة حدد **أحداث التشفير**.

ستظهر قائمة بأحداث التشفير.

تعرض النافذة معلومات حول المشاكل التي حدثت أثناء تشفير البيانات على الأجهزة.

يمكنك تصدير قائمة محركات الأقراص المشفرة إلى ملف CSV أو TXT.

إنشاء تقارير التشفير وعرضها

يمكنك إنشاء التقارير التالية:

- تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة. يحتوي هذا التقرير على معلومات حول حالة تشفير الأجهزة لكافة مجموعات الأجهزة.
 - تقرير حول حقوق الوصول إلى برامج التشغيل المشفرة. يحتوي هذا التقرير على معلومات حول حالة حسابات المستخدمين الذين تم منحهم الوصول إلى برامج التشغيل المشفرة.
 - تقرير حول أخطاء تشفير الملف. يحتوي هذا التقرير على معلومات حول الأخطاء التي حدثت عند تشغيل مهام تشفير البيانات أو فك تشفيرها على الأجهزة.
 - تقرير حول حجب الوصول إلى الملفات المشفرة. يحتوي هذا التقرير على معلومات حول منع وصول التطبيق إلى الملفات المشفرة.
- يمكنك إنشاء [أي تقرير](#) في قسم **التقارير (المراقبة والإبلاغ)** ← **التقارير**. يمكنك كحل بديل إنشاء بعض تقارير التشفير في قسم **برامج التشغيل المشفرة** وقسم **أحداث التشفير**.

لإنشاء تقارير تشفير في قسم برامج التشغيل المشفرة:

1. تأكد أنك قمت بتفعيل خيار **عرض تشفير البيانات وحمايتها** في [خيارات الواجهة](#).

2. حدد العمليات ← تشفير البيانات وحمايتها، ومن القائمة المنسدلة حدد برامج التشغيل المشفرة.

3. لإنشاء تقرير تشفير، انقر على اسم التقرير الذي ترغب في إنشائه:

- تقرير حول حالة تشفير أجهزة التخزين كبيرة السعة
- الإبلاغ عن حقوق الوصول إلى برامج التشغيل المشفرة

يبدأ إنشاء التقرير.

لإنشاء تقرير حول أخطاء تشفير ملف في قسم أحداث التشفير:

1. تأكد أنك قمت بتفعيل خيار عرض تشفير البيانات وحمايتها في [خيارات الواجهة](#).

2. حدد العمليات ← تشفير البيانات وحمايتها، ومن القائمة المنسدلة حدد أحداث التشفير.

3. لإنشاء تقرير التشفير، انقر على رابط تقرير حول أخطاء تشفير الملف.

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 مثبتاً على الجهاز المُدار. بعد أن تستقبل الطلب، يمكنك إنشاء ملف مفتاح وصول وإرساله إلى المستخدم. جميع حالات الاستخدام والإرشادات المفصلة متوفرة في [وثائق Kaspersky Endpoint Security for Windows](#).

لمنح حق الوصول إلى محرك أقراص مشفر في وضع عدم الاتصال:

1. حدد العمليات ← تشفير البيانات وحمايتها، ومن القائمة المنسدلة حدد برامج التشغيل المشفرة.

ستظهر قائمة ببرامج التشغيل المشفرة.

2. حدد محرك الأقراص الذي طلب المستخدم الوصول إليه.

3. انقر على زر منح الوصول إلى الجهاز في وضع عدم الاتصال.

4. في النافذة التي تفتح، حدد المكون الإضافي المقابل لتطبيق Kaspersky المستخدم في تشفير محرك الأقراص المحدد.

في حال تشفير محرك أقراص بتطبيق Kaspersky ليس مدعوماً من Kaspersky Security Center 14 Web Console، استخدم وحدة تحكم إدارة مستندة على Microsoft Management Console من أجل منح الوصول دون اتصال.

5. اتبع التعليمات المتوفرة في [وثائق Kaspersky Endpoint Security for Windows](#).

يمكن للمستخدم 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.

يمكنك ربط أدوار المستخدم بملفات تعريف السياسة. في حال تخصيص دور لمستخدم، يحصل 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، و فقط 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 كبيراً، 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.

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 مسبقاً من الحقوق وتعيين هذه الأدوار للمستخدمين اعتماداً على مدى نطاق واجباتهم.

يهدف تطبيق أدوار المستخدم إلى تبسيط وتفصيل الإجراءات الروتينية لتكوين حقوق وصول المستخدمين إلى ميزات التطبيق. يتم تكوين حقوق الوصول ضمن دور ما وفقاً للمهام القياسية ونطاق واجبات المستخدمين.

يمكن تعيين أسماء لأدوار المستخدمين وفقاً لأغراض كل منها. يمكنك إنشاء عدد غير محدود من الأدوار في التطبيق.

يمكنك استخدام [أدوار المستخدم المحددة مسبقاً](#) مع مجموعة الحقوق المكونة بالفعل، أو [إنشاء أدوار جديدة](#) لتكوين 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 القراءة والتعديل والتنفيذ على أي مهمة أو تقرير أو إعداد. بالإضافة إلى هذه الحقوق، يجب أن يكون لدى المستخدم حق تنفيذ العمليات على تحديدات الجهاز لإدارة المهام أو التقارير أو الإعدادات في تحديدات الجهاز.

تنتمي جميع المهام والتقارير والإعدادات وحزم التثبيت المفقودة في الجدول إلى الميزات العامة: المجال الوظيفي للوظيفة الأساسية.

حقوق الوصول إلى ميزات التطبيق

المجال الوظيفي	حق	إجراء المستخدم: الحقوق المطلوبة لتنفيذ الإجراء	المهمة	تقرير	أخرى
الميزات العامة: إدارة المجموعات الإدارية	تعديل	<ul style="list-style-type: none"> إضافة جهاز إلى مجموعة الإدارة: قم بالتعديل حذف الجهاز من مجموعة الإدارة: قم بالتعديل أضف مجموعة إدارة إلى مجموعة إدارة أخرى: قم بالتعديل حذف مجموعة إدارة من مجموعة إدارة أخرى: قم بالتعديل 	لا شيء	لا شيء	لا شيء
الميزات العامة: الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم	قراءة	الحصول على وصول القراءة لجميع الكائنات: اقرأ	لا شيء	لا شيء	لا شيء
الميزات العامة: الوظائف الأساسية	<ul style="list-style-type: none"> قراءة تعديل تنفيذ إجراء عمليات على تحديدات الجهاز 	<ul style="list-style-type: none"> قواعد نقل الجهاز (إنشاء أو تعديل أو حذف) للخادم الافتراضي: قم بالتعديل، وتنفيذ العمليات على تحديدات الجهاز احصل على شهادة مخصصة لبروتوكول (Mobile (LWNGT: اقرأ تعيين شهادة بروتوكول (Mobile (LWNGT المخصصة: اكتب احصل على قائمة الشبكة المعرفة من قبل NLA: اقرأ 	<ul style="list-style-type: none"> "تنزيل التحديثات إلى مستودع خادم الإدارة" "تسليم التقارير" "توزيع حزم التثبيت" "تثبيت التطبيق عن بُعد على خوادم الإدارة الثانوية" 	<ul style="list-style-type: none"> "تقرير حالة الحماية" "تقرير التهديدات" "تقرير حول الأجهزة الأكثر إصابة" "تقرير حول حالة قواعد بيانات مكافحة الفيروسات" "تقرير الأخطاء" 	لا شيء

- "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"

- إضافة أو تعديل أو حذف قائمة الشبكة المعرفة من قبل NLA: قم بالتعديل
- اعرض قائمة مجموعات التحكم في الوصول: اقرأ
- اعرض سجل أحداث Kaspersky: اقرأ

<ul style="list-style-type: none"> • "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 أدونات المستخدم الفعالة" • "تقرير حول الحقوق" 					
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • عرض الكائنات المحذوفة في سلة المحذوفات: اقرأ • حذف كائنات من سلة المحذوفات: قم بالتعديل 	<ul style="list-style-type: none"> • قراءة • تعديل 	الميزات العامة: الكائنات المحذوفة
<p>الإعدادات:</p> <ul style="list-style-type: none"> • 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 المخزنة في قاعدة البيانات 	لا شيء	لا شيء	<ul style="list-style-type: none"> • تغيير إعدادات تسجيل الأحداث: قم بتحرير إعدادات تسجيل الدخول إلى الأحداث • تغيير إعدادات إشعار الأحداث: قم بتحرير إعدادات إشعار الحدث • حذف الأحداث: احذف الأحداث 	<ul style="list-style-type: none"> • حذف الأحداث • تحرير إعدادات إشعار الحدث • تحرير إعدادات تسجيل الدخول إلى الأحداث • تعديل 	الميزات العامة: معالجة الحدث

<ul style="list-style-type: none"> • فترة زمنية لتخزين الأحداث من الأجهزة المحذوفة 					
<p>لا شيء</p>	<p>لا شيء</p>	<ul style="list-style-type: none"> • "النسخ الاحتياطي لبيانات خادم الإدارة" • "صيانة قاعدة البيانات" 	<ul style="list-style-type: none"> • حدد منافذ خادم الإدارة لاتصال عميل الشبكة: قم بالتعديل • حدد منافذ وكيل التنشيط الذي تم تشغيله على خادم الإدارة: قم بالتعديل • حدد منافذ وكيل التنشيط للجوال التي تم تشغيلها على خادم الإدارة: قم بالتعديل • حدد منافذ خادم الويب لتوزيع الحزم المستقلة: قم بالتعديل • حدد منافذ خادم الويب لتوزيع ملفات تعريف MDM: قم بالتعديل • حدد منافذ SSL لخادم الإدارة للاتصال عبر Kaspersky Security Center Web Console: تعديل • حدد منافذ خادم الإدارة للاتصال الهاتف المحمول: قم بالتعديل • قم بتغيير الحد الأقصى لعدد الأحداث المخزنة في قاعدة بيانات خادم الإدارة: قم بالتعديل • حدد الحد الأقصى لعدد الأحداث التي يمكن أن يرسلها خادم الإدارة: قم بالتعديل • حدد الفترة الزمنية التي يمكن خلالها إرسال الأحداث بواسطة خادم الإدارة: قم بالتعديل 	<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • تعديل كائن ACL • إجراء عمليات على تحديثات الجهاز 	<p>الميزات العامة: العمليات على خادم الإدارة</p>
<p>حزمة التثبيت: "Kaspersky"</p>	<ul style="list-style-type: none"> • "تقرير حول استخدام مفتاح الترخيص بواسطة خادم" 	<p>لا شيء</p>	<p>اقبل تثبيت التصحيح أو ارفضه: إدارة تصحيحات Kaspersky</p>	<ul style="list-style-type: none"> • إدارة تصحيحات Kaspersky 	<p>الميزات العامة: نشر برامج Kaspersky</p>

<p>الإدارة الافتراضي"</p> <ul style="list-style-type: none"> • "تقرير حول إصدارات برامج "Kaspersky" • "تقرير التطبيقات غير المتوافقة" • "تقرير حول إصدارات تحديثات وحدة برامج "Kaspersky" • "تقرير نشر الحماية" 				<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديثات الجهاز 	
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • تصدير ملف مفتاح: تصدير ملف مفتاح • تعديل إعدادات مفتاح ترخيص خادم الإدارة: قم بالتعديل 	<ul style="list-style-type: none"> • تصدير إلى ملف • تعديل 	الميزات العامة: إدارة المفاتيح
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • إنشاء التقارير بغض النظر عن قوائم ACL الخاصة بهم: اكتب • تنفيذ التقارير بغض النظر عن قوائم ACL الخاصة بهم: اقرأ 	<ul style="list-style-type: none"> • قراءة • تعديل 	الميزات العامة: إدارة التقارير الإلزامية
لا شيء	لا شيء	لا شيء	تسجيل خوادم الإدارة الثانوية أو تحديثها أو حذفها: تكوين التسلسل الهرمي لخوادم الإدارة	تهيئة التسلسل الهرمي لخوادم الإدارة	الميزات العامة: التسلسل الهرمي لخوادم الإدارة
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • تغيير خصائص "الأمان" لأي كائن: تغيير قوائم التحكم في الوصول للكائن • إدارة أدوار المستخدم: تغيير قوائم التحكم في الوصول للكائن • إدارة المستخدمين الداخليين: تغيير قوائم التحكم في الوصول للكائن 	تعديل كائن ACL	الميزات العامة: أذونات المستخدم

			<ul style="list-style-type: none"> • إدارة مجموعات الأمان: تغيير قوائم التحكم في الوصول للكانن • إدارة الأسماء المستعارة: تغيير قوائم التحكم في الوصول للكانن 		
لا شيء	"تقرير حول نتائج تثبيت تحديثات برامج الجهات الخارجية"	لا شيء	<ul style="list-style-type: none"> • الحصول على قائمة خوادم الإدارة الافتراضية: اقرأ • الحصول على معلومات حول خادم الإدارة الافتراضي: اقرأ • إنشاء خادم إدارة افتراضي أو تحديثه أو حذفه: إدارة خوادم الإدارة الافتراضية • نقل خادم الإدارة الافتراضي إلى مجموعة أخرى: إدارة خوادم الإدارة الافتراضية • تعيين أذونات خادم الإدارة الافتراضي: إدارة خوادم الإدارة الافتراضية 	<ul style="list-style-type: none"> • إدارة خوادم الإدارة الافتراضية • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديثات الجهاز 	الميزات العامة: خوادم الإدارة الافتراضية
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • الحصول على بيانات استعادة خدمة إدارة المفاتيح: اقرأ • حذف شهادات المستخدم: إدارة الشهادات • الحصول على الجزء العام لشهادة المستخدم: اقرأ • تحقق مما إذا تم تمكين البنية الأساسية للمفتاح العام: اقرأ • تحقق من حساب البنية التحتية للمفتاح العام: اقرأ • احصل على قوالب البنية التحتية للمفتاح العام: اقرأ • احصل على قوالب البنية التحتية للمفتاح العام عن طريق شهادة استخدام المفتاح الموسع: اقرأ 	<ul style="list-style-type: none"> • توصيل أجهزة جديدة • إرسال أوامر المعلومات فقط إلى الأجهزة المحمولة • إرسال أوامر إلى الأجهزة المحمولة. • إدارة الشهادات • قراءة • تعديل 	إدارة جهاز المحمول: عام

			<ul style="list-style-type: none"> • تحقق مما إذا تم إبطال شهادة البنية التحتية للمفتاح العام: اقرأ • تحديث إعدادات إصدار شهادة المستخدم: إدارة الشهادات • الحصول على إعدادات إصدار شهادة المستخدم: اقرأ • احصل على الحزم حسب اسم المنتج والإصدار: اقرأ • تعيين أو إلغاء شهادة المستخدم: إدارة الشهادات • تجديد شهادة المستخدم: إدارة الشهادات • تعيين علامة شهادة المستخدم: إدارة الشهادات • تشغيل إنشاء حزمة تثبيت MDM؛ إلغاء إنشاء حزمة تثبيت MDM: قم بتوصيل أجهزة جديدة 		
لا شيء	"تقرير حول مستخدمي الأجهزة"	لا شيء	<ul style="list-style-type: none"> • إنشاء جلسة مشاركة سطح المكتب: الحق في إنشاء جلسة مشاركة سطح المكتب • إنشاء جلسة RDP: الاتصال بجلسات RDP الموجودة • إنشاء نفق: بدء إنشاء نفق • حفظ قائمة شبكة المحتوى: احفظ الملفات من الأجهزة إلى محطة عمل المسؤول 	<ul style="list-style-type: none"> • بدء جلسات RDP • الاتصال بجلسات RDP الموجودة • بدء حفر الأنفاق • حفظ الملفات من الأجهزة إلى محطة عمل المسؤول • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديدات الجهاز 	إدارة النظام: الاتصال

لا شيء	<ul style="list-style-type: none"> • "تقرير حول سجل الأجهزة" • "تقرير حول تغييرات التكوين" • "تقرير حول الأجهزة" 	لا شيء	<ul style="list-style-type: none"> • الحصول على كائن مخزون الأجهزة أو تصديره: اقرأ • إضافة جرد الأجهزة أو تعيينه أو حذفه: اكتب 	<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديدات الجهاز 	إدارة النظام: جرد الأجهزة
لا شيء	لا شيء	لا شيء	<ul style="list-style-type: none"> • عرض إعدادات CISCO: اقرأ • تغيير إعدادات CISCO: اكتب 	<ul style="list-style-type: none"> • قراءة • تعديل 	إدارة النظام: التحكم في الوصول إلى الشبكة
حزمة التثبيت: "صورة نظام التشغيل"	لا شيء	"إنشاء حزمة التثبيت على مرجع صورة نظام التشغيل للجهاز"	<ul style="list-style-type: none"> • نشر خادم PXE: انشر خادم PXE • عرض قائمة بخوادم PXE: اقرأ • بدأ عملية التثبيت على عملاء PXE أو وقفها: قم بالتنفيذ • إدارة برامج التشغيل لـ WinPE وصور نظام التشغيل: قم بالتعديل 	<ul style="list-style-type: none"> • نشر خادم PXE • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديدات الجهاز 	إدارة النظام: نشر نظام التشغيل
لا شيء	"تقرير تحديثات البرامج"	<ul style="list-style-type: none"> • "مزمنة Windows Update" • "تثبيت تحديثات Windows Update" • "إصلاح الثغرات الأمنية" • "قم بتثبيت التحديثات المطلوبة وضبط إعدادات مهمة إصلاح الثغرات الأمنية" 	<ul style="list-style-type: none"> • عرض خصائص تصحيح الطرف الثالث: اقرأ • تغيير خصائص تصحيح الطرف الثالث: قم بالتعديل 	<ul style="list-style-type: none"> • قراءة • تعديل • تنفيذ • إجراء عمليات على تحديدات الجهاز 	إدارة النظام: إدارة الثغرات الأمنية والتصحيحات

إدارة النظام: التثبيت عن بُعد	<ul style="list-style-type: none"> قراءة تعديل تنفيذ إجراء عمليات على تحدييدات الجهاز 	<ul style="list-style-type: none"> عرض خصائص حزمة التثبيت المستندة إلى إدارة الثغرات الأمنية والتصحيحات من جهة خارجية: اقرأ تغيير خصائص حزمة التثبيت المستندة إلى إدارة الثغرات الأمنية والتصحيحات من جهة خارجية: تعديل 	لا شيء	لا شيء	حزم التثبيت: <ul style="list-style-type: none"> "تطبيق مخصص" "حزمة VAPM"
إدارة النظام: جرد البرامج	<ul style="list-style-type: none"> قراءة تعديل تنفيذ إجراء عمليات على تحدييدات الجهاز 	لا شيء	لا شيء	<ul style="list-style-type: none"> "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 مسبقاً

توفر أدوار المستخدم المعينة لمستخدمي Kaspersky Security Center مجموعات من [حقوق الوصول إلى ميزات التطبيق](#).

يمكنك استخدام أدوار المستخدم المحددة مسبقاً مع مجموعة الحقوق المكونة بالفعل، أو إنشاء أدوار جديدة وتكوين الحقوق المطلوبة بنفسك. يمكن ربط بعض أدوار المستخدم المحددة مسبقاً والمتوفرة في Kaspersky Security Center بـمناصب وظيفية محددة، على سبيل المثال، **المدقق**، **مسؤول الأمن**، **المشرف** (هذه الأدوار موجودة في Kaspersky Security Center بدءاً من الإصدار 11). تم تكوين حقوق الوصول لهذه الأدوار مسبقاً وفقاً 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	يسمح بتنفيذ جميع العمليات مع جميع أنواع التقارير، وجميع عمليات العرض بما يشمل عرض الكائنات المحذوفة (يمنح أذونات قراءة وتعديل في حقل الكائنات) المحذوفة. لا يسمح بتنفيذ عمليات أخرى. يمكنك تعيين هذا الدور لشخص يقوم بإجراء تدقيق لمؤسستك.
المشرف	يسمح بتنفيذ جميع عمليات العرض، لا يسمح بتنفيذ عمليات أخرى. يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمن 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 أمن تكنولوجيا المعلومات في مؤسستك.

يوضح الجدول أدناه حقوق الوصول المعينة لكل دور مستخدم محدد مسبقاً.

الوصف	الدور
<p>يسمح بجميع العمليات في المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: • الوظائف الأساسية • معالجة الحدث • التسلسل الهرمي لخوادم الإدارة • خوادم الإدارة الافتراضية • إدارة النظام: • الاتصال • مخزون الأجهزة • مخزون البرنامج 	<p>مسؤول خادم الإدارة</p>
<p>يمنح حقوق القراءة والتنفيذ في جميع المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: • الوظائف الأساسية • خوادم الإدارة الافتراضية • إدارة النظام: • الاتصال • مخزون الأجهزة • مخزون البرنامج 	<p>مشغل خادم الإدارة</p>
<p>للسماح بجميع العمليات في المجالات الوظيفية ، في الميزات العامة :</p> <ul style="list-style-type: none"> • الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم • الكائنات المحذوفة • إدارة التقارير المفروضة <p>يمكنك تعيين هذا الدور لشخص يقوم بإجراء تدقيق لمؤسستك.</p>	<p>مدقق الحسابات</p>
<p>يسمح بجميع العمليات في المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: • الوظائف الأساسية • نشر برنامج Kaspersky • إدارة مفتاح الترخيص 	<p>مسؤول التثبيت</p>

<ul style="list-style-type: none"> • إدارة النظام: • نشر نظام التشغيل • إدارة الثغرات الأمنية والتصحيحات • التثبيت عن بُعد • مخزون البرنامج <p>منح حقوق القراءة والتنفيذ في الميزات العامة: المجالات الوظيفية لخوادم الإدارة الافتراضية.</p>	
<p>يمنح حقوق القراءة والتنفيذ في جميع المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: • الوظائف الأساسية • نشر برنامج Kaspersky (يمنح أيضًا تصحيحات إدارة Kaspersky مباشرة في هذه المنطقة) • خوادم الإدارة الافتراضية • إدارة النظام: • نشر نظام التشغيل • إدارة الثغرات الأمنية والتصحيحات • التثبيت عن بُعد • مخزون البرنامج 	<p>مشغل التثبيت</p>
<p>يسمح بجميع العمليات في المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: الوظائف الأساسية • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات 	<p>مسؤول Kaspersky Endpoint Security</p>
<p>يمنح حقوق القراءة والتنفيذ في جميع المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: الوظائف الأساسية • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات 	<p>مشغل Kaspersky Endpoint Security</p>
<p>يسمح بجميع العمليات في المجالات الوظيفية، باستثناء المجالات التالية، في الميزات العامة:</p> <ul style="list-style-type: none"> • الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم • إدارة التقارير المفروضة 	<p>المسؤول الرئيسي</p>
<p>يمنح حقوق القراءة والتنفيذ (إن أمكن) في جميع المجالات الوظيفية التالية:</p> <ul style="list-style-type: none"> • الميزات العامة: • الوظائف الأساسية • الكائنات المحذوفة 	<p>المشغل الرئيسي</p>

<ul style="list-style-type: none"> • العمليات على خادم الإدارة • نشر برنامج Kaspersky • خوادم الإدارة الافتراضية • إدارة جهاز المحمول: عام • إدارة النظام، بما في ذلك جميع الميزات • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات 	
<ul style="list-style-type: none"> • إدارة جهاز المحمول • يسمح بجميع العمليات في المجالات الوظيفية التالية: • الميزات العامة: الوظائف الأساسية • إدارة جهاز المحمول: عام 	
<ul style="list-style-type: none"> • يمنح حقوق القراءة والتنفيذ في الميزات العامة: المجالات الوظيفية للوظائف الأساسية. • يمنح قراءة وإرسال أوامر المعلومات فقط إلى الأجهزة المحمولة في المجال الوظيفي إدارة الجهاز المحمول: عام. 	مشغل إدارة جهاز المحمول
<ul style="list-style-type: none"> • 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 • يمنح قراءة وتعديل وتنفيذ وحفظ الملفات من الأجهزة على محطة عمل المسؤول وتنفيذ العمليات على حقوق تحديدات الأجهزة في نطاق إدارة النظام: المجالات الوظيفية للاتصال. • يمكنك تعيين هذا الدور لموظف أمن مسؤول عن أمن تكنولوجيا المعلومات في مؤسستك. 	مسؤول الأمن
<ul style="list-style-type: none"> • يسمح بجميع العمليات في إدارة جهاز المحمول: المجالات الوظيفية لـ Self Service Portal. هذه الميزة غير مدعومة في Kaspersky Security Center 11 والإصدار الأحدث. 	مستخدم Self Service Portal
<ul style="list-style-type: none"> • يمنح حق القراءة في الميزات العامة: الوصول إلى الكائنات، بغض النظر عن قوائم التحكم في الوصول ACLs والميزات العامة: المجالات الوظيفية لإدارة التقارير المفروضة. • يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمن تكنولوجيا المعلومات في مؤسستك. 	المشرف
<ul style="list-style-type: none"> • يسمح بجميع العمليات في الميزات العامة: المجالات الوظيفية للوظائف الأساسية وإدارة النظام (بما في ذلك جميع الميزات). 	مسؤول الثغرات الأمنية والتصحيحات
<ul style="list-style-type: none"> • يمنح حقوق القراءة والتنفيذ (إن أمكن) في الميزات العامة: المجالات الوظيفية للوظائف الأساسية وإدارة النظام (بما في ذلك جميع الميزات). 	مشغل إدارة الثغرات الأمنية والتصحيحات

إضافة حساب خاص بمستخدم داخلي

لإضافة حساب مستخدم داخلي جديد إلى Kaspersky Security Center:

1. في القائمة الرئيسية، انتقل إلى المستخدمين والأدوار ← المستخدمين.
2. انقر فوق إضافة.

3. في النافذة كيان جديد التي تفتح، حدد الإعدادات الخاصة بحساب المستخدم الجديد:

• احتفظ بالخيار الافتراضي المستخدم.

• الاسم.

• كلمة المرور لتوصيل المستخدم بـ Kaspersky Security Center

يجب أن تتوافق كلمة المرور مع القواعد التالية:

• يجب أن تتضمن كلمة المرور من 8 إلى 16 حرفاً.

• 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 الحروف التي أدخلتها، انقر مع الاستمرار على زر إظهار.

عدد محاولات إدخال كلمة المرور محدود. افتراضياً، 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. يمكنك إلغاء قفل حساب المستخدم فقط عن طريق تغيير كلمة المرور.

• الاسم بالكامل

• الوصف

• عنوان البريد الإلكتروني

• الهاتف

4. انقر فوق موافق لحفظ التغييرات.

يظهر حسابات المستخدم الجديد في قائمة المستخدمين ومجموعات المستخدمين.

إنشاء مجموعة مستخدمين

لإنشاء مجموعة مستخدم:

1. في القائمة الرئيسية، انتقل إلى المستخدمين والأدوار ← المستخدمين.

2. انقر فوق إضافة.

3. في نافذة كيان جديد التي تفتح، حدد مجموعة.

4. حدد الإعدادات التالية لمجموعة المستخدم الجديدة:

• اسم المجموعة

• الوصف

5. انقر فوق موافق لحفظ التغييرات.

تظهر مجموعة المستخدم الجديدة في قائمة المستخدمين ومجموعات المستخدمين.

تحرير حساب خاص بمستخدم داخلي

قم بما يلي لتحرير حساب مستخدم داخلي في Kaspersky Security Center:

1. في القائمة الرئيسية، انتقل إلى المستخدمين والأدوار ← المستخدمين.

2. انقر على اسم حساب المستخدم الذي ترغب في تحريره.

3. في نافذة إعدادات المستخدم التي تفتح، قم بتغيير إعدادات حساب المستخدم في تبويب عام:

• الوصف

• الاسم بالكامل

• عنوان البريد الإلكتروني

• الهاتف الرئيسي

• كلمة المرور لتوصيل المستخدم بـ Kaspersky Security Center

يجب أن تتوافق كلمة المرور مع القواعد التالية:

• يجب أن تتضمن كلمة المرور من 8 إلى 16 حرفاً.

• 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 أحرف 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. افتراضياً، يكون الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به هو 10. يمكنك تغيير عدد المحاولات المسموح بها؛ ومع ذلك، لا نوصي بتقليل هذا الرقم لأسباب أمنية. إذا أدخل المستخدم كلمة مرور غير صالحة لعدد المرات المحدد، فسيتم منع الوصول إلى حساب المستخدم لمدة ساعة واحدة. يمكنك إلغاء قفل حساب المستخدم فقط عن طريق تغيير كلمة المرور.

• يمكنك عند الضرورة وضع زر التبديل على **معطل** لمنع المستخدم من التوصل بالتطبيق. يمكنك تعطيل حساب، مثلاً بعد ترك الموظف للشركة.

4. في تبويب **حماية المصادقة**، يمكنك تحديد إعدادات الأمان لهذا الحساب.

5. في تبويب **المجموعات**، يمكنك إضافة المستخدم إلى مجموعات الأمان.

6. في تبويب **الأجهزة**، يمكنك تخصيص الأجهزة إلى المستخدم.

7. في تبويب **الأدوار**، يمكنك تخصيص الأدوار إلى المستخدم.

8. انقر على **حفظ** لحفظ التغييرات.

يظهر حسابات المستخدم المحدث في قائمة المستخدمين ومجموعات الأمان.

تحرير مجموعة مستخدمين

لا يمكنك تحرير إلا المجموعات الداخلية.

لتحرير مجموعة مستخدم:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **المستخدمون**.

2. انقر على اسم مجموعة المستخدم التي ترغب في تحريرها.

3. في نافذة إعدادات المجموعة التي تفتح، قم بتغيير إعدادات مجموعة المستخدم:

• الاسم

• الوصف

4. انقر على **حفظ** لحفظ التغييرات.

تظهر مجموعة المستخدم المحدثة في قائمة المستخدمين ومجموعات المستخدمين.

إضافة حسابات المستخدمين إلى مجموعة داخلية

لا يمكنك إضافة إلا حسابات المستخدمين الداخليين إلى مجموعة داخلية.

لإضافة حسابات المستخدمين إلى مجموعة داخلية:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **المستخدمون**.

2. حدد خانة الاختيار الموجودة بجوار حسابات المستخدمين التي ترغب في إضافتها إلى مجموعة.

3. انقر على زر **تعيين مجموعة**.

4. في نافذة **تعيين مجموعة** التي تفتح، حدد المجموعة التي ترغب في إضافة حسابات المستخدمين إليها.

5. انقر على زر **تعيين**.

يتم إضافة حسابات المستخدمين إلى المجموعة.

تعيين مستخدم كمالك للجهاز

للحصول على معلومات حول تعيين مستخدم كمالك للجهاز المحمول، راجع [تعليمات Kaspersky Security for Mobile](#).

لتعيين مستخدم كمالك للجهاز:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **المستخدمون**.

2. انقر على اسم حساب المستخدم الذي ترغب في تعيينه كمالك لجهاز.

3. في نافذة إعدادات المستخدم التي تفتح، حدد علامة تبويب **الأجهزة**.

4. انقر فوق **إضافة**.

5. من قائمة الجهاز، حدد الجهاز التي ترغب في تعيينه إلى المستخدم.

6. انقر على **موافق**.

يتم إضافة الجهاز المحدد إلى قائمة الأجهزة المعينة للمستخدم.

يمكنك إجراء العملية نفسها في **الأجهزة المُدارة** ← **الأجهزة المُدارة** عن طريق النقر على اسم الجهاز الذي ترغب في تعيينه ثم النقر على رابط **جارٍ إدارة مالك الجهاز**.

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 إلى **المستخدمون والأدوار** ← **المستخدمون**.

2. حدد خانة الاختيار الموجودة بجوار المستخدم أو مجموعة الأمان التي ترغب في حذفها.

3. انقر على **حذف**.

4. في النافذة التي تفتح، انقر على **موافق**.

يتم حذف المستخدم أو مجموعة الأمان.

إنشاء دور للمستخدم

لإنشاء دور للمستخدم:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **الأدوار**.

2. انقر فوق **إضافة**.

3. في نافذة **اسم دور جديد** التي تفتح، أدخل اسم الدور الجديد.

4. انقر على **موافق** لتطبيق التغييرات.

5. في نافذة خصائص الدور التي تفتح، قم بتغيير إعدادات الدور:

- في تبويب **عام**، قم بتحرير اسم الدور.
لا يمكنك تحرير اسم دور محدد مسبقاً.
- في تبويب **إعدادات**، **قم بتحرير نطاق الدور** والسياسات وملفات التعريف المرتبطة بالدور.
- في تبويب **حقوق الوصول**، قم بتحرير حقوق الوصول إلى تطبيقات Kaspersky.

6. انقر على **حفظ** لحفظ التغييرات.

يظهر الدور الجديد في قائمة أدوار المستخدم.

تحرير دور المستخدم

لتحرير دور مستخدم:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **الأدوار**.

2. انقر على اسم الدور التي ترغب في تحريره.

3. في نافذة خصائص الدور التي تفتح، قم بتغيير إعدادات الدور:

- في تبويب **عام**، قم بتحرير اسم الدور.
لا يمكنك تحرير اسم دور محدد مسبقاً.
- في تبويب **إعدادات**، **قم بتحرير نطاق الدور** والسياسات وملفات التعريف المرتبطة بالدور.
- في تبويب **حقوق الوصول**، قم بتحرير حقوق الوصول إلى تطبيقات Kaspersky.

4. انقر على **حفظ** 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، و فقط 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 إلى **المستخدمون والأدوار** ← **المستخدمون**.
 2. حدد خانة الاختيار الموجودة بجوار المستخدمين ومجموعات الأمان التي ترغب في إضافتها إلى نطاق دور المستخدم.
 3. انقر على زر **تعيين المهمة**.
 - سيبدأ معالج تعيين الدور. انتقل عبر المعالج من خلال استخدام زر **التالي**.
 4. في صفحة **تحديد مهمة** في المعالج، حدد دور المستخدم الذي ترغب في تعيينه.
 5. في صفحة **تحديد النطاق** في المعالج، حدد مجموعة الإدارة التي ترغب في إضافتها إلى نطاق دور المستخدم.
 6. انقر على زر **تعيين المهمة لإغلاق المعالج**.
- تتم إضافة المستخدمين المحددين أو مجموعات الأمان المحددة ومجموعة الإدارة المحددة إلى نطاق دور المستخدم.

الطريقة الثانية:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **الأدوار**.
 2. انقر على اسم الدور الذي ترغب في تحديد نطاقه.
 3. في نافذة خصائص السياسة التي تفتح، حدد تبويب **إعدادات**.
 4. في قسم **نطاق المهمة**، انقر على **إضافة**.
 - سيبدأ معالج تعيين الدور. انتقل عبر المعالج من خلال استخدام زر **التالي**.
 5. في صفحة **تحديد النطاق** في المعالج، حدد مجموعة الإدارة التي ترغب في إضافتها إلى نطاق دور المستخدم.
 6. في صفحة **تحديد مستخدمين** في المعالج، حدد المستخدمين ومجموعات الأمان التي ترغب في إضافتها إلى نطاق دور المستخدم.
 7. انقر على زر **تعيين المهمة لإغلاق المعالج**.
 8. انقر على زر **إغلاق (X)** لإغلاق نافذة خصائص الدور.
- تتم إضافة المستخدمين المحددين أو مجموعات الأمان المحددة ومجموعة الإدارة المحددة إلى نطاق دور المستخدم.

حذف دور مستخدم

لحذف دور مستخدم:

1. في القائمة الرئيسية، انتقل إلى المستخدمين والأدوار ← الأدوار.

2. حدد خانة الاختيار الموجودة بجوار اسم الدور الذي ترغب في حذفه.

3. انقر على حذف.

4. في النافذة التي تفتح، انقر على موافق.

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 نشطاً 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 "ساح". 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 وقت 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 المستخدمين والأدوار ← الأدوار.

2. انقر على اسم الدور التي ترغب في رباطه بملف تعريف سياسة.

ستفتح نافذة خصائص الدور مع تحديد تبويب عام.

3. حدد تبويب إعدادات ثم مرر لأسفل حتى تصل إلى قسم السياسات وملفات التعريف.

4. انقر على تحرير.

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 ملف تعريف السياسة الجديد.

c. حدد اسماً لملف التعريف الجديد وقم بتكوين إعدادات ملف التعريف.

d. انقر على زر حفظ.

e. حدد خانة الاختيار الموجودة بجوار ملف التعريف الجديد.

6. انقر على تعيين إلى الدور.

بهذا يتم ربط ملف التعريف بالدور ويظهر في خصائص الدور. ينطبق ملف التعريف تلقائياً بأي جهاز مخصص لمالكه دور.

إدارة الكائنات في Kaspersky Security Center 14 Web Console

يحتوي هذا القسم على معلومات حول إدارة مراجعات الكائنات. يتيح لك Kaspersky Security Center تتبع تعديل الكائن. في كل مرة تحفظ فيها التغييرات التي أجريت على الكائن، يتم إنشاء مراجعة. لكل مراجعة رقم.

تشتمل كائنات التطبيق التي تدعم إدارة المراجعة على:

- خوادم 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 أجريت 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 أتم إجراؤه على إعدادات الكائن

تكون خانة وصف مراجعة الكائن فارغة بشكل افتراضي. لإضافة وصف إلى مراجعة، حدد المراجعة ذات الصلة وانقر فوق الزر **الوصف**. في النافذة **وصف مراجعة الكائن**، أدخل نصاً لوصف المراجعة.

إضافة وصف للمراجعة

يتيح لك Kaspersky Security Center تتبع تعديل الكائن. في كل مرة تحفظ فيها التغييرات التي أجريت على الكائن، يتم إنشاء مراجعة. لكل مراجعة رقم.

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 [تحرير الوصف](#).

تفتح نافذة [الوصف](#).

4. في النافذة [الوصف](#)، أدخل نصًا لوصف المراجعة.

تكون خانة وصف مراجعة الكائن فارغة بشكل افتراضي.

5. انقر على زر [حفظ](#).

يضاف الوصف لمراجعة الكائن.

حذف كائن

يمكنك حذف الكائنات كالسياسات والمهام وحزم التثبيت والمستخدمين الداخليين والمستخدمين الداخليين ومجموعات المستخدمين الداخليين إذا كان لديك إذن التعديل الموجود في [فئة حقوق الوظائف الأساسية](#).

لحذف كائن:

1. حدد الكائن أو الكائنات المتعددة التي تريد حذفها.

2. انقر على زر [حذف](#).

3. انقر فوق الزر [موافق](#) لتأكيد حذف الكائنات المحددة.

سيتم حذف الكائن المحدد أو الكائنات المحددة، وتخزين المعلومات حوله (حولها) في قاعدة البيانات.

(Kaspersky Security Network (KSN

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.

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.

بالمشاركة في KSN، فأنت توافق على إرسال معلومات بشكل تلقائي إلى Kaspersky حول تشغيل تطبيقات Kaspersky المثبتة على الأجهزة العميلة والمُدارة عبر Kaspersky Security Center. يتم نقل المعلومات وفقًا [لإعدادات وصول KSN](#) الحالية.

يطلبك 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، سيتم عرضه لك عندما تحدث خادم الإدارة أو تقوم بترقيته. 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 DNS العام. يعد ذلك ضروريًا للتأكد من الحفاظ على مستوى الأمان للأجهزة المُدارة.

تتفاعل الأجهزة العملية المُدارة بواسطة خادم الإدارة مع KSN عبر خدمة وكيل KSN. يوفر وكيل KSN الميزات التالية:

- يمكن للأجهزة العملية 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.

يمكنك تكوين خادم وكيل KSN في القسم **وكيل KSN من 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. انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **عام**، حدد قسم **إعدادات وكيل KSN**.

3. قم بتبديل زر التبديل إلى وضع **تمكين وكيل KSN على خادم الإدارة ممكن**.

يتم إرسال البيانات من الأجهزة العملية إلى KSN وفقًا لسياسة Kaspersky Endpoint Security، والتي تكون نشطة على الأجهزة العملية تلك. إذا تم إلغاء خانة الاختيار هذه، فلن يتم إرسال أي بيانات إلى KSN من خادم الإدارة ومن الأجهزة العملية عبر Kaspersky Security Center. ومع ذلك، يمكن للأجهزة العملية إرسال بيانات إلى KSN مباشرة (عبر تجاوز Kaspersky Security Center)، وفقًا للإعدادات الخاصة بهم. تحدد سياسة Kaspersky Endpoint Security for Windows المفعلة على الأجهزة العملية، البيانات التي سيتم إرسالها بشكل مباشر (عبر تجاوز Kaspersky Security Center) من هذه الأجهزة إلى KSN.

4. بدل زر التبديل إلى وضع **استخدام شبكة Kaspersky Security Network مفعّل**.

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 KSN الخاصة**، بدل زر التبديل إلى وضع **استخدام شبكة Kaspersky Private Security Network خاصة مفعّل** وانقر على زر **تحديد ملف من خلال إعدادات وكيل شبكة KSN** لتنزيل إعدادات شبكة KSN الخاصة (الملفات بالامتدادين pem و pkcs7). عقب تنزيل الإعدادات، تعرض الواجهة اسم المزود وجهات الاتصال، وكذلك تاريخ إنشاء الملف مع إعدادات شبكة KSN الخاصة.

عند تمكين شبكة KSN الخاصة، انتبه إلى نقاط التوزيع التي تم تكوينها لإرسال طلبات KSN مباشرة إلى سحابة KSN. 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 KSN الخاصة، مكن خيار **توجيه طلبات KSN إلى خادم الإدارة** لكل نقطة توزيع. يمكنك تمكين هذا الخيار في خصائص نقطة التوزيع أو في سياسة عميل الشبكة.

عند تبديل زر التبديل إلى وضع **استخدام شبكة Kaspersky Private Security Network خاصة مفعّل**، ستظهر رسالة تحتوي على تفاصيل حول شبكة KSN الخاصة.

تدعم تطبيقات Kaspersky التالية شبكة KSN الخاصة:

• Kaspersky Security Center 10 Service Pack 1 أو أحدث

• Kaspersky Endpoint Security 10 Service Pack 1 for Windows أو أحدث

في حالة تمكين شبكة KSN الخاصة في Kaspersky Security Center، تتلقى هذه التطبيقات معلومات حول دعم شبكة KSN الخاصة. في نافذة إعدادات التطبيق وفي القسم الفرعي **Kaspersky Security Network** الخاص بالقسم الحماية المتقدمة من التهديد، يظهر موفر شبكة KSN: شبكة KSN الخاصة. وإلا، يظهر موفر شبكة KSN: شبكة KSN العالمية.

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 KSN الخاصة، نوصيك باستخدام خوادم الإدارة الثانوية التي لم يتم تمكين استخدام شبكة KSN الخاصة لها.

لا يرسل Kaspersky Security Center أي بيانات إحصائية إلى Kaspersky Security Network في حالة تكوين شبكة KSN الخاصة في القسم 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 KSN الخاصة مباشرة، مكن خيار **تجاهل إعدادات خادم وكيل عند الاتصال بشبكة KSN الخاصة**. وإلا، لا يمكن وصول الطلبات الصادرة من التطبيقات المُدارة إلى شبكة KSN الخاصة.

5. تكوين اتصال خادم الإدارة بخدمة وكيل KSN:

• ضمن إعدادات الاتصال، للمنفذ **منفذ TCP**، حدد رقم منفذ TCP الذي سيُستخدم للاتصال بخادم وكيل KSN. والمنفذ الافتراضي للاتصال بخادم وكيل KSN هو 13111.

• إذا أردت أن يكون خادم الإدارة متصلاً بخادم وكيل KSN عبر منفذ UDP، مكن خيار **استخدام منفذ UDP** وحدد رقم منفذ لـ **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.

6. قم بتبديل زر التبديل إلى وضع **توصيل خوادم الإدارة الثانوية بشبكة KSN عبر خادم الإدارة الأساسي**.

إذا تم تحديد هذا الخيار، ستستخدم خوادم الإدارة الثانوية خادم الإدارة الرئيسي كخادم وكيل KSN. إذا تم تعطيل هذا الخيار، فستتصل خوادم الإدارة الثانوية بشبكة KSN بنفسهم. وفي هذه الحالة، ستستخدم الأجهزة المُدارة خوادم الإدارة الثانوية كخوادم لوكيل KSN

خوادم الإدارة الثانوية تستخدم خادم الإدارة الرئيسي كخادم وكيل إذا كان زر التبديل في الجزء الأيمن بالقسم **إعدادات وكيل KSN** في خصائص خادم الإدارة الثانوي على وضع **تمكين وكيل KSN على خادم الإدارة** ممكن.

7. انقر على زر **حفظ**.

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 KSN (Kaspersky Security Network):

1. تأكد من أن نقطة التوزيع **معينة يدويًا**.

2. في نافذة التطبيق الرئيسية، انقر فوق أيقونة **الإعدادات** (⚙️) بجوار اسم خادم الإدارة المطلوب. تفتح نافذة خصائص خادم الإدارة.

3. في علامة التبويب **عام**، حدد قسم **نقاط التوزيع**.

4. انقر على اسم نقطة التوزيع لفتح نافذة خصائصها.

5. في نافذة خصائص نقطة التوزيع، في قسم وكيل KSN، قم بتمكين خيار تمكين وكيل KSN من جانب نقطة التوزيع، ثم قم بتمكين خيار الوصول إلى KSN / Cloud / شبكة KSN الخاصة مباشرة عبر الإنترنت.

6. انقر على موافق.

ستعمل نقطة التوزيع كخادم وكيل KSN.

تمكين وتعطيل KSN

لتمكين KSN:

1. انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، حدد قسم إعدادات وكيل KSN.

3. قم بتبديل زر التبديل إلى وضع تمكين وكيل KSN على خادم الإدارة ممكن.

تم تمكين خادم وكيل KSN.

4. بدل زر التبديل إلى وضع استخدام شبكة Kaspersky Security Network **مفعل**.

سيتم تمكين KSN.

إذا تم تمكين زر التبديل هذا، سترسل أجهزة العملاء نتائج تثبيت التصحيح إلى Kaspersky. عند تمكين زر التبديل هذا، ينبغي عليك قراءة بنود بيان KSN والموافقة عليها.

5. انقر على زر **حفظ**.

لتعطيل KSN:

1. انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، حدد قسم إعدادات وكيل KSN.

3. قم بتبديل زر التبديل إلى وضع تمكين وكيل KSN على خادم الإدارة **معطل** لتعطيل خدمة وكيل KSN، أو قم بتبديل زر التبديل إلى وضع استخدام شبكة Kaspersky Security Network **معطل**.

إذا تم تعطيل زر التبديل هذا، فلن ترسل الأجهزة العميلة نتائج تثبيت التصحيح إلى Kaspersky.

إذا كنت تستخدم شبكة KSN الخاصة، قم بتبديل زر التبديل إلى وضع استخدام شبكة Kaspersky Private Security Network **خاصة معطل**.

سيتم تعطيل KSN.

4. انقر على زر **حفظ**.

عرض بيان KSN المقبول

عندما تقوم بتمكين KSN (Kaspersky Security Network)، يجب عليك قراءة بيان KSN وقبوله. يمكنك عرض بيان KSN المقبول في أي وقت.

لعرض بيان KSN المقبول:

1. انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، حدد قسم إعدادات وكيل KSN.

3. انقر على رابط عرض بيان شبكة Kaspersky Security Network.

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، سيتم عرضه لك عندما تحدث خادم الإدارة أو تقوم بتحديثه. 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 ترفيقته، 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. انقر على الرابط عرض الإخطارات في الزاوية العلوية اليمنى من نافذة التطبيق الرئيسية.

سنفتح نافذة الإخطارات.

2. انقر على رابط عرض بيان KSN المحدث.

سنفتح نافذة تحديث بيان Kaspersky Security Network.

3. اقرأ بيان KSN بعناية 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 كوكيل KSN

يمكنك تمكين وكيل KSN على جهاز مُدار تم تعيينه للعمل كنقطة توزيع. يعمل الجهاز المُدار كوكيل KSN عند تشغيل خدمة ksnproxy على الجهاز. يمكنك التحقق من هذه الخدمة أو تشغيلها أو إيقاف تشغيلها على الجهاز محليًا.

للتحقق مما إذا كانت نقطة التوزيع تعمل كوكيل 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 كوكيل 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.

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 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.

2 الحصول على ملف المثبت 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.

3 إنشاء نسخة احتياطية من الإصدار السابق

استخدم [الأداة المساعدة للنسخ الاحتياطي واسترداد البيانات](#) لإنشاء نسخة احتياطية من بيانات خادم الإدارة.

4 تشغيل المثبت

[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.

5 ترقية التطبيقات المُدارة

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 14 Web Console، انقر في أعلى الشاشة على أيقونة [الإعدادات](#) (⚙️) الموجودة بجوار اسم خادم الإدارة. في نافذة خصائص خادم الإدارة التي تفتح، حدد قسم عام في تبويب عام. سيتم عرض الإصدار.

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 المثبتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

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 المثبتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان
- عند إكمال هذا 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 14 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 تشغّل "المعالج"، قم بإنشاء المهمة الآن.

المهمة المطلوبة لتنزيل التحديثات من خوادم تحديث Kaspersky إلى مستودع خادم الإدارة وكذلك لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج - 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 14 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 مباشرة 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 تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع، 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 14 Web Console](#): إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

4 تكوين نقاط التوزيع

عندما تقوم شبكتك بتخصيص نقاط توزيع، تأكد أن خيار نشر التحديثات 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 توزيع الملفات عبر نقاط التوزيع فقط 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 تنزيل التحديثات وقواعد بيانات مكافحة الفيروسات من خادم الإدارة مقدماً (مستحسن) في [سياسة وكيل 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 يشعل 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 تنزيل ملفات تفاضلية في خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة و/أو مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع.

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 14 Web Console](#): [تمكين النموذج غير المتصل بالإنترنت لتنزيل التحديثات وتعطيله](#)

6 التحقق من التحديثات المُنزلة (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 الفيروسات 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 التحكم الإدارية أو خيار التحقق من صحة التحديث في Kaspersky Security Center 14 Web Console.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [التحقق من التحديثات المُنزلة](#)

- [Kaspersky Security Center 14 Web Console](#): [التحقق من التحديثات المُنزلة](#)

- 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 دائماً. 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 مسبقاً، سيحاول Kaspersky Security Center إلغاء تثبيت ذلك التحديث من جميع الأجهزة. لا يمكن إلغاء تثبيت التحديثات لمكونات Kaspersky Security Center.

تعليمات للمساعدة:

• وحدة تحكم الإدارة: [الموافقة على تحديثات البرامج ورفضها](#)

• [Kaspersky Security Center 14 Web Console](#): [الموافقة على تحديثات البرامج ورفضها](#)

8 تكوين التثبيت التلقائي للتحديثات والتصحيحات المخصصة لمكونات Kaspersky Security Center

بدءاً من الإصدار Service Pack 2 10، يتم تلقائياً تثبيت التحديثات والتصحيحات المنزلة لعميل الشبكة ومكونات [Kaspersky Security Center الأخرى](#). إذا تركت خيار التثبيت التلقائي للتحديثات القابلة للتطبيق وتصحيحات المكونات التي لها حالة غير محددة مفعلاً في خصائص عميل الشبكة، عندها سيتم جميع التحديثات تلقائياً 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.

بالنسبة لإصدارات وكيل الشبكة الأقدم من Service Pack 2 10، تأكد من تمكين الخيار تحديث الوحدات النمطية لعميل الشبكة في خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة أو مهمة تنزيل التحديثات إلى مستودعات توزيع النقاط.

تعليمات للمساعدة:

• وحدة تحكم الإدارة: [تمكين وتعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center](#)

• [Kaspersky Security Center 14 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 تلقائياً ويجب أن تتم الموافقة عليها بشكل مبدئي من قبل المسؤول في تبويب المراقبة في وحدة تحكم الإدارة (خادم الإدارة > اسم الخادم < المراقبة) أو في قسم الإخطارات في وحدة تحكم الويب Kaspersky Security Center 14 (المراقبة والإبلاغ ← الإخطارات). يجب أن يقوم المدير بعد ذلك بتنشغيل تثبيت التحديثات بشكل صريح.

10 تكوين التثبيت التلقائي لتحديثات تطبيقات الأمان.

قم بإنشاء مهام التحديثات للتطبيقات المُدارة من أجل توفير تحديثات 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 عند تنزيل تحديثات جديدة إلى المستودع 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) و عميل الشبكة (الإصدار الأقدم من 13.2) على الإدارة الأجهزة.

بشكل افتراضي، لا يتم تثبيت تحديثات Kaspersky Endpoint Security for Windows و Kaspersky 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 14 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:

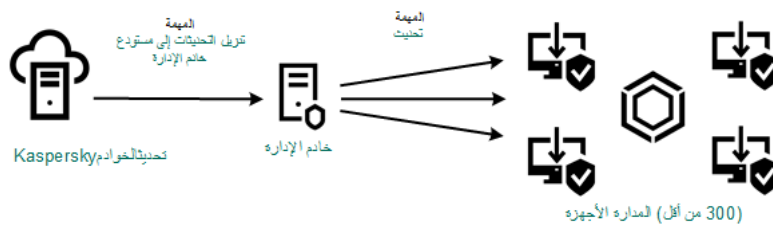
- قواعد بيانات Kaspersky والوحدات النمطية للبرامج

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 DNS العام. يُعد ذلك ضروريًا للتأكد من تحديث قواعد بيانات مكافحة الفيروسات والحفاظ على مستوى الأمان للأجهزة المُدارة.

- تطبيقات Kaspersky المثبتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان
- 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 for Windows على الأجهزة المُدارة

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).

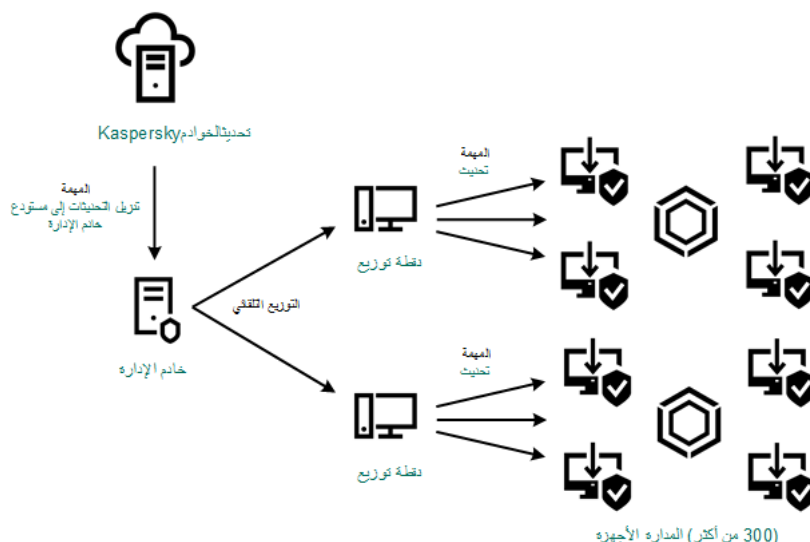


التحديث باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة دون نقاط توزيع

يتصل خادم الإدارة افتراضياً 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 المطلوبة 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 لـ Kaspersky Endpoint Security for Windows](#).
- تحديثات خادم الإدارة لا يتم تثبيت هذه التحديثات تلقائيًا. ويجب على المسؤول الموافقة صراحة على تثبيت التحديثات وتشغيلها.

تلتزم حقوق المسؤول المحلي لتثبيت التصحيحات على خادم الإدارة.

- تحديثات مكونات Kaspersky Security Center يتم افتراضياً تثبيت هذه التحديثات تلقائيًا. ويمكنك [تغيير الإعدادات في سياسة عميل الشبكة](#).
- تحديثات تطبيقات الأمان 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 14 Web Console](#)). ويتم تثبيت التحديثات من خلال المهمة تحديث ويمكن تكوينها في خصائص هذه المهمة.

لا تتوفر تنزيل التحديثات إلى مستودع مهمة خادم الإدارة على خوادم الإدارة الافتراضية. مستودع خادم الإدارة الافتراضي يعرض التحديثات المنزلة 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.

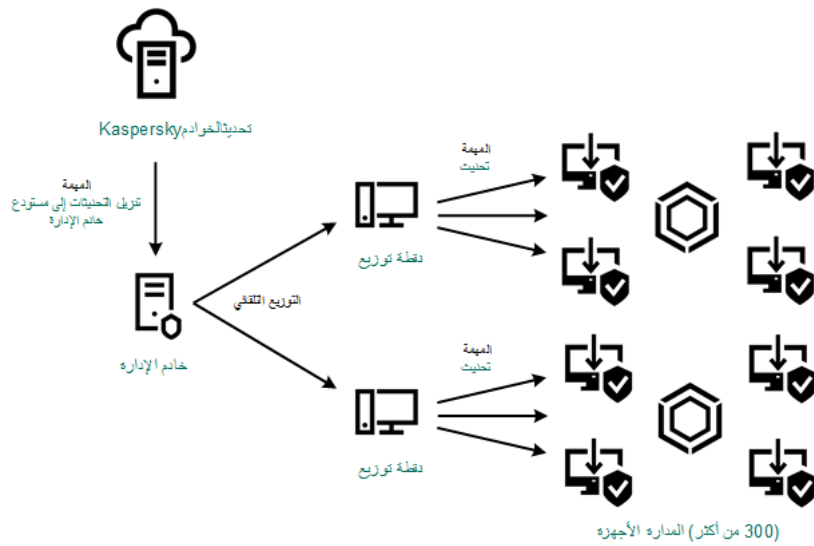
يتطلب كل تطبيق من تطبيقات Kaspersky تحديثات من خادم الإدارة. قام خادم الإدارة بتجميع تلك الطلبات وتنزيل التحديثات التي تم طلبها من قبل التطبيق فقط. يضمن هذا عدم تنزيل نفس التحديثات عدة مرات وعدم تنزيل التحديثات غير الضرورية أبدًا. عند تشغيل مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يرسل خادم الإدارة 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 المفعّل
- معرف تشغيل تنزيل التحديثات إلى مستودع مهمة خادم الإدارة

لا تحتوي أيّ من المعلومات المنقولة على تفاصيل شخصية أو بيانات سرية أخرى. يحمي AO Kaspersky Lab المعلومات وفقاً 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 افتراضياً 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 التوزيع بالإضافة إلى مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. وبعد ذلك، ستقوم نقاط التوزيع بتنزيل التحديثات من خوادم تحديث Kaspersky وليس من مستودع خادم الإدارة.

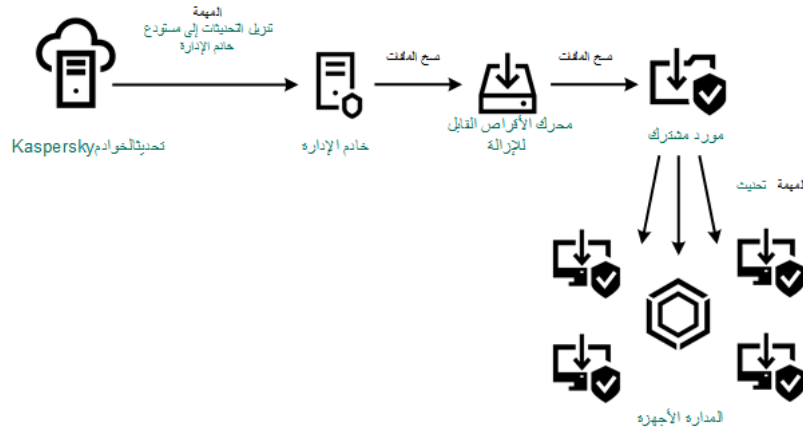
لا يمكن لأجهزة نقاط التوزيع التي تعمل بنظام macOS تنزيل التحديثات من خوادم تحديث Kaspersky.

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، نظراً 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

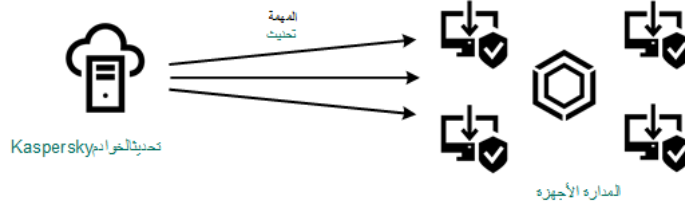
إذا لم تتمتع الأجهزة العملية باتصال بخادم الإدارة، يمكنك استخدام مجلد محلي أو مورد مشترك كمصدر لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. وفي هذا المخطط، تحتاج إلى نسخ التحديثات اللازمة من مستودع خادم الإدارة إلى محرك الأقراص القابل للإزالة ونسخ التحديثات إلى المجلد المحلي أو المورد المشترك المحدد كمصدر تحديث في إعدادات Kaspersky Endpoint Security for Windows (انظر الشكل أدناه).



التحديث من خلال مجلد محلي أو مجلد مشترك أو خادم FTP

مباشرة من خوادم تحديث Kaspersky إلى Kaspersky Endpoint Security for Windows على الأجهزة المُدارة

على الأجهزة المُدارة، يمكنك تكوين Kaspersky Endpoint Security for Windows لتلقي التحديثات مباشرة من خوادم تحديث Kaspersky (انظر الشكل أدناه).



تحديث تطبيقات الأمان مباشرة من خوادم تحديث Kaspersky

في هذا المخطط، لا يستخدم تطبيق الأمان المستودعات المتوفرة من Kaspersky Security Center. ولتلقى التحديثات مباشرة من خوادم تحديث Kaspersky، حدد خوادم تحديث Kaspersky كمصدر تحديث في واجهة تطبيق الأمان. للحصول على وصف كامل لهذه الإعدادات، يرجى الرجوع إلى وثائق [Kaspersky Endpoint Security for Windows](#).

إنشاء مهمة لتنزيل التحديثات إلى مستودع خادم الإدارة

يتم إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة لخادم الإدارة تلقائيًا بواسطة معالج البدء السريع لـ Kaspersky Security Center. لا يمكنك إنشاء إلا مهمة تنزيل التحديثات إلى مستودع خادم الإدارة واحدة. ولهذا السبب، لا يمكنك إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة 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 المُدارة، يمكنك تشغيل المهمة **التحقق من التحديث**. يمكنك ذلك من التأكد من أن خادم الإدارة سبُتت التحديثات التي تم تنزيلها بشكل صحيح ولن ينخفض مستوى الأمان بسبب التحديثات. للتحقق منها قبل التوزيع، عليك تكوين الخيار **التحقق من صحة التحديث في إعدادات** مهمة تنزيل التحديثات إلى مستودع خادم الإدارة.

لإنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

2. انقر فوق **إضافة**.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة **تنزيل التحديثات إلى مستودع خادم الإدارة**.

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 **فتح تفاصيل المهمة عند اكتمال الإنشاء** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

6. انقر فوق الزر **إنشاء**.

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 **إعدادات التطبيق**:

• **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.

إذا قمت بتمكين الخيار **لا تستخدم الخادم الوكيل** خوادم تحديث Kaspersky أو مصادر التحديث المجلد المحلي أو مجلد الشبكة، فلن يستخدم خادم الإدارة خادمًا وكيلاً لتنزيل التحديثات.

• مجلد لتخزين التحديثات ⑤

المسار إلى المجلد المحدد لتخزين التحديثات المحفوظة. يمكنك نسخ مسار المجلد المحدد إلى الحافظة. لا يمكنك تغيير المسار إلى مجلد محدد لمهمة جماعية.

• إعدادات أخرى:

• فرض التحديث لخوادم الإدارة الثانوية ⑤

إذا تم تمكين هذا الخيار، فسيبدأ خادم الإدارة بتشغيل مهام التحديث على خوادم الإدارة الثانوية بمجرد أن يتم تنزيل التحديثات الجديدة. بخلاف ذلك، تبدأ مهام التحديث على خوادم الإدارة الثانوية بالعمل وفقاً للجدول الزمنية الخاصة بهم. يتم تعطيل هذا الخيار افتراضياً.

• نسخ التحديثات التي تم تنزيلها إلى مجلدات إضافية ⑤

بعد تلقي خادم الإدارة للتحديثات، يقوم بنسخها إلى المجلدات المحددة. استخدم هذا الخيار في حال رغبت في إدارة توزيع التحديثات يدوياً 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 إلى مستودع المهام لخوادم إدارة أخرى، قم بتحديد نفس مشاركة الشبكة كمصدر تحديث.

يتم تعطيل هذا الخيار افتراضياً.

• لا تفرض تحديث الأجهزة وخوادم الإدارة الثانوية إلا عند اكتمال النسخ ⑤

تبدأ مهام تنزيل التحديثات على الأجهزة العملية وخوادم الإدارة الثانوية فقط بعد نسخ تلك التحديثات من مجلد التحديث الرئيسي إلى مجلدات التحديث الإضافية.

يجب تمكين هذا الخيار إذا كانت الأجهزة العملية وخوادم الإدارة الثانوية تقوم بتنزيل تحديثات من مجلدات شبكة إضافية. يتم تعطيل هذا الخيار افتراضياً.

• محتوى التحديثات:

• تنزيل ملفات تفاضلية ⑤

يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff. يتم تعطيل هذا الخيار افتراضياً.

• تنزيل التحديثات باستخدام النظام القديم ⑤

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 بيانات تعريف متوافقة مع النظام الجديد. إذا كان مصدر التحديث يحتوي على ملفات تحديث بيانات 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.

• [التحقق من صحة التحديث](#)

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.

1. في تبويب **الجدول** من نافذة خصائص المهمة، قم بإنشاء جدول لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

• [البدء المُجدول](#)

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

• [يدويًا](#)

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط. يتم تمكين هذا الخيار افتراضيًا.

• [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.

• [كل N ساعة](#)

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين. بشكل افتراضي، تعمل المهمة كل ست 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 ⑤

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.

• يوميًا (التوقيت الصيفي غير مدعوم) ⑤

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 ⑤

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• حسب أيام الأسبوع ⑤

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد. بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهريًا ⑤

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 ⑤

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد. بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• عند انتشار الفيروس ⑤

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 المحيط

• مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.

قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• 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، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدويًا ومرة وفورًا، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.

يتم تمكين هذا الخيار افتراضيًا.

• استخدام التأخير العشوائي لتلقائي 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.

• 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.

2. انقر على زر **حفظ**.

سيتم إنشاء المهمة وتكوينها.

عندما يجري خادم الإدارة مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، 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 العملية وخوادم الإدارة الثانوية من المجلد المشترك لخادم الإدارة.

عرض التحديثات المُنزلة

عندما يجري خادم الإدارة مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يتم تنزيل تحديثات قواعد البيانات والوحدات النمطية للبرامج من مصدر التحديثات ويتم تخزينها في مجلد خادم الإدارة المشترك. يمكنك عرض التحديثات التي تم تنزيلها في قسم **تحديثات قواعد بيانات KASPERSKY** ووحدات البرامج النمطية.

لعرض قائمة التحديثات المنزلة:

في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات KASPERSKY** ← **تحديثات قواعد بيانات KASPERSKY** ووحدات البرامج النمطية.

ستظهر قائمة بالتحديثات المتاحة.

التحقق من التحديثات المُنزلة

قبل تثبيت التحديثات على الأجهزة المدارة، يمكنك أولاً التحقق من صحة التحديث الخاصة بقبالية التشغيل والأخطاء من خلال مهمة التحقق من صحة التحديث. يتم تنفيذ مهمة التحقق من صحة التحديث تلقائياً كجزء من مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. 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. أيضاً 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 صحيحاً 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.

نوصى 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. **إنشاء مهام التحديث وفحص الفيروسات** لتطبيق مدعوم من Kaspersky Security Center، على سبيل المثال Kaspersky Endpoint Security for Windows أو Kaspersky Security for Windows Server. عند إنشاء مهام التحديث وفحص الفيروسات، حدد مجموعة الإدارة مع أجهزة

تقوم مهمة التحقق من صحة التحديث بتشغيل مهام التحديث وفحص الفيروسات بالتتابع على أجهزة الاختبار للتحقق من صحة جميع التحديثات. بالإضافة إلى ذلك، عند إنشاء مهمة التحقق من صحة التحديث، تحتاج إلى تحديد مهمتي التحديث وفحص الفيروسات.

3. إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة.

لجعل التطبيق Kaspersky Security Center يتحقق من التحديثات التي تم تنزيلها قبل توزيعها إلى الأجهزة العملية:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← المهام.
2. انقر على مهمة تنزيل التحديثات إلى مستودع خادم الإدارة.
3. في النافذة خصائص المهمة التي تفتح، انتقل إلى علامة التبويب إعدادات التطبيق، ومن ثم قم بتمكين الخيار التحقق من صحة التحديث.
4. إذا كانت مهمة التحقق من صحة التحديث موجودة، فانقر فوق الزر حدد المهمة. 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 مهمة جديدة.

b. في معالج إضافة مهمة 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 الفيروسات.

بعد ذلك، تظهر الخيارات التالية. نوصي بتركها ممكّنة:

• **أعد تشغيل الجهاز بعد تحديث قاعدة البيانات**

بعد تحديث قواعد بيانات مكافحة الفيروسات على الجهاز، نوصي بإعادة تشغيل الجهاز. يتم تمكين هذا الخيار بشكل افتراضي.

• **تحقق من حالة الحماية في الوقت الحقيقي بعد تحديث قاعدة البيانات وإعادة تشغيل الجهاز**

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 افتراضياً.

e. حدد حسابًا سيتم تشغيل مهمة التحقق من صحة التحديث منه. يمكنك استخدام حسابك وترك خيار الحساب الافتراضي ممكّنًا. أو بدلاً من ذلك، يمكنك تحديد أنه يجب أن يتم تشغيل المهمة ضمن حساب آخر لديه حقوق الوصول الضرورية. وللقيام بذلك، حدد خيار تحديد حساب، ثم أدخل بيانات اعتماد هذا الحساب.

6. انقر فوق حفظ لإغلاق نافذة الخصائص الخاصة بالمهمة تنزيل التحديثات إلى مستودع خادم الإدارة.

يتم تفعيل التحقق التلقائي من التحديثات. يمكنك الآن تشغيل مهمة تنزيل التحديثات إلى مستودع خادم الإدارة وستبدأ من التحقق من صحة التحديث.

إنشاء مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع

لا تعمل مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع إلا على أجهزة نقاط التوزيع التي تعمل بنظام Windows. أجهزة نقطة التوزيع التي تعمل بنظام Linux أو macOS لا يمكن أن تقوم بتنزيل التحديثات من خوادم تحديث Kaspersky. وفي حال وجود جهاز واحد على الأقل يعمل بنظام أو Linux أو macOS داخل نطاق المهمة، ستكون حالة المهمة فشلت. حتى إذا تم إكمال المهمة بنجاح على جميع الأجهزة التي تعمل بنظام Windows، سوف تُرجع خطأ 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.

لإنشاء مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع لمجموعة إدارة محددة:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← المهام.

2. انقر على زر إضافة.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر التالي.

3. لتطبيق Kaspersky Security Center في حقل نوع المهمة، حدد تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع.

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 إنهاء عملية إنشاء المهمة، إذا كنت تريد تعديل إعدادات المهمة الافتراضية، فقم بتمكين فتح تفاصيل المهمة عند اكتمال الإنشاء اختيار. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقاً في أي وقت.

7. انقر فوق الزر إنشاء.

يتم إنشاء المهمة وعرضها في قائمة المهام.

8. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

9. في تبويب إعدادات التطبيق في نافذة خصائص المهمة، حدد الإعدادات التالية:

• [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 المثبت 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.

إذا قمت بتمكين الخيار **لا تستخدم الخادم الوكيل** خوادم تحديث Kaspersky أو مصادر التحديث المجلد المحلي أو مجلد الشبكة، فلن تستخدم نقطة التوزيع خادمًا وكيلاً لتنزيل التحديثات، حتى عند تمكين الخيار **استخدام الخادم الوكيل في إعدادات سياسة عميل الشبكة** الخاصة بنقطة التوزيع.

- **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 ملفات تفاضلية**

يقوم هذا الخيار بتمكين ميزة **تنزيل ملفات diff**.

يتم تعطيل هذا الخيار افتراضياً.

- **تنزيل التحديثات باستخدام النظام القديم**

بدءاً 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 افتراضياً.

• **البدء المُجدول** ④

حدد الجدول الذي تعمل المهمة وفقاً له، وقم بتكوين الجدول المحدد.

• **يدويًا** ④

لا يتم تشغيل المهمة تلقائيًا. يمكنك بدء تشغيلها يدويًا فقط.
يتم تمكين هذا الخيار افتراضيًا.

• **كل N دقيقة** ④

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.

• **كل N ساعة** ④

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.
بشكل افتراضي، تعمل المهمة كل ست ساعات، بداية من التاريخ والوقت الحاليين للنظام.

• **كل N يومًا** ④

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** ④

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.

• **يوميًا (التوقيت الصيفي غير مدعوم)** ④

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** ④

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

• **حسب أيام الأسبوع** ④

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.
بشكل افتراضي، تعمل المهمة كل يوم جمعة الساعة 6:00:00 مساءً.

• شهرياً ⑤

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 ⑤

تعمل المهمة بشكل منتظم، في الأيام المحددة من كل شهر وفي الوقت المحدد.
بشكل افتراضي، لا يتم تحديد أي يوم من أيام الشهر، حيث يكون وقت البدء الافتراضي عند 6:00:00 مساءً.

• عند انتشار الفيروس ⑤

تعمل المهمة بعد وقوع حدث انتشار الفيروسات. حدد أنواع التطبيق التي ستقوم بمراقبة انتشار الفيروسات. تتوفر أنواع التطبيق التالية:

- مكافحة الفيروسات لمحطات العمل وخوادم الملفات
- مكافحة الفيروسات للدفاع المحيط
- مكافحة الفيروسات لأنظمة البريد.

بشكل افتراضي، يتم تحديد جميع أنواع التطبيق.
قد ترغب في تشغيل مهام مختلفة وفقاً لنوع تطبيق مكافحة الفيروسات والذي يقوم بالإبلاغ عن انتشار الفيروسات. في هذه الحالة، قم بإزالة التحديد من أنواع التطبيق التي لا تحتاجها.

• عند إكمال مهمة أخرى ⑤

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية. على سبيل المثال، قد ترغب في تشغيل مهمة إدارة الأجهزة باستخدام الخيار **تشغيل الجهاز** وبعد اكتمالها، قم بتشغيل مهمة فحص الفيروسات.

• تشغيل المهام الفائتة ⑤

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 يدوياً أو مرة أو فوراً، فستبدأ المهمة على الفور بعد ظهور الجهاز على الشبكة أو بعد تضمين الجهاز في نطاق المهمة.
إذا تم تعطيل هذا الخيار، فسيتم تشغيل المهام المجدولة فقط على أجهزة العميل؛ ولأوضاع يدوياً ومرة وفوراً، فسيتم تشغيل المهام فقط على هذه الأجهزة العميلة الظاهرة على الشبكة. على سبيل المثال، قد ترغب في تعطيل هذا الخيار لمهمة مستهلكة للموارد ترغب في تشغيلها خارج ساعات العمل فقط.
يتم تمكين هذا الخيار افتراضياً.

• استخدم التأخير العشوائي لبدء المهام تلقائياً ⑤

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) [5]

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 حفظ.

سيتم إنشاء المهمة وتكوينها.

بالإضافة إلى الإعدادات التي تقوم بتحديدتها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

عند تنفيذ مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط 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.

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 العمليات ← المستودعات ← حزم التثبيت.

2. انقر على حزمة عميل شبكة Kaspersky Security Center > رقم الإصدار.

3. في نافذة الخصائص، افتح تبويب إعدادات.

4. أعلّق زر التبديل 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.

لتمكن أو تعطيل التحديث والتصحيح التلقائيين لمكونات Kaspersky Security Center باستخدام سياسة عميل الشبكة:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← السياسات وملفات التعريف.

2. انقر على سياسة عميل الشبكة:

3. في نافذة خصائص السياسة، افتح تبويب إعدادات التطبيق.

4. في قسم إدارة التصحيحات والتحديثات، قم بتشغيل أو إيقاف زر التبديل التلقائي للتحديثات القابلة للتطبيق وتصحيحات المكونات التي لها حالة غير محددة 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 للبرامج الخاصة بـ 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 الأجهزة ← المهام.

2. انقر على زر إضافة.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر التالي.

3. لتطبيق Kaspersky Endpoint Security for Windows، حدد التحديث كالتنوع 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 إنهاء عملية إنشاء المهمة، إذا كنت تريد تعديل إعدادات المهمة الافتراضية، فقم بتمكين فتح تفاصيل المهمة عند اكتمال الإنشاء اختيار. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقاً في أي وقت.

8. انقر فوق الزر إنشاء.

يتم إنشاء المهمة وعرضها في قائمة المهام.

9. انقر على اسم المهمة التي تم إنشاؤها لفتح نافذة خصائص المهمة.

10. في تبويب إعدادات التطبيق 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 زر **نقل لأعلى** و**نقل لأسفل** إذا كان ذلك ضرورياً. في حال تفعيل عدة مصادر تحديث، يحاول Kaspersky Endpoint Security for Windows الاتصال بهم واحداً بعد الآخر بدءاً 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 جنباً إلى جنب مع قواعد بيانات التطبيق. في حال تفعيل هذا الخيار، يقوم Kaspersky Endpoint Security for Windows بإخطار المستخدم بتحديثات الوحدة النمطية للبرنامج المتوفرة وتضمن 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 محلياً من خلال واجهة التطبيق أو من خلال Kaspersky Security Center.

يمكنك كذلك تفعيل خيار **تثبيت التحديثات الحرجة للوحدة النمطية للتطبيق تلقائياً**. إذا توافرت أي تحديثات للوحدات النمطية للبرنامج، يقوم Kaspersky Endpoint Security for Windows بتثبيت التحديثات التي حالتها حرجة تلقائياً؛ 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 فوق **حفظ**.

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 أولاً بالتحقق من تثبيت التحديثات في بيئة اختبار والتأكد من عدم تدخلها في عملية تشغيل الأجهزة، وبعد ذلك فقط تسمح بتثبيت تلك التحديثات على الأجهزة العميلة.

قم بما يلي للموافقة على أو رفض تحديث واحد أو عدة تحديثات:

1. انتقل إلى **العمليات** ← **تطبيقات KASPERSKY**، ومن القائمة المنسدلة حدد **تحديثات مستمرة**.

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. س يُطلب منك ترقية مثيلك من Kaspersky Security Center إلى الإصدار الأدنى المطلوب.

2. حدد التحديثات التي ترغب في الموافقة عليها أو رفضها.

3. انقر على **الموافقة** للموافقة على التحديثات المحددة أو **رفض** 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 تثبت 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 تحديث معالج خادم الإدارة.

لتثبيت تحديث خادم إدارة:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات KASPERSKY** ← **تحديثات مستمرة**.

2. قم بتشغيل تحديث معالج خادم الإدارة بإحدى الطرق التالية:

- انقر على اسم تحديث خادم الإدارة في قائمة التحديثات، وفي النافذة التي تفتح انقر على **رابط تشغيل معالج تحديث خادم الإدارة**.
- انقر على **رابط تشغيل معالج تحديث خادم الإدارة** في حقل الإخطار في أعلى النافذة.
- 3. في نافذة تحديث معالج خادم الإدارة، حدد واحدًا مما يلي لتحديد متى تقوم بتثبيت تحديث:
 - **تثبيت الآن**. 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 **إنشاء نسخة احتياطية من خادم الإدارة قبل تثبيت التحديث** إذا كنت ترغب في إنشاء نسخة احتياطية من خادم الإدارة قبل تثبيت التحديث.

5. انقر على زر **موافق لإنهاء المعالج**.

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 الأجهزة ← السياسات وملفات التعريف.

2. انقر على المجموعات.

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 مورثة، ستحتاج أولاً إلى إنشاء سياسة جديدة لعميل الشبكة في مجموعات الإدارة المطلوبة. يمكنك في السياسة التي تم إنشاؤها حديثاً تعديل الإعدادات التي ليست مقفولة في السياسة الأصلية.

5. في تبويب إعدادات التطبيق، حدد قسم إدارة التصحيحات والتحديثات.

6. قم بتمكين أو تعطيل الخيار تنزيل التحديثات وقواعد بيانات مكافحة الفيروسات من خادم الإدارة مقدماً (مستحسن) 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 الإدارة مثبت عليه نفس تطبيق الأمان. يجب تكوين هذا التطبيق لاستقبال تحديثات من مستودع خادم الإدارة من خلال مهمة تنزيل التحديثات إلى مستودع خادم الإدارة.

- أي جهاز مثبت عليه نفس تطبيق الأمان ومكون من أجل استلام التحديثات من مستودع خادم الإدارة أو مستودع نقطة توزيع أو مباشرة 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.

بشكل 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 **نسخ التحديثات التي تم تنزيلها إلى مجلدات إضافية** في خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. إذا حددت مجلدًا موجودًا على محرك أقراص فلاش أو محرك أقراص ثابت خارجي كالمجلد المستهدف 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 استخدامه 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 14 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 وحدة التحكم** ← **المكونات الإضافية للويب**.

سنتفتح نافذة **إعدادات وحدة التحكم**.

2. في علامة التبويب **المكونات الإضافية للويب**، حدد مكونات الويب الإضافية التي تريد نسخها احتياطيًا، ثم انقر على زر **إنشاء نسخة من النسخة الاحتياطية**.

يتم نسخ مكونات الويب الإضافية المحددة احتياطيًا. يمكنك عرض النسخ الاحتياطية التي تم إنشاؤها على علامة التبويب **النسخ الاحتياطية**.

لاستعادة مكون ويب إضافي من نسخة احتياطية:

1. في القائمة الرئيسية، انتقل إلى **إعدادات وحدة التحكم** ← **النسخ الاحتياطية**.

سنتفتح نافذة **إعدادات وحدة التحكم**.

2. في علامة التبويب **النسخ الاحتياطية**، حدد النسخة الاحتياطية من المكون الإضافي للويب الذي تريد استعادته، ثم انقر على زر **استعادة من النسخة الاحتياطية**.

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 التوافق 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 عميل من عملاء الشبكة في الإصدار Service Pack 110 أو الإصدارات الأحدث بنقطة التوزيع التي لديها المسار الأقصر. 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 والمكتب 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 يدويًا أو تلقائيًا.

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 مباشرة (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.

لتعيين نقاط التوزيع تلقائيًا:

1. في نافذة التطبيق الرئيسية، انقر فوق أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، حدد قسم نقاط التوزيع.

3. 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.

4. انقر على زر حفظ.

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. ولكن، إذا كان يتعين عليك إلغاء الاشتراك في تعيين نقاط التوزيع تلقائيًا لأي سبب (على سبيل المثال، إذا كنت ترغب في استخدام خوادم معينة 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 نافذة التطبيق الرئيسية، انقر فوق أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب عام، حدد قسم نقاط التوزيع.

3. حدد خيار تعيين نقاط التوزيع يدويًا.

4. انقر فوق الزر تعيين

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 إضافة.

سيتم عرض نقطة التوزيع التي أضفتها في قائمة نقاط التوزيع، في القسم نقاط التوزيع.

8. حدد نقطة التوزيع التي تمت إضافتها مؤخرًا في القائمة لفتح نافذة خصائصه.

9. قم بتكوين نقطة التوزيع في نافذة الخصائص:

• يحتوي قسم 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 ⑤

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 ⑤

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 ⑤

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 للاتصال SSL.

• نشر التحديثات ⑤

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 ⑤

يتم توزيع حزم التثبيت 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 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.

• تشغيل خادم الإرسال ⑤

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** للأجهزة 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.

• [إرسال منفذ الخادم](#)

رقم منفذ خادم الإرسال. يمكنك تحديد رقم أي منفذ فارغ.

- في القسم **النطاق**، حدد النطاق الذي ستقوم فيه 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.

- في قسم **مصدر التحديثات**، يمكنك تحديد مصدر تحديثات لنقطة التوزيع:

• [مصادر التحديثات](#)

حدد مصدر تحديثات لنقطة التوزيع:

- للسماح لنقطة التوزيع بتلقي التحديثات من خادم الإدارة، حدد **الاستعادة من خادم الإدارة**.
- للسماح لنقطة التوزيع بتلقي التحديثات باستخدام مهمة، حدد **استخدام مهمة تنزيل التحديث**، ثم حدد المهمة لتنزيل 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 **إنشاء مهمة لإنشاء مهمة**. يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج.

• [تنزيل ملفات تفاضلية](#)

يقوم هذا الخيار بتمكين **ميزة تنزيل ملفات diff**.

يتم تمكين هذا الخيار افتراضيًا.

- من القسم **وكيل KSN**، يمكنك تكوين التطبيق لاستخدام نقطة التوزيع لإعادة توجيه طلبات KSN من الأجهزة المدارة:

• [تمكين وكيل KSN من 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. يوجد بيان KSN افتراضيًا في %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula. يتم تعطيل هذا الخيار افتراضيًا. يسري تمكين هذا الخيار فقط في حالة **تمكين** الخيارين استخدام خادم الإدارة وكيل وأوافق على استخدام Kaspersky Security Network في نافذة خصائص خادم الإدارة. يمكنك تعيين عقدة مجموعة نشط-خامل إلى نقطة توزيع، وتمكين وكيل 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 / شبكة KSN الخاصة مباشرة عبر الإنترنت**

تقوم نقطة التوزيع بإعادة توجيه طلبات KSN من الأجهزة المدارة إلى KSN Cloud أو شبكة KSN الخاصة. يتم أيضًا إرسال طلبات KSN - التي تم إنشاؤها على نقطة التوزيع نفسها - مباشرة إلى KSN Cloud أو Private KSN. لا يمكن لنقاط التوزيع التي لديها الإصدار 11 المثبت لعملاء الشبكة (أو الأقدم)، الوصول إلى شبكة KSN الخاصة مباشرة. إذا كنت ترغب في إعادة تكوين نقاط التوزيع لإرسال طلبات KSN إلى شبكة KSN الخاصة، 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 شبكة KSN الخاصة مباشرة.

• **تجاهل إعدادات خادم وكيل KSC عند الاتصال بشبكة KSN الخاصة**

قم بتمكين هذا الخيار، إذا كانت إعدادات خادم الوكيل مكوّنة في خصائص نقطة التوزيع أو في سياسة Network Agent، لكن كانت بنية شبكتك تتطلب استخدام شبكة KSN الخاصة مباشرة. وإلا، لا يمكن وصول الطلبات الصادرة من التطبيقات المدارة إلى شبكة KSN الخاصة.

• **منفذ TCP**

رقم منفذ TCP الذي ستستخدمه الأجهزة المدارة للاتصال بخادم وكيل KSN. رقم المنفذ الافتراضي هو 13111.

• **منفذ UDP**

إذا احتجت أن تكون الأجهزة المدارة متصلة بخادم وكيل KSN عبر منفذ UDP، فقم بتمكين خيار استخدام منفذ UDP وحدد رقم منفذ UDP. يتم تمكين هذا الخيار افتراضيًا. والمنفذ الافتراضي لـ UDP للاتصال بخادم وكيل KSN هو 15111.

• قم بتكوين استقصاء مجالات Windows، و Active Directory، ونطاقات IP بواسطة نقطة التوزيع:

• **مجالات Windows**

يمكنك تمكين اكتشاف الأجهزة لمجالات Windows وتعيين الجدول للاكتشاف.

• **Active Directory**

يمكنك تمكين استقصاء الشبكة لـ Active Directory وتعيين الجدول للاستقصاء. إذا قمت بتحديد خانة الاختيار **تمكين استقصاء الشبكة**، فيمكنك 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.

• نطاقات IP

يمكنك تمكين اكتشاف الجهاز لنطاقات IPv4 وشبكات IPv6.

إذا مكنت خيار **تمكين استقصاء النطاق**، فيمكنك إضافة نطاقات ممسوحة ضوئياً وتعيين الجدول الزمني لها. يمكنك **إضافة نطاقات IP لقائمة النطاقات التي تم فحصها.**

إذا مكنت خيار **تمكين الاستقصاء باستخدام تقنية شبكة لا تتطلب تكويناً** فستقوم نقطة التوزيع تلقائياً باستقصاء شبكة IPv6 باستخدام **شبكات التكوين الصفري** (وكما يشار إليها باسم شبكة لا تتطلب تكويناً). في هذه الحالة، يتم تجاهل نطاقات IP المحددة لأن نقطة التوزيع تستقصي الشبكة بالكامل.

- 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 موافق.

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 **الأجهزة** ← **المجموعات**.

2. في بنية مجموعة الإدارة، حدد مجموعة الإدارة التي ترغب في عرض نقاط التوزيع بها.

3. حدد علامة التبويب **نقاط التوزيع**.

4. أضف نقاط توزيع إلى مجموعة الإدارة باستخدام زر **تعيين** أو أزل نقاط التوزيع المخصصة عن طريق استخدام زر **إلغاء تعيين**.

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 Google Firebase Cloud Messaging**.

مزامنة جهاز واحد

لفرض المزامنة بين خادم الإدارة وجهاز مُدار:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **الأجهزة المُدارة**.

2. انقر على اسم الجهاز الذي ترغب في مزامنته مع خادم الإدارة.
سنفتح نافذة خصائص مع قسم عام محدد.

3. انقر على زر **فرض المزامنة**.

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 **الأجهزة** ← **الأجهزة المُدارة** ← **المجموعات**، وبعدها حدد مجموعة الإدارة التي تحتوي على أجهزة لمزامنتها.
- **أجر تحديد جهاز** لعرض قائمة الجهاز.

2. حدد خانة الاختيار الموجودة بجوار الأجهزة التي ترغب في مزامنتها مع خادم الإدارة.

3. انقر على زر **فرض المزامنة**.

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 **تحديث**.

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 **الأجهزة** ← **الأجهزة المُدارة**.
2. انقر على اسم الجهاز الذي ترغب في مزامنته مع خادم الإدارة.
سنفتح نافذة خصائص مع قسم عام محدد.
3. حدد علامة التبويب **التطبيقات**.
4. حدد التطبيق الذي ترغب في عرض تاريخ مزامنة السياسة له.
سنفتح نافذة سياسة التطبيق مع تحديد قسم عام 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 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. 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 **عَدك قَطع الاتصال بخادم الإدارة** على الأجهزة المدارة أو إرسال الحزم إلى منفذ UDP الخاص بوكيل الشبكة.

يدعم خادم الدفع تحميل ما يصل إلى 50000 اتصال متزامن.

لتمكين خادم الإرسال على نقطة توزيع:

1. انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.
2. في علامة التبويب **عام**، حدد قسم **نقاط التوزيع**.
3. انقر فوق اسم نقطة التوزيع التي تريد تمكين خادم الإرسال عليها.
يتم فتح نافذة خصائص نقطة التوزيع.
4. في قسم **عام**، مَكِّن خيار **تشغيل خادم الإرسال**.
5. في حقل **إرسال منفذ الخادم**، 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 **موافق**.

إدارة تطبيقات الجهات الخارجية على أجهزة العميل

يصف هذا القسم مزايا Kaspersky Security Center المتعلقة بإدارة تطبيقات الأطراف الخارجية المثبتة على أجهزة العميل.

حول تطبيقات الجهات الخارجية

يمكن أن يساعدك Kaspersky Security Center على تحديث برامج الجهات الخارجية المثبتة على أجهزة العميل وإصلاح نقاط الضعف في برنامج الجهة الخارجية. يمكن لـ Kaspersky Security Center تحديث برامج الجهات الخارجية من الإصدار الحالي إلى الإصدار الأحدث فقط. تمثل القائمة التالية برامج الجهة الخارجية التي يمكنك تحديثها باستخدام Kaspersky Security Center:

يمكن تحديث قائمة برامج الجهات الخارجية وتوسيعها باستخدام تطبيقات جديدة. يمكنك التحقق مما إذا كان بإمكانك تحديث برنامج الجهة الخارجية (المثبت على أجهزة المستخدمين) باستخدام Kaspersky Security Center من خلال [عرض قائمة التحديثات المتوفرة في Kaspersky Security Center 14 Web Console](#).

- مطورو Zip: 7-Zip-7
- Adobe Systems
- Adobe Acrobat DC
- Adobe Acrobat Reader DC
- Adobe Acrobat
- Adobe Reader
- Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple
- Apple iTunes
- Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber

- Code Sector: TeraCopy •
- DbVis Software AB: DbVisualizer •
- Srl: Iperius Backup أدخل •
- دليل الترميز: •
- K-Lite Codec Pack Basic •
- K-Lite Codec Pack Full •
- K-Lite Codec Pack Mega •
- K-Lite Codec Pack Standard •
- :Decho Corp •
- Mozy Enterprise •
- Mozy Home •
- Mozy Pro •
- Dominik Reichl: KeePass Password Safe •
- ++Don HO don.h@free.fr: Notepad •
- DoubleGIS: 2GIS •
- Dropbox, Inc.: Dropbox •
- EaseUs: EaseUS Todo Backup Free •
- Electrum Technologies GmbH: Electrum •
- Eric Lawrence: Fiddler •
- EverNote: EverNote •
- Exodus Movement Inc: Exodus •
- EZB Systems: UltraISO •
- :Famatech •
- Radmin •
- المسؤول عن بعد •
- Far Manager: FAR Manager •
- FastStone Soft: FastStone Image Viewer •
- Firebird Developers: Firebird •

- :Foxit Corporation
- Foxit Reader
- Foxit Reader Enterprise
- Free Download Manager.ORG: مدير تنزيل مجاني
- GIMP project: GIMP
- GlavSoft LLC.: TightVNC
- GNU Project: Gpg4win
- :Google
- Google Earth
- Google Chrome
- Google Chrome Enterprise
- Google Earth Pro
- Google Backup and Sync
- Inkscape Project: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- JustSystems Corporation: Ichitaro
- Logitech: SetPoint
- :LogMeIn, Inc
- LogMeIn
- Hamachi
- LogMeIn Rescue Technician Console
- RemotelyAnywhere Workstation Edition
- Martin Prikryl: WinSCP
- :Mozilla Foundation
- Mozilla Firefox
- Mozilla Firefox ESR
- Mozilla SeaMonkey

- Mozilla Thunderbird •
- OpenOffice.org: OpenOffice.org •
- Opera Software: Opera •
- :Oracle Corporation •
- Oracle Java JRE •
- Oracle VirtualBox •
- PDF44: PDF24 MSI / EXE •
- :Piriform •
- CCleaner •
- Defraggler •
- Recuva •
- Speccy •
- Postgresql: PostgreSQL •
- RealNetworks: RealPlayer Cloud •
- :RealVNC •
- RealVNC Server •
- RealVNC Viewer •
- Simon Tatham: PuTTY •
- :.Sober Lemur S.a.s •
- PDFsam Basic •
- PDFsam Visual •
- Softland: FBackup •
- Skype Technologies: Skype for Windows •
- Splashtop Streamer :.Splashtop Inc •
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP •
- Sublime HQ Pty Ltd: Sublime Text •
- :TeamViewer GmbH •
- TeamViewer Host •

- TeamViewer •
- Telegram Messenger LLP: Telegram Desktop •
- :The Document Foundation •
- LibreOffice •
- LibreOffice HelpPack •
- :The Git Development Community •
- Git for Windows •
- Git LFS •
- The Pidgin developer community: Pidgin •
- The qBittorrent project: qBittorrent •
- TortoiseSVN Developers: TortoiseSVN •
- VideoLAN: VLC media player •
- :VMware •
- VMware Player •
- VMware Workstation •
- WinRAR Developers: WinRAR •
- WinZip: WinZip •
- Wireshark Foundation: Wireshark •
- Wrike: Wrike •
- Zimbra: Zimbra Desktop •
- (Zoom (MSI Distributions :Zoom Video Communications, Inc •

تثبيت تحديثات برامج الجهات الخارجية

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](#) و**بائعي 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 Windows المنتشرة 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 المدارة، قم بتشغيل مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. عند اكتمال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المكتشفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة.

يتم إنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائياً بواسطة معالج البدء السريع لخادم الإدارة. إذا لم تشغل "المعالج"، قم بإنشاء المهمة أو تشغيل معالج البدء السريع الآن.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [فحص التطبيقات بحثاً عن الثغرات الأمنية](#)، وجدولة مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة

- Kaspersky Security Center 14 Web Console: [إنشاء بحث عن الثغرات الأمنية والتحديثات المطلوبة المهمة](#)، و**البحث عن الثغرات الأمنية وإعدادات مهمة التحديثات المطلوبة**

2 تحليل قائمة التحديثات التي تم العثور عليها

اعرض قائمة تحديثات البرنامج وحدد التحديثات التي ترغب في تثبيتها. لعرض معلومات تفصيلية حول كل تحديث، انقر على اسم التحديث في القائمة لكل تحديث في القائمة، يمكنك أيضاً عرض إحصاءات حول تثبيت التحديث على أجهزة العميل.

تعليمات للمساعدة:

- وحدة تحكم الإدارة: [عرض معلومات حول التحديثات المتوفرة](#)

- Kaspersky Security Center 14 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. يمكنك إنشاء إحدى المهام التالية. يمكنك إنشاء هذه المهام في تبويب المهام أو باستخدام قائمة تحديثات البرنامج.

تستخدم مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية في تثبيت التحديثات لتطبيقات Microsoft، بما في ذلك التحديثات التي توفرها خدمة Windows Update وتحديثات منتجات 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 ترخيصاً، ولكن يمكن استخدامها لتثبيت تحديثات Windows Update فقط.

لتنصيب بعض تحديثات البرامج، يجب أن توافق على اتفاقية ترخيص المستخدم النهائي لبرنامج التنصيب. 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 بحث عن الثغرات الأمنية والتحديثات المطلوبة.

تعليمات للمساعدة:

• وحدة تحكم الإدارة: [إصلاح الثغرات الأمنية في التطبيقات](#)، [عرض معلومات حول التحديثات المتوفرة](#)

• Kaspersky Security Center 14 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 جدول المهام

للتأكد من أن قائمة التحديث مُحدّثة دائماً، قم بجدولة مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة لتشغيل المهمة تلقائياً من وقتٍ لآخر. التكرار الافتراضي هو مرة واحدة في الأسبوع.

إذا كنت قد أنشأت مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك جدولتها لتعمل بالتكرار نفسه الذي تعمل به مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة 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 بحث عن الثغرات الأمنية والتحديثات المطلوبة.

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 اعتماداً على حالة التحديث: غير محدد أو مقبول أو مرفوض. قد ترغب على سبيل المثال في إنشاء خمسة محددة للخوادم ووضع قاعدة لهذه المهمة من أجل السماح بتثبيت تحديثات Windows Update فقط والتحديثات التي بحالة مقبول. بعدها أنت تقوم يدوياً 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 تنفي 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 تحديثات البرنامج (العمليات ← إدارة التصحيحات ← تحديثات البرنامج).

تعليمات للمساعدة:

• وحدة تحكم الإدارة: [الموافقة على تحديثات البرامج ورفضها](#)

• Kaspersky Security Center 14 Web Console: [الموافقة على تحديثات برامج الأطراف الخارجية ورفضها](#)

6 تكوين خادم الإدارة للعمل كخادم (WSUS Windows Server Update Services) (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 14 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.

عرض 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 14 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.

حول 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 الصناعات الأخرى للبرامج من خلال تثبيت التحديثات المطلوبة.

Kaspersky Security Center يبحث عن التحديثات من خلال مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. عند اكتمال هذه المهمة، يتلقى خادم الإدارة قوائم بالثغرات الأمنية المكتشفة 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 لفحص الملفات بشكل تلقائي، كما تتضمن فحصًا مضادًا للفيروسات، 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، بجانب عدم إجراء أنواع أخرى من تحليل التحديثات بخلاف ما هو محدد 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 منتجات 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 إلتاك 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 Update (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.

تثبيت تحديثات برامج الجهات الخارجية

يمكنك تثبيت تحديثات برامج الجهات الخارجية على الأجهزة المُدارة عن طريق إنشاء إحدى المهام التالية وتشغيلها:

• [تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية](#)

لا يمكن إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية إلا إذا كان لديك ترخيص لميزة إدارة الثغرات الأمنية والتصحيحات. يمكنك استخدام هذه المهمة في تثبيت كل من تحديثات Windows Update التي توفرها Microsoft وتحديثات منتجات البائعين الآخرين.

• [تثبيت تحديثات Windows Update](#)

يمكنك استخدام مهمة تثبيت تحديثات Windows Update 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.
- وكنيجة 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، انتقل إلى **العمليات** ← **إدارة التصحيحات** ← **تحديثات البرنامج**.
 - لفتح قائمة التحديث لجهاز مُدار، انتقل إلى **الأجهزة** ← **الأجهزة المُدارة** ← **اسم الجهاز** ← **خيارات متقدمة** ← **التحديثات المتوفرة**.
 - لفتح قائمة التحديث لتطبيق محدد، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **سجل التطبيقات** ← **اسم التطبيق** ← **التحديثات المتوفرة**.
- ستظهر قائمة بالتحديثات المتاحة.

2. حدد خانة الاختيار الموجودة بجوار التحديثات التي ترغب في تثبيتها.

3. انقر على زر **تثبيت تحديثات**.

لتنصيب 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:

• مهمة جديدة

سيبدأ **إضافة معالج المهمة** إذا كان لديك **ترخيص إدارة الثغرات الأمنية والتصحيحات**، يتم تحديد مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية مسبقاً. إذا لم يكن لديك الترخيص، يتم تحديد مهمة تثبيت تحديثات Windows Update مسبقاً. اتبع خطوات المعالج لإكمال إنشاء المهمة.

• تثبيت تحديث (إضافة قاعدة لمهمة محددة)

حدد مهمة ترغب في إضافة التحديثات المحددة إليها. إذا كان لديك **ترخيص إدارة الثغرات الأمنية والتصحيحات**، حدد مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. سيتم تلقائياً إضافة قاعدة جديدة لتنصيب التحديثات المحددة إلى المهمة المحددة. إذا لم يكن لديك الترخيص، حدد مهمة تثبيت تحديثات Windows Update. سيتم إضافة التحديثات إلى خصائص المهمة. ستفتح نافذة خصائص المهمة. انقر على زر **حفظ** لحفظ التغييرات.

إذا اخترت إنشاء مهمة، سيتم إنشاء المهمة وعرضها في قائمة المهام في **الأجهزة** ← **المهام**. إذا اخترت إضافة التحديثات إلى مهمة موجودة، يتم حفظ التحديثات في خصائص المهمة.

لتنصيب تحديثات برامج الجهات الخارجية، ابدأ مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو مهمة تثبيت تحديثات Windows Update. يمكنك بدأ أي من هذه المهام **يدوياً** أو تحديد إعدادات الجدول في خصائص المهمة التي تبدأها. عند تحديد جدول المهام، تأكد من بدء مهمة تثبيت التحديث بعد اكتمال مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة.

تثبيت تحديثات برامج الجهات الخارجية باستخدام معالج تثبيت التحديث.

لا تتوفر مزايا معالج تثبيت التحديث إلا بموجب **ترخيص إدارة الثغرات الأمنية والتصحيحات**.

لتنصيب مهمة لتنصيب تحديثات برامج الجهات الخارجية باستخدام معالج تثبيت التحديث:

1. حدد **العمليات** ← **إدارة التصحيحات**، ومن القائمة المنسدلة حدد **تحديثات البرنامج**.
ستظهر قائمة بالتحديثات المتاحة.

2. حدد خانة الاختيار الموجودة بجوار التحديث الذي ترغب في تثبيته.

3. انقر على زر **تشغيل معالج تثبيت التحديث**.

يبدأ تشغيل معالج تثبيت التحديث. صفحة **تحديد مهمة تثبيت التحديث** تعرض قائمة بجميع المهام الموجودة من الأنواع التالية:

- تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية

• تثبيت تحديثات Windows Update

• إصلاح الثغرات الأمنية

لا يمكنك تعديل المهام لآخر نوعين لتثبيت التحديثات الجديدة. لتثبيت التحديثات الجديدة، لا يمكنك استخدام إلا مهام تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.

4. إذا كنت ترغب في ألا يعرض المعالج إلا المهام التي تثبت التحديث الذي حددته، قم بتفعيل خيار عرض المهام التي تقوم بتثبيت هذا التحديث فقط.

5. اختر ما ترغب في فعله:

• لبدء مهمة، حدد خانة الاختيار الموجودة بجوار اسم المهمة ثم انقر على زر بدء.

• لإضافة قاعدة جديدة إلى مهمة موجودة:

a. حدد خانة الاختيار الموجودة بجوار اسم المهمة ثم انقر على زر إضافة قاعدة.

b. قم بتكوين القاعدة الجديدة في الصفحة التي تفتح:

• مهمة تثبيت التحديثات ذات مستوى الأهمية هذا

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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 مساوياً 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 افتراضياً.

• مهمة تثبيت التحديثات ذات مستوى الأهمية هذا وفقاً لـ MSRC

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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) مساوياً 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 افتراضياً.

• قاعدة التثبيت للتحديثات من جانب هذا البائع

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 افتراضياً.

• قاعدة تثبيت تحديثات النوع

• قاعدة تثبيت التحديث المحدد

• الموافقة على التحديثات المحددة 9

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 افتراضياً.

• تثبيت كل تحديثات التطبيق السابقة المطلوبة لتثبيت التحديثات المحددة تلقائياً 9

استمر في تمكين هذا الخيار إذا كنت توافق على تثبيت إصدارات التطبيق مؤقتاً 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 تدريجياً. 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 افتراضياً.

c. انقر على زر إضافة.

• لإنشاء مهمة:

a. انقر على زر مهمة جديدة.

b. قم بتكوين القاعدة الجديدة في الصفحة التي تفتح:

• مهمة تثبيت التحديثات ذات مستوى الأهمية هذا 9

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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 مساوياً 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 افتراضياً.

• مهمة تثبيت التحديثات ذات مستوى الأهمية هذا وفقاً لـ MSRC 9

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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) مساوياً 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 افتراضياً.

• قاعدة التثبيت للتحديثات من جانب هذا البائع 9

هذا الخيار متاح فقط لتحديثات تطبيقات الطرف الثالث. لا يقوم Kaspersky Security Center إلا بتنصيب التحديثات التي تتعلق فقط بالتطبيقات التي قام بها نفس البائع مثل التحديث المحدد. لا يتم تنصيب التحديثات المرفوضة وتحديثات التطبيقات التي أجراها بائعون آخرون.
يتم تعطيل هذا الخيار افتراضياً.

- قاعدة تثبيت تحديثات النوع

- قاعدة تثبيت التحديث المحدد

- [الموافقة على التحديثات المحددة](#)

سيتم اعتماد التحديث المحدد للتثبيت. تمكن هذا الخيار في حالة سماح بعض القواعد المطبقة الخاصة بتنصيب التحديث بتثبيت تحديثات مصدق عليها فقط.

يتم تعطيل هذا الخيار افتراضياً.

- [تثبيت كل تحديثات التطبيق السابقة المطلوبة لتثبيت التحديثات المحددة تلقائياً](#)

استمر في تمكين هذا الخيار إذا كنت توافق على تثبيت إصدارات التطبيق مؤقتاً عندما يُطلب ذلك لتنصيب 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 تدريجياً. إذا لم يكن من الممكن تثبيت التحديثات المحددة دون تثبيت إصدارات سابقة من التطبيقات، سيفشل 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 بتنصيب الإصدار رقم 4، ومن ثم تثبيت الإصدار رقم 5. إذا تم تعطيل هذا الخيار، فإن البرنامج يفشل في تحديث التطبيق.
يتم تمكين هذا الخيار افتراضياً.

c. انقر على زر إضافة.

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 **حفظ** لحفظ التغييرات.

إذا اخترت إنشاء مهمة، **ستستمر في إنشاء المهمة** في إضافة معالج المهمة. المهمة الجديدة التي أضفتها إلى معالج تثبيت التحديث سيتم عرضها في إضافة معالج المهمة. عندما تكمل المعالج، سيتم إضافة مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية إلى قائمة المهمة.

إنشاء مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة

خلال مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المكتشفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة المُدارة.

يتم إنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائياً عند تشغيل **معالج البدء السريع**. إذا لم تشغّل المعالج، يمكنك إنشاء المهمة يدوياً.

لإنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة:

1. في نافذة التطبيق الرئيسية، اذهب إلى **الأجهزة** ← **المهام**.

2. انقر فوق إضافة.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر التالي.

3. لتطبيق Kaspersky Security Center، حدد نوع المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة.

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 فتح تفاصيل المهمة عند اكتمال الإنشاء في صفحة إنهاء عملية إنشاء المهمة. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

7. انقر فوق الزر إنشاء.

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 إعدادات التطبيق، حدد الإعدادات التالية:

• 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 جهة خارجية.

يتم تمكين هذا الخيار افتراضيًا.

• 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 ، فسيتم تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft لتحديث المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق.

إذا تم تعطيل هذا الخيار ، فسيستخدم وكيل تحديث Windows على جهاز مُدار يستخدم المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها من مصدر تحديثات Microsoft في وقت سابق والمُخزَّنة في الذاكرة المؤقتة للجهاز.

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:

• لا يتصل وكيل تحديث Windows على جهاز مُدار بخادم التحديث للحصول على التحديثات إلا في حالة تمكين الخيار الاتصال بخادم التحديث لتحديث البيانات وتحديد الخيار نشط، في مجموعة الإعدادات وضع بحث تحديث Windows.

• يستخدم وكيل تحديث Windows على جهاز مُدار المعلومات المتعلقة بتحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها مسبقًا من مصدر تحديثات Microsoft وتم تخزينها في الذاكرة المؤقتة للجهاز، في حالة تمكين خيار الاتصال بخادم التحديث للبيانات وتحديد خيار سلبي، في مجموعة إعدادات وضع بحث تحديث Windows، أو في حالة تعطيل خيار الاتصال بخادم التحديث لتحديث البيانات وتحديد خيار نشط في مجموعة إعدادات وضع بحث تحديث Windows.

• بغض النظر عن حالة الخيار الاتصال بخادم التحديث لتحديث البيانات (ممكّن أو معطل)، إذا تم تحديد الخيار معطل، في مجموعة الإعدادات وضع بحث تحديث Windows، لا يطلب Kaspersky Security Center أي معلومات حول 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 و Microsoft) 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 عن التطبيقات عبر نظام الملف

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 بشكل افتراضي على مجلدات النظام التي يتم تثبيت معظم التطبيقات بها.

• تمكين التشخيصات المتقدمة

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع حتى وإن كان التتبع معطلًا لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الآخر؛ 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 %Temp%\WINDIR. 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 5

القيمة الافتراضية هي 100 ميجابايت، وتكون 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 **حفظ**.

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 بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائيًا عند تشغيل معالج البدء السريع. إذا لم تشغل المعالج، يمكنك إنشاء المهمة يدويًا.

بالإضافة إلى [إعدادات المهمة العامة](#)، يمكنك تحديد الإعدادات التالية عند إنشاء مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة أو بعد ذلك عند تكوين خصائص المهمة التي تم إنشاؤها:

• تم إدراج البحث عن الثغرات الأمنية والتحديثات بواسطة Microsoft 5

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.

• الاتصال بخادم التحديث لتحديث البيانات 5

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، فسيتم وصل وكيل تحديث Windows على جهاز مُدار بمصدر تحديثات Microsoft لتحديث المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق.

إذا تم تعطيل هذا الخيار، فسيستخدم وكيل تحديث Windows على جهاز مُدار يستخدم المعلومات حول تحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها من مصدر تحديثات Microsoft في وقت سابق والمُخزّنة في الذاكرة المؤقتة للجهاز.

يمكن أن يكون الاتصال بمصدر تحديثات Microsoft مستهلكاً 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 عشوائياً في غضون 360 دقيقة. يتم تمكين هذا الخيار افتراضياً.

يحدد مزيج الخيارات التالية لإعدادات سياسة وكلاء الشبكة طريقة الحصول على التحديثات:

• لا يتصل وكيل تحديث Windows على جهاز مُدار بخادم التحديث للحصول على التحديثات إلا في حالة تمكين الخيار **الاتصال بخادم التحديث لتحديث البيانات** وتحديد الخيار **نشط**، في مجموعة الإعدادات **وضع بحث تحديث Windows**.

• يستخدم وكيل تحديث Windows على جهاز مُدار المعلومات المتعلقة بتحديثات Microsoft Windows القابلة للتطبيق التي تم تلقيها مسبقاً من مصدر تحديثات Microsoft وتم تخزينها في الذاكرة المؤقتة للجهاز، في حالة تمكين خيار **الاتصال بخادم التحديث لتحديث البيانات** وتحديد خيار **سليبي**، في مجموعة إعدادات **وضع بحث تحديث Windows**، أو في حالة تعطيل خيار **الاتصال بخادم التحديث لتحديث البيانات** وتحديد خيار **نشط** في مجموعة إعدادات **وضع بحث تحديث Windows**.

• بغض النظر عن حالة الخيار **الاتصال بخادم التحديث لتحديث البيانات** (ممكّن أو معطل)، إذا تم تحديد الخيار **معطل**، في مجموعة الإعدادات **وضع بحث تحديث Windows**، لا يطلب Kaspersky Security Center أي معلومات حول 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 افتراضياً.

• [تحديد مسارات للبحث المتقدم عن التطبيقات عبر نظام الملف](#)

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 بشكل افتراضي على مجلدات النظام التي يتم تثبيت معظم التطبيقات بها.

• [تمكين التشخيصات المتقدمة](#)

إذا تم تمكين هذه الميزة، فسيقوم عميل الشبكة بكتابة عمليات التتبع حتى وإن كان التتبع معطلًا لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الآخر؛ 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 %Temp%\WINDIR. 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** [3]

القيمة الافتراضية هي 100 ميجابايت، وتكون 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 بحث عن الثغرات الأمنية والتحديثات المطلوبة، تأكد من تفعيل خيار **تشغيل المهام الفائتة** واستخدم **التأخير العشوائي لبدء المهام تلقائيًا**.

بشكل افتراضي، يتم تعيين مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة للبدء في تمام الساعة 6:00 مساءً. إذا كانت قواعد مكان العمل في المؤسسة تذكر موعدًا لإغلاق جميع الأجهزة في هذا الوقت، ستعمل مهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة 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 ملاءمة للمهمة بناءً على قواعد مكان العمل التي تتبناها المؤسسة.

إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية

لا تتوفر مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية إلا بموجب **ترخيص إدارة الثغرات الأمنية والتصحيحات**.

تُستخدم 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.

لتثبيت التحديثات أو إصلاح الثغرات الأمنية باستخدام مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك القيام بأي مما يلي:

- تشغيل **معالج تثبيت التحديث** أو **معالج إصلاح الثغرات الأمنية**.
- إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.
- **أضف قاعدة لتثبيت التحديث** إلى مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية موجودة.

لإنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

2. انقر فوق **إضافة**.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.

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:

• 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 **مجلد تحميل التحديثات**.

إذا تم تعطيل هذا الخيار، فسيتم تثبيت التحديثات على الجهاز تلقائيًا.

يتم تعطيل هذا الخيار افتراضيًا.

• مجلد تحميل التحديثات

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 عمليات التتبع حتى وإن كان التتبع معطلًا لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الآخر؛ 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 ⑤

القيمة الافتراضية هي 100 ميجابايت، وتكون 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:

• لا تقم بإعادة تشغيل الجهاز ⑤

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.

• إعادة تشغيل الجهاز ⑤

يتم إعادة تشغيل الأجهزة العملية 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 ⑤

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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضيًا.

• تكرار المطالبة كل (بالدقائق) ⑤

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) ⑤

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) 9

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 **فتح تفاصيل المهمة عند اكتمال الإنشاء** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

9. انقر على زر **إنهاء**.

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 **حفظ**.

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 تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، 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 Microsoft وKaspersky) 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 تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية جديدة**.
- عن طريق إضافة قاعدة في تبويب **إعدادات التطبيق** في نافذة الخصائص للمهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية الموجودة.
- من خلال **معالج تثبيت التحديث** أو **معالج إصلاح الثغرات الأمنية**.

لإضافة قاعدة جديدة لجميع التحديثات:

1. انقر على زر **إضافة**.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج باستخدام 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 سلبًا 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 الصفحة 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 المعنية 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** ⑤

إصلاح جميع الثغرات الأمنية التي تتوافق مع المعايير المحددة في الصفحة معايير عامة الخاصة بالمعالج. يتم تحديده بصورة افتراضية.

• **إصلاح الثغرات الأمنية من القائمة فقط** ⑤

قم بإصلاح الثغرات الأمنية التي تحدها 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 إضافة المهمة أو في خصائص المهمة.

لإضافة قاعدة جديدة إلى تحديثات Windows Update:

1. انقر على زر إضافة.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج باستخدام زر التالي.

2. في صفحة نوع القاعدة، حدد قاعدة تحديث Windows.

3. في صفحة المعايير العامة، حدد الإعدادات التالية:

• **مجموعة التحديثات المراد تثبيتها** ⑤

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** ⑤

قد تؤثر تحديثات البرامج في بعض الأحيان سلبًا 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** ⑤

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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) مساوياً 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 افتراضياً.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضياً.

5. في الصفحة **فئات التحديثات**، حدد فئات التحديثات المطلوب تثبيتها. هذه الفئات هي نفس الفئات الموجودة في Microsoft Update Catalog. يتم تحديد جميع الفئات افتراضياً.

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 إضافة المهمة أو في خصائص المهمة.

لإضافة قاعدة جديدة لتحديثات تطبيقات الجهات الخارجية:

1. انقر على زر **إضافة**.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج باستخدام 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 العملية:

• **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 سلبياً 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 مساوياً 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 افتراضياً.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضياً.

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 إضافة المهمة أو في خصائص المهمة.

إنشاء مهمة تثبيت تحديثات Windows Update

تتيح لك مهمة تثبيت تحديثات Windows Update 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 تثبيت تحديثات Windows Update. لتثبيت التحديثات الجديدة، يمكنك إضافتها إلى مهمة تثبيت تحديثات Windows Update موجودة. نوصي باستخدام مهمة [تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية](#) بدلاً من مهمة تثبيت تحديثات Windows Update. يمكنك مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية من تثبيت تحديثات متعددة وإصلاح العديد من الثغرات الأمنية تلقائيًا وفقًا للقواعد التي تحددها. بالإضافة إلى ذلك، يمكنك 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 نافذة التطبيق الرئيسية، اذهب إلى [الأجهزة](#) ← [المهام](#).
2. انقر فوق [إضافة](#).
3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة [تثبيت تحديثات Windows Update](#).
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 [إضافة](#).
ستفتح قائمة التحديثات.
7. حدد تحديثات Windows Update التي ترغب في تثبيتها ثم انقر على [موافق](#).
8. حدد 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.

• [إعادة تشغيل الجهاز](#)

يتم إعادة تشغيل الأجهزة العملية 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 9

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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة لإعادة التشغيل. يتم تحديد هذا الخيار افتراضيًا.

• تكرار المطالبة كل (بالدقائق) 9

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) 9

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 9

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 المستخدم 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:

• الحساب الافتراضي 9

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه. يتم تحديد هذا الخيار افتراضيًا.

• تحديد حساب 9

املاً حقل الحساب وكلمة المرور لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

• الحساب 9

الحساب الذي يتم تشغيل المهمة من خلاله.

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

10. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **فتح تفاصيل المهمة عند اكتمال الإنشاء** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقاً في أي وقت.

11. انقر على زر **إنهاء**.

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** وفقاً لاحتياجاتك.

14. انقر على زر **حفظ**.

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:

1. حدد **العمليات** ← **إدارة التصحيحات**.

2. حدد **تحديثات البرنامج** في القائمة المنسدلة:

ستظهر قائمة بالتحديثات المتاحة.

يمكنك تحديد عامل تصفية لعرض قائمة تحديثات البرنامج. انقر على أيقونة **عامل التصفية** (☰) في أعلى يمين قائمة تحديثات البرنامج لإدارة عامل التصفية. يمكنك كذلك تحديد أحد عوامل التصفية المعدة مسبقاً من القائمة المنسدلة **عوامل تصفية محددة مسبقاً** 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:

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

• السمات

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

• الأجهزة

يعرض هذا التبويب قائمة بالأجهزة التي تم تثبيت التحديث المحدد عليها.

• الثغرات الأمنية المصلحة

يعرض هذا التبويب قائمة بالثغرات الأمنية التي يمكن للتحديث المحدد إصلاحها.

• [تقاطع التحديثات](#) 5

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).

• [المهام التي تستهدف تثبيت هذا التحديث](#) 5

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 إحصائيات حالات تثبيت التحديث.

يتم عرض مخطط حالات تثبيت التحديث. انقر 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. حدد الأجهزة ← الأجهزة المُدارة.

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 خيارات متقدمة.

4. في الجزء الأيسر، حدد قسم التحديثات المتوفرة. إذا كنت ترغب في عرض التحديثات المثبتة فقط، قم بتفعيل خيار عرض التحديثات المثبتة.

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 تبويب العمليات في القائمة المنسدلة إدارة التصحيحات، حدد تحديثات البرنامج.

لعرض الصفحة قائمة بالتحديثات المتوفرة لبرامج الجهات الخارجية المثبتة على جميع الأجهزة المُدارة.

2. انقر على زر تصدير الصفوف إلى ملف TXT أو تصدير الصفوف إلى ملف 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 **عرض التحديثات المثبتة**.

3. انقر على زر **تصدير الصفوف إلى ملف TXT** أو **تصدير الصفوف إلى ملف 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

عما تقوم بتكوين مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، 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 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 القائمة الرئيسية، انتقل إلى **العمليات** ← **إدارة التصحيحات**، ومن القائمة المنسدلة حدد **تحديثات البرنامج**.

ستظهر قائمة بالتحديثات المتاحة.

2. حدد التحديثات التي ترغب في الموافقة عليها أو رفضها.

3. انقر على **الموافقة للموافقة على التحديثات المحددة أو رفض 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 **العمليات** ← **إدارة التصحيحات**، ومن ثم حدد **تحديثات البرنامج** من القائمة المنسدلة.

ستظهر قائمة بالتحديثات المتاحة.

2. انقر على اسم التحديث التي ترغب في الموافقة عليه أو رفضه.

سنفتح نافذة خصائص التحديث.

3. في قسم عام، حدد حالة للتحديث بتغيير خيار **حالة اعتماد التحديث**. يمكنك تحديد حالة معتمد أو تم رفضه أو غير معرف

4. انقر على زر **حفظ** 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 تثبت 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 فقط 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\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.

لإنشاء مهمة إجراء مزامنة Windows Update:

1. في نافذة التطبيق الرئيسية، اذهب إلى **الأجهزة** ← **المهام**.

2. انقر فوق **إضافة**.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة إجراء مزامنة **Windows Update**.

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 **تنزيل ملفات التثبيت السريع** 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 **تنزيل ملفات التثبيت السريع**.

6. حدد التطبيق الذي ترغب في تنزيل التحديثات له.

إذا تم تحديد خانة الاختيار **جميع التطبيقات**، 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 **كافة الفئات**، فسيتم تنزيل تحديثات لجميع فئات التحديثات الموجودة، ولجميع الفئات التي قد تظهر في المستقبل.

8. حدد لغات الترجمة للتحديثات التي ترغب في تنزيلها إلى خادم الإدارة. حدد أحد الخيارات التالية:

• **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.

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 حقل **الحساب وكلمة 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 **فتح تفاصيل المهمة عند اكتمال الإنشاء** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقًا في أي وقت.

11. انقر على زر **إنهاء**.

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 **حفظ**.

سيتم إنشاء المهمة وتكوينها.

تحديث تطبيقات الجهات الخارجية تلقائيًا

يمكن تحديث بعض تطبيقات الجهات الخارجية تلقائيًا. باع 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 التحديث، مثل تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وتثبيت تحديثات Windows Update وإصلاح الثغرات الأمنية.

لتكوين إعداد التحديث التلقائي لتطبيق جهة خارجية:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **سجل التطبيقات**.

2. انقر على اسم التطبيق الذي ترغب في تغيير إعداد التحديث التلقائي له.

لتبسيط البحث، يمكنك تصفية القائمة بعمود **حالة التحديثات التلقائية**.

ستفتح نافذة خصائص التطبيق.

3. في قسم **عام**، حدد قيمة للإعداد التالي:

حالة التحديثات التلقائية

حدد أحد الخيارات التالية:

• غير معرف

يتم تعطيل ميزة التحديث التلقائي. يقوم Kaspersky Security Center بتثبيت تحديثات تطبيقات الجهات الخارجية باستخدام المهام: تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وتثبيت تحديثات Windows Update وإصلاح الثغرات الأمنية.

• مسموح به

بعد أن يصدر البائع تحديثًا للتطبيق، يتم تثبيت ذلك التحديث على الأجهزة المُدارة تلقائيًا. لا يلزم اتخاذ أي إجراءات إضافية.

• محجوب

لا يتم تثبيت تحديثات التطبيق تلقائيًا. يقوم Kaspersky Security Center بتثبيت تحديثات تطبيقات الجهات الخارجية باستخدام المهام: تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وتثبيت تحديثات Windows Update وإصلاح الثغرات الأمنية.

4. انقر على زر **حفظ** 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 الأمنية الموجودة في البرامج المثبتة على الأجهزة المُدارة، قم بتشغيل المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة. عند اكتمال هذه المهمة، يتلقى Kaspersky Security Center قوائم بالثغرات الأمنية المكتشفة والتحديثات المطلوبة لبرامج الجهات الخارجية المثبتة على الأجهزة التي حددتها في خصائص المهمة.

تم إنشاء المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة تلقائيًا بواسطة معالج البدء السريع لـ Kaspersky Security Center. إذا لم تشغل "المعالج"، فابدأ 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 14 Web Console](#): إنشاء بحث عن الثغرات الأمنية والتحديثات المطلوبة المهمة، و**البحث عن الثغرات الأمنية وإعدادات مهمة التحديثات المطلوبة**

2 تحليل قائمة الثغرات الأمنية المكتشفة 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](#)، و**عرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة**

- [Kaspersky Security Center 14 Web Console](#): [عرض معلومات حول ثغرات البرامج](#)، و**عرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة**

3 تكوين إصلاح الثغرات الأمنية

عند اكتشاف الثغرات الأمنية بالبرامج، يمكنك إصلاح الثغرات الأمنية بالبرامج على الأجهزة المُدارة باستخدام المهمة [تنصيب التحديثات المطلوبة وإصلاح الثغرات الأمنية](#) أو المهمة [إصلاح الثغرات الأمنية](#).

تُستخدم المهمة تنصيب 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 تنصيب 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 المهمة تنصيب التحديثات المطلوبة وإصلاح الثغرات الأمنية تحديثات البرامج الموصى بها.

المهمة إصلاح الثغرات الأمنية لا تتطلب 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 تحديداً يدوياً. 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 تلقائياً، أو يمكنك إنشاء واحدة من هذه المهام يدوياً.

تعليمات للمساعدة:

• وحدة تحكم الإدارة: [تحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية، إصلاح الثغرات الأمنية في التطبيقات](#)

• [Kaspersky Security Center 14 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 جدول المهام

للتأكد من أن قائمة الثغرات الأمنية محدثة دائماً، قم بجدولة المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة لتشغيلها تلقائياً من وقت 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 غالباً. 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 14 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 14 Web Console](#): [إنشاء تقرير وعرضه](#)

8 التحقق من تكوين البحث عن الثغرات الأمنية 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

إذا أنشأت المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية وكوّنتها، 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](#).

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 المهمة بحث عن الثغرات الأمنية والتحديثات المطلوبة للعثور على الثغرات الأمنية بالبرامج.

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 تُحدّد 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 إصلاح ثغرات البرامج التي يمكنك استخدامها 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 لفحص الملفات بشكل تلقائي، كما تتضمن فحصًا مضادًا للفيروسات، 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 الموثوقة في مثل هذه التحديثات، بجانب عدم إجراء أنواع أخرى من تحليل التحديثات بخلاف ما هو محدد 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 [إصلاح الثغرات الأمنية](#) وتشغيلها أو مهمة [تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية](#).

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.
- وكنتيجه 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، انتقل إلى **العمليات** ← **إدارة التصحيحات** ← **الثغرات الأمنية بالبرنامج**.
- لفتح قائمة الثغرات الأمنية لجهاز مُدار، انتقل إلى **الأجهزة** ← **الأجهزة المُدارة** ← **اسم الجهاز** ← **خيارات متقدمة** ← **الثغرات الأمنية بالبرنامج**.
- لفتح قائمة الثغرات الأمنية لتطبيق محدد، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **سجل التطبيقات** ← **اسم التطبيق** ← **الثغرات الأمنية**.

سيتم عرض صفحة بها قائمة الثغرات الأمنية في برنامج الجهة الخارجية.

2. حدد ثغرة أمنية أو أكثر في القائمة ثم انقر على زر **إصلاح الثغرات الأمنية**.

في غياب تحديث برنامج موصى به لإصلاح إحدى الثغرات الأمنية المحددة، سيتم عرض رسالة تفيد ذلك.

إصلاح 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:

• مهمة جديدة

سيبدأ **إضافة معالج المهمة** إذا كان لديك **ترخيص إدارة الثغرات الأمنية والتصحيحات**، يتم تحديد مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية مسبقًا. إذا لم يكن لديك الترخيص، يتم تحديد مهمة إصلاح الثغرات الأمنية مسبقًا. اتبع خطوات المعالج لإكمال إنشاء المهمة.

• إصلاح الثغرات الأمنية (إضافة قاعدة لمهمة محددة)

حدد مهمة ترغب في إضافة الثغرات الأمنية المحددة إليها. إذا كان لديك **ترخيص إدارة الثغرات الأمنية والتصحيحات**، حدد مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية. سيتم تلقائيًا إضافة قاعدة جديدة لإصلاح الثغرات الأمنية المحددة إلى المهمة المحددة. إذا لم يكن لديك الترخيص، حدد مهمة إصلاح الثغرات الأمنية. سيتم إضافة الثغرات الأمنية إلى خصائص المهمة.

ستفتح نافذة خصائص المهمة. انقر على زر **حفظ** لحفظ التغييرات.

إذا اخترت إنشاء مهمة، سيتم إنشاء المهمة وعرضها في قائمة المهام في **الأجهزة** ← **المهام**. إذا اخترت إضافة الثغرات الأمنية إلى مهمة موجودة، يتم حفظ الثغرات الأمنية في خصائص المهمة.

لإصلاح الثغرات الأمنية لبرامج الجهات الخارجية، ابدأ مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية أو مهمة إصلاح الثغرات الأمنية. إذا كنت قد أنشأت مهمة إصلاح الثغرات الأمنية، 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 تبويب **العمليات**، في القائمة المنسدلة **إدارة التصحيحات**، حدد **الثغرات الأمنية بالبرنامج**. 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 **تشغيل معالج إصلاح الثغرات الأمنية**.

يبدأ معالج إصلاح الثغرات الأمنية. صفحة **تحديد مهمة إصلاح الثغرة الأمنية** تعرض قائمة بجميع المهام الموجودة من الأنواع التالية:

• تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية

• تثبيت تحديثات Windows Update

• إصلاح الثغرات الأمنية

لا يمكنك تعديل آخر نوعين من المهام لتثبيت التحديثات الجديدة. لتثبيت التحديثات الجديدة، لا يمكنك استخدام إلا مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.

4. إذا كنت ترغب في ألا يعرض المعالج إلا المهام التي تصلح الثغرة الأمنية التي حددتها، قم بتفعيل خيار **عرض المهام التي تصلح هذه الثغرة الأمنية فقط**.

5. اختر ما ترغب في فعله:

• لبدء مهمة، حدد خانة الاختيار الموجودة بجوار اسم المهمة ثم انقر على زر **بدء**.

• لإضافة قاعدة جديدة إلى مهمة موجودة:

a. حدد خانة الاختيار الموجودة بجوار اسم المهمة ثم انقر على زر إضافة قاعدة.

b. قم بتكوين القاعدة الجديدة في الصفحة التي تفتح:

• قاعدة لإصلاح الثغرات الأمنية ذات مستوى الخطورة هذا 9

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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 مساوياً 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 افتراضياً.

• 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)

• قاعدة إصلاح الثغرات الأمنية في تطبيقات البائع المحدد (غير متاح إلا للثغرات الأمنية لبرامج الجهات الخارجية)

• قاعدة إصلاح الثغرة الأمنية في جميع إصدارات التطبيق المحددة (غير متاح إلا للثغرات الأمنية لبرامج الجهات الخارجية)

• قاعدة لإصلاح الثغرات الأمنية المحددة

• الموافقة على التحديثات التي تستهدف إصلاح هذه الثغرات الأمنية 9

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 افتراضياً.

c. انقر على زر إضافة.

• لإنشاء مهمة:

a. انقر على زر مهمة جديدة.

b. قم بتكوين القاعدة الجديدة في الصفحة التي تفتح:

• قاعدة لإصلاح الثغرات الأمنية ذات مستوى الخطورة هذا 9

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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 مساوياً 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 افتراضياً.

• 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)

• قاعدة إصلاح الثغرات الأمنية في تطبيقات البائع المحدد (غير متاح إلا للثغرات الأمنية لبرامج الجهات الخارجية)

• قاعدة إصلاح الثغرة الأمنية في جميع إصدارات التطبيق المحددة (غير متاح إلا للثغرات الأمنية لبرامج الجهات الخارجية)

• قاعدة لإصلاح الثغرات الأمنية المحددة

• **الموافقة على التحديثات التي تستهدف إصلاح هذه الثغرات الأمنية** ⁵

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 افتراضياً.

C. انقر على زر إضافة.

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 **حفظ** لحفظ التغييرات.

إذا اخترت إنشاء مهمة، **ستستمر في إنشاء المهمة** في إضافة معالج المهمة. يتم عرض القاعدة الجديدة التي أضفتها في معالج إصلاح الثغرات الأمنية في معالج إضافة المهمة. عندما تكمل المعالج، سيتم إضافة مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية إلى قائمة المهام.

إنشاء مهمة إصلاح الثغرات الأمنية.

مهمة إصلاح الثغرات الأمنية 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 إصلاح الثغرات الأمنية. لإصلاح الثغرات الأمنية الجديدة، يمكنك إضافتها إلى مهمة إصلاح الثغرات الأمنية موجودة. نوصي باستخدام مهمة **تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية** بدلاً من مهمة إصلاح الثغرات الأمنية. يمكنك مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية من تثبيت تحديثات متعددة وإصلاح العديد من الثغرات الأمنية تلقائياً وفقاً للقواعد التي تحددها.

قد يكون تفاعل المستخدم مطلوباً 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 مفتوحاً حالياً.

لإنشاء مهمة إصلاح الثغرات الأمنية.

1. في نافذة التطبيق الرئيسية، اذهب إلى **الأجهزة** ← **المهام**.

2. انقر فوق **إضافة**.

يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام الزر التالي.

3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة **إصلاح الثغرات الأمنية**.

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 **إضافة**.

7. حدد الثغرات الأمنية التي ترغب في إصلاحها ثم انقر على موافق.

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 إصلاح الثغرات الأمنية.

8. حدد 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.

• **إعادة 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 ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة 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 الموقوف على إغلاق قبل إعادة تشغيل الجهاز. كنتيجة لذلك، قد يفقد المستخدم 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 المستخدمون بإغلاق كافة التطبيقات التي تعمل على الأجهزة الموقوفة يدويًا وإعادة تشغيل هذه الأجهزة. يتم تعطيل هذا الخيار افتراضيًا.

• **الحساب الافتراضي**

سيتم تشغيل المهمة بموجب نفس الحساب الذي قام التطبيق بإجراء هذه المهمة بموجبه. يتم تحديد هذا الخيار افتراضياً.

• **تحديد حساب**

املاً حقل **الحساب** وكلمة 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.

10. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار **فتح تفاصيل المهمة عند اكتمال الإنشاء** في صفحة **إنهاء عملية إنشاء المهمة**. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقاً في أي وقت.

11. انقر على زر **إنهاء**.

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** وفقاً لاحتياجاتك.

14. انقر على زر **حفظ**.

سيتم إنشاء المهمة وتكوينها.

إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية

لا تتوفر مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية إلا بموجب **ترخيص إدارة الثغرات الأمنية والتصحيحات**.

تُستخدم 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 وفقاً لقواعد معينة.

لتثبيت التحديثات أو إصلاح الثغرات الأمنية باستخدام مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، يمكنك القيام بأي مما يلي:

- تشغيل **معالج تثبيت التحديث** أو **معالج إصلاح الثغرات الأمنية**.
- إنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.
- **أضف قاعدة لتثبيت التحديث** إلى مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية موجودة.

لإنشاء مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← المهام.
2. انقر فوق إضافة.
3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع المهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية.
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:

• 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 افتراضياً.

• 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 افتراضياً.

• 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 افتراضياً.

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 مجلد تحميل التحديثات. إذا تم تعطيل هذا الخيار، فسيتم تثبيت التحديثات على الجهاز تلقائيًا. يتم تعطيل هذا الخيار افتراضياً.

• مجلد تحميل التحديثات

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 عمليات التتبع حتى وإن كان التتبع معطلًا لعميل الشبكة في أداة التشخيصات المساعدة عن بُعد من Kaspersky Security Center. يتم كتابة عمليات التتبع في ملفين الواحد تلو الآخر؛ 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 %Temp%\WINDIR%. 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، وتكون 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:

• **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.

• **إعادة تشغيل الجهاز**

يتم إعادة تشغيل الأجهزة العملية 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 والفواصل الزمنية الذي سيستم بعده فرض إعادة التشغيل (دون تأكيد المستخدم). يُعد هذا الخيار الأكثر ملاءمة لمحطات العمل حيث يجب أن يتمكن المستخدمون من تحديد الوقت الأكثر ملاءمة 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) 5

عقب مطالبة المستخدم، يقوم التطبيق بإجبار إعادة تشغيل نظام التشغيل عند انتهاء الفاصل الزمني المحدد. يتم تمكين هذا الخيار افتراضياً. التأخير الافتراضي هو 30 دقيقة. القيم المتوفرة بين 1 و1440 دقيقة.

• فترة الانتظار قبل فرض إغلاق التطبيقات في الجلسات المحجوبة (بالدقائق) 9

يتم غلق التطبيقات إجبارياً عند قفل جهاز المستخدم (تلقائياً عقب فترة زمنية محددة من عدم النشاط، أو يدوياً) 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 افتراضياً.

8. إذا كنت ترغب في تعديل إعدادات المهمة الافتراضية، قم بتفعيل خيار فتح تفاصيل المهمة عند اكتمال الإنشاء في صفحة إنهاء عملية إنشاء المهمة. إذا لم تقم بتمكين هذا الخيار، سيتم إنشاء المهمة بالإعدادات الافتراضية. يمكنك تعديل الإعدادات الافتراضية لاحقاً في أي وقت.

9. انقر على زر إنهاء.

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 وفقاً لاحتياجاتك.

12. انقر على زر حفظ.

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 لتنشيط التحديثات

هذه الميزة غير متاحة إلا بموجب ترخيص إدارة الثغرات الأمنية والتصحيحات.

عند تثبيت تحديثات برامج أو إصلاح ثغرات أمنية في برنامج باستخدام مهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية، 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 Microsoft وKaspersky) 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 تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية جديدة.

• عن طريق إضافة قاعدة في تبويب إعدادات التطبيق في نافذة الخصائص للمهمة تثبيت التحديثات المطلوبة وإصلاح الثغرات الأمنية الموجودة.

- من خلال معالج تثبيت التحديث أو معالج إصلاح الثغرات الأمنية.

لإضافة قاعدة جديدة لجميع التحديثات:

1. انقر على زر إضافة.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج باستخدام 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 سلبياً 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 مساوياً 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 افتراضياً.

4. في صفحة التحديثات، حدد التحديثات المراد تثبيتها:

• تثبيت جميع التحديثات المناسبة

تثبيت جميع تحديثات البرامج التي تتوافق مع المعايير المحددة في الصفحة معايير عامة الخاصة بالمعالج. يتم تحديده بصورة افتراضية.

• تثبيت التحديثات من القائمة فقط

قم بتثبيت تحديثات البرامج التي تحددها يدوياً 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 المعنية فقط.

• تثبيت كل تحديثات التطبيق السابقة المطلوبة لتثبيت التحديثات المحددة تلقائياً

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، فسيُفشل 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](#) ⑤

إصلاح جميع الثغرات الأمنية التي تتوافق مع المعايير المحددة في الصفحة معايير عامة الخاصة بالمعالج. يتم تحديده بصورة افتراضية.

• [إصلاح الثغرات الأمنية من القائمة فقط](#) ⑥

قم بإصلاح الثغرات الأمنية التي تحدها 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 إضافة المهمة أو في خصائص المهمة.

لإضافة قاعدة جديدة إلى تحديثات Windows Update:

1. انقر على زر إضافة.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج باستخدام زر التالي.

2. في صفحة نوع القاعدة، حدد قاعدة تحديث Windows.

3. في صفحة المعايير العامة، حدد الإعدادات التالية:

• [مجموعة التحديثات المراد تثبيتها](#) ⑤

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](#) ⑤

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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 مساوياً 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 افتراضياً.

• قم بإصلاح الثغرات الأمنية ذات مستوى الخطورة MSRC الذي يساوي أو أعلى من 9

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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) مساوياً 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 افتراضياً.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضياً.

5. في الصفحة **فئات التحديثات**، حدد فئات التحديثات المطلوب تثبيتها. هذه الفئات هي نفس الفئات الموجودة في Microsoft Update Catalog. يتم تحديد جميع الفئات افتراضياً.

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 إضافة المهمة أو في خصائص المهمة.

لإضافة قاعدة جديدة لتحديثات تطبيقات الجهات الخارجية:

1. انقر على زر **إضافة**.

يبدأ معالج إنشاء القاعدة. انتقل عبر المعالج باستخدام زر التالي.

2. في صفحة **نوع القاعدة**، حدد قاعدة تحديثات الأطراف الخارجية.

3. في صفحة **المعايير العامة**، حدد الإعدادات التالية:

• مجموعة التحديثات المراد تثبيتها 9

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 9

قد تؤثر تحديثات البرامج في بعض الأحيان سلبياً 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 مساوياً 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 افتراضياً.

4. في صفحة **التطبيقات**، حدد التطبيقات وإصدارات التطبيق التي ترغب في تثبيت التحديثات من أجلها. يتم تحديد جميع التطبيقات افتراضياً.

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 إضافة المهمة أو في خصائص المهمة.

تحديد إصلاحات المستخدم للثغرات الأمنية في برامج الجهات الخارجية

لاستخدام المهمة إصلاح الثغرات الأمنية، يجب عليك تحديد تحديثات البرامج يدوياً 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 يدوياً للتثبيت.

لتحديد إصلاحات المستخدم لثغرات أمنية في برامج الجهات الخارجية:

1. في تبويب **العمليات**، في القائمة المنسدلة **إدارة التصحيحات**، حدد **الثغرات الأمنية بالبرنامج**.

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. سنفتح نافذة خصائص الثغرة الأمنية.

3. في الجزء الأيسر، حدد قسم **إصلاحات المستخدم وإصلاحات أخرى**.

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 **العمليات** ← **المستودعات** ← **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 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 المدارة بحثاً عن الثغرات الأمنية، يمكنك عرض قائمة الثغرات الأمنية في البرامج التي تم اكتشافها على جميع الأجهزة المدارة.

لعرض قائمة الثغرات الأمنية في البرامج المكتشفة على جميع الأجهزة المدارة،

في تبويب العمليات، في القائمة المنسدلة إدارة التصحيحات، حدد الثغرات الأمنية بالبرنامج.

تعرض الصفحة قائمة الثغرات الأمنية في البرامج التي تم اكتشافها على أجهزة العميل.

يمكنك كذلك إنشاء وعرض تقرير الثغرات الأمنية.

يمكنك تحديد عامل تصفية لعرض قائمة الثغرات الأمنية في البرامج. انقر على أيقونة عامل التصفية (☰) في أعلى يمين قائمة الثغرات الأمنية في البرنامج لإدارة عامل التصفية. يمكنك كذلك تحديد أحد عوامل التصفية المعدة مسبقاً من القائمة المنسدلة عوامل تصفية محددة مسبقاً 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 المدار المحدد

يمكنك عرض معلومات حول ثغرات البرامج المكتشفة على الجهاز المدار المحدد ويعمل بنظام Windows.

لعرض قائمة الثغرات الأمنية في البرامج المكتشفة على الجهاز المدار المحدد:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← الأجهزة المدارة.

يتم عرض قائمة الأجهزة المدارة.

2. في قائمة الأجهزة المدارة، انقر على رابط اسم الجهاز الذي ترغب في عرض الثغرات الأمنية المكتشفة عليه.

يتم عرض نافذة خصائص الجهاز المحدد.

3. في نافذة الخصائص للجهاز المحدد، حدد تبويب خيارات متقدمة.

4. في الجزء الأيسر، حدد قسم الثغرات الأمنية بالبرنامج.

إذا كنت ترغب في عرض الثغرات الأمنية في البرنامج التي يمكن إصلاحها فقط، حدد خيار إظهار الثغرات الأمنية التي يمكن إصلاحها فقط.

سيتم عرض قائمة الثغرات الأمنية في البرامج المكتشفة على الجهاز المدار المحدد.

لعرض خصائص الثغرة الأمنية في البرنامج المحددة،

انقر على رابط اسم الثغرة الأمنية في البرنامج في قائمة الثغرات الأمنية في البرنامج.

عرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة

يمكنك عرض إحصائيات لكل ثغرة أمنية في البرامج على الأجهزة المُدارة. تُمثل الإحصاءات كمخطط. يعرض المخطط عدد الأجهزة بالحالات التالية:

- تم تجاهله على: <عدد الأجهزة>. يتم تعيين الحالة إذا عيّنت يدويًا، في خصائص الثغرة الأمنية، الخيار لتجاهل الثغرات الأمنية.
- مثبت على: <عدد الأجهزة>. يتم تعيين الحالة إذا تم إكمال مهمة إصلاح الثغرات الأمنية بنجاح.
- الإصلاح مقرر في: <عدد الأجهزة>. يتم تعيين الحالة إذا كنت قد أنشأت المهمة لإصلاح الثغرات الأمنية لكن لم يتم تنفيذ المهمة بعد.
- التصحيح المطبق على: <عدد الأجهزة>. يتم تعيين الحالة إذا حددت تحديث برنامج يدويًا لإصلاح الثغرات الأمنية لكن هذا البرنامج الذي تم تحديثه لم يحل الثغرات الأمنية.
- الإصلاح مطلوب في: <عدد الأجهزة>. يتم تعيين الحالة إذا تم إصلاح الثغرات الأمنية فقط من جانب الأجهزة المُدارة، وإذا كان مطلوبًا إصلاحها في الجزء المتبقي من الأجهزة المُدارة.

لعرض إحصاءات الثغرات الأمنية على الأجهزة المُدارة:

1. في تبويب العمليات، في القائمة المنسدلة إدارة التصحيحات، حدد الثغرات الأمنية بالبرنامج.

تعرض الصفحة قائمة بالثغرات الأمنية في التطبيقات المكتشفة على الأجهزة المُدارة.

2. حدد خانة الاختيار الموجودة بجوار الثغرة الأمنية المطلوبة.

3. انقر على زر إحصائيات الثغرات الأمنية في الأجهزة.

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 تبويب العمليات، في القائمة المنسدلة إدارة التصحيحات، حدد الثغرات الأمنية بالبرنامج.

تعرض الصفحة قائمة بالثغرات الأمنية في التطبيقات المكتشفة على الأجهزة المُدارة.

2. انقر على زر تصدير الصفوف إلى ملف TXT أو تصدير الصفوف إلى ملف 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 **تصدير الصفوف إلى ملف TXT** أو **تصدير الصفوف إلى ملف 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 الثغرة الأمنية بالبرامج مشكلة حرجة بمؤسستك.
- 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 المُدارة المحددة فقط.

لتجاهل ثغرة أمنية في البرامج على جميع الأجهزة المُدارة:

1. في تبويب **العمليات**، في القائمة المنسدلة **إدارة التصحيحات**، حدد **الثغرات الأمنية بالبرنامج**.

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.

سنتفتح نافذة خصائص الثغرة الأمنية في البرنامج.

3. في تبويب **عام**، قم بتفعيل خيار **تجاهل الثغرات الأمنية**.

4. انقر على زر **حفظ**.

سنتغلق 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 تبويب **الأجهزة**، حدد تبويب **الأجهزة المُدارة**.

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.

سنتفتح نافذة خصائص الجهاز.

3. في نافذة خصائص الجهاز، حدد تبويب **خيارات متقدمة**.

4. في الجزء الأيسر، حدد قسم **الثغرات الأمنية بالبرنامج**.

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 عام، قم بتفعيل خيار تجاهل الثغرات الأمنية.

7. انقر على زر حفظ.

ستغلق نافذة خصائص الثغرات الأمنية بالبرامج.

8. أغلق نافذة خصائص الجهاز.

يتم تجاهل الثغرات الأمنية بالبرامج على الجهاز المُحدّد.

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 استبعاد الثغرات الأمنية بالبرامج التي تم تجاهلها من قائمة الثغرات الأمنية من خلال عامل التصفية.

إدارة التطبيقات المشغلة على أجهزة العميل

يصف هذا القسم مزايا Kaspersky Security Center المتعلقة بإدارة التطبيقات التي تعمل على أجهزة العميل.

السيناريو: إدارة التطبيق

يمكنك إدارة بدء التطبيقات على أجهزة المستخدم. يمكنك السماح للتطبيقات بالعمل على الأجهزة المُدارة أو حظرها من العمل عليها. يمكن تحقيق هذه الوظيفة من خلال مكون التحكم في التطبيقات. يمكنك إدارة التطبيقات المثبتة على أجهزة Windows فقط.

المتطلبات الأساسية

- يتم نشر Kaspersky Security Center في مؤسستك.
- من ضمن الأجهزة المُدارة في مؤسستك، يوجد أجهزة تعمل بنظام Windows.
- تم إنشاء سياسة Kaspersky Endpoint Security for Windows ونشطة.

المراحل

يسير سيناريو استخدام التحكم في التطبيقات في مراحل:

1 تشكيل قائمة بالتطبيقات على أجهزة العميل وعرضها

تساعدك هذه المرحلة في معرفة التطبيقات المثبتة على الأجهزة المُدارة. يمكنك عرض قائمة التطبيقات وتحديد التطبيقات التي ترغب في السماح لها والتطبيقات التي ترغب في حظرها وفق سياسات أمان مؤسستك. يمكن أن تكون القيود متعلقة بسياسات أمان المعلومات في مؤسستك. يمكنك تخطي هذه المرحلة إذا كنت تعرف تمامًا التطبيقات المثبتة على الأجهزة المُدارة.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [عرض سجل التطبيقات](#)

○ [الحصول على قائمة بالتطبيقات المثبتة على أجهزة العميل وعرضها](#): Kaspersky Security Center 14 Web Console

2 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. يمكنك تخطي هذه المرحلة إذا كنت تعرف تمامًا الملفات التنفيذية المثبتة على الأجهزة المُدارة.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [مخزون الملفات التنفيذية](#)

○ [الحصول على قائمة الملفات التنفيذية المخزنة على أجهزة العميل وعرضها](#): Kaspersky Security Center 14 Web Console

3 إنشاء فئات التطبيقات للتطبيقات المستخدمة في مؤسستك

قم بتحليل قوائم التطبيقات والملفات التنفيذية المخزنة على الأجهزة المُدارة. أنشئ فئات التطبيقات بناءً على التحليل. من الموصى به إنشاء فئة "تطبيقات العمل" تغطي المجموعة القياسية من التطبيقات المستخدمة في مؤسستك. في حال وجود مجموعات مستخدمين مختلفة تستخدم مجموعات مختلفة من التطبيقات في أعمالهم، يمكن إنشاء فئة تطبيق منفصلة لكل مجموعة مستخدم.

يمكنك إنشاء فئات التطبيقات من ثلاثة أنواع، ويعتمد ذلك على مجموعة المعايير لإنشاء فئة تطبيق.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [إنشاء فئات التطبيق من أجل سياسات Kaspersky Endpoint Security for Windows](#)، [إنشاء فئة تطبيق مضافاً إليها المحتوى يدوياً](#)، [إنشاء فئة تطبيق مضافاً إليها المحتوى تلقائياً](#)

○ [إنشاء فئة تطبيق مضافاً إليها المحتوى يدوياً](#): Kaspersky Security Center 14 Web Console [إنشاء فئة تطبيق تتضمن ملفات تنفيذية من مجلد محدد](#)

4 تكوين التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows

تكوين مكون التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows باستخدام فئات التطبيق التي قد أنشأتها في المرحلة السابقة.

تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [تكوين إدارة بدء تشغيل التطبيق على أجهزة العميل](#)

○ [تكوين التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Windows](#): Kaspersky Security Center 14 Web Console [Windows](#).

5 تشغيل مكون التحكم في التطبيقات في وضع الاختبار

لضمان أن قواعد التحكم في التطبيقات لا تحظر التطبيقات المطلوبة لعمل المستخدم، يُنصح بتفعيل اختبار قواعد التحكم في التطبيقات وتحليل عملها بعد إنشاء قواعد جديدة. عند تفعيل الاختبار، Kaspersky Endpoint Security for Windows لن يحظر التطبيقات الممنوع أن تبدأ بقواعد التحكم في التطبيقات، لكن بدلاً من ذلك سوف يرسل إخطارات عن بدءها 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 14 Web Console: [تكوين مكون التحكم في التطبيقات في سياسة Kaspersky Endpoint Security](#) [Windows](#). اتبع هذه التعليمات وقم بتفعيل خيار [وضع الاختبار](#) في عملية التكوين.

6 تغيير إعدادات فئات التطبيق لمكون التحكم في التطبيقات

أجر تغييرات في إعدادات التحكم في التطبيقات عند الضرورة. بناءً على نتائج الاختبار، يمكنك إضافة ملفات تنفيذية متعلقة بأحداث مكون التحكم في التطبيقات إلى فئة تطبيق مضاف إليها المحتوى يدويًا. تعليمات للمساعدة:

○ وحدة تحكم الإدارة: [إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق](#)

○ Kaspersky Security Center 14 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 فئات التطبيق، يمكنك تطبيق قواعد التحكم في التطبيقات في وضع التشغيل.

تعليمات إرشادات Kaspersky Security Center 14 Web Console: [تكوين مكون التحكم في التطبيقات في سياسة Kaspersky Endpoint Security](#). 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 التطبيقات.
- قم بتكوين التحكم في التطبيقات باستخدام فئات التطبيقات.
- قد طبقت قواعد التحكم في التطبيقات في وضع التشغيل.

النتائج

عند اكتمال السيناريو، يتم التحكم في بدء تشغيل التطبيقات على الأجهزة المُدارة. لا يمكن للمستخدمين تشغيل إلا تلك التطبيقات المسموح بتشغيلها في مؤسستك ولا يمكنهم تشغيل التطبيقات المحظورة في مؤسستك.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى [التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows](#) وإلى [Kaspersky Security for Virtualization Light Agent](#).

حول التحكم في التطبيقات

مكون التحكم في التطبيقات يراقب محاولات المستخدمين لبدء التطبيقات وينظم بدء تشغيل التطبيقات باستخدام قواعد التحكم في التطبيقات.

مكون التحكم في التطبيقات متوفر لكلٍ من Kaspersky Security for و Kaspersky Endpoint Security for Windows. جميع التعليمات الواردة في هذا القسم تصف تكوين التحكم في التطبيقات لتطبيق Kaspersky Endpoint Security for Windows.

يتم تنظيم بدء تشغيل التطبيقات التي لا تطابق إعداداتها أي من قواعد التحكم في التطبيقات عبر وضع التشغيل المحدد للمكون:

- قائمة الرفض. يُستخدم هذا الوضع إذا كنت ترغب في السماح بتشغيل جميع التطبيقات باستثناء التطبيقات المحددة في قواعد الحظر. يتم تحديد هذا الوضع بصورة افتراضية.
- قائمة السماح. يُستخدم هذا الوضع إذا كنت ترغب في حظر تشغيل جميع التطبيقات باستثناء التطبيقات المحددة في قواعد السماح.

يتم تنفيذ قواعد التحكم في التطبيقات من خلال فئات التطبيقات. أنت تقوم بإنشاء فئات التطبيقات التي تضع معايير محددة. يوجد في Kaspersky Security Center ثلاثة أنواع من فئات التطبيقات:

• 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.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى [التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows](#) وإلى [Kaspersky Security for Virtualization Light Agent](#).

الحصول على قائمة بالتطبيقات المثبتة على أجهزة العميل وعرضها

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.

لعرض قائمة التطبيقات المثبتة على الأجهزة المُدارة:

في **العمليات** ← القائمة المنسدلة **تطبيقات الطرف الثالث**، حدد **سجل التطبيقات**.

تعرض الصفحة قائمة التطبيقات المثبتة على الأجهزة المُدارة.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى [التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows](#) وإلى [Kaspersky Security for Virtualization Light Agent](#).

الحصول على قائمة بالملفات التنفيذية المخزنة على أجهزة العميل وعرضها

يمكنك الحصول على قائمة بالملفات التنفيذية المخزنة على الأجهزة المُدارة. لجرد الملفات التنفيذية، يجب أن تقوم بإنشاء مهمة جرد.

هذه الميزة لجرد الملفات التنفيذية متوفرة لتطبيق Kaspersky Endpoint Security 10 for Windows والإصدارات الأحدث، وكذلك Kaspersky Security for Virtualization 4.0 Light Agent والإصدارات الأحدث.

لإنشاء مهمة مخزون للملفات التنفيذية على الأجهزة العميلة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

يتم عرض قائمة المهام.

2. انقر على زر **إضافة**.

يبدأ تشغيل **معالج إضافة مهمة**. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. في صفحة **مهمة جديدة**، من القائمة المنسدلة **التطبيق**، حدد Kaspersky Endpoint Security for Windows.

4. من القائمة المنسدلة **نوع المهمة**، حدد **المخزون**.

5. في صفحة **إنهاء عملية إنشاء المهمة**، انقر على زر **إنهاء**.

بعد انتهاء معالج المهمة الجديدة، يتم إنشاء مهمة المخزون وتكوينها. يمكنك إذا كنت ترغب أن تقوم بتغيير إعدادات المهمة التي تم إنشاؤها. يتم عرض المهمة التي تم إنشاؤها في قائمة المهام.

للاطلاع على وصف تفصيلي لمهمة الجرد، يُرجى الرجوع إلى [التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows](#) وإلى [Kaspersky Security for Virtualization Light Agent](#).

بعد إجراء مهمة المخزون، يتم تشكيل قائمة الملفات التنفيذية المخزنة على الأجهزة المُدارة، ويمكنك عرض القائمة.

أثناء الجرد، يتم اكتشاف الملفات التنفيذية بالامتدادات التالية: MSI و REG و VBS و JS و PS1 و CMD, BAT و SYS و NE و PE و COM و MZ و HTML و JAR و DLL و CPL و

لعرض قائمة الملفات التنفيذية المخزنة على أجهزة العميل:

في **العمليات** ← القائمة المنسدلة **تطبيقات الطرف الثالث**، حدد **الملفات التنفيذية**.

تعرض الصفحة قائمة الملفات التنفيذية المخزنة على أجهزة العميل.

لإرسال الملف التنفيذي للجهاز المُدار إلى Kaspersky:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **الملفات التنفيذية**.

2. انقر على رابط الملف التنفيذي الذي تريد إرساله إلى Kaspersky.

3. في النافذة التي تفتح، انتقل إلى قسم **الأجهزة** ثم حدد خانة الاختيار الخاصة بالجهاز المُدار الذي تريد إرسال الملف التنفيذي منه.

قبل إرسال الملف التنفيذي تأكد من أن الجهاز المُدار لديه اتصال مباشر بخادم الإدارة، عن طريق تحديد خانة اختيار **عدم قطع الاتصال عن خادم الإدارة**.

4. انقر فوق الزر **إرسال إلى Kaspersky**.

يتم تنزيل الملف التنفيذي المحدد لإرساله مرة أخرى إلى Kaspersky.

إنشاء فئة تطبيق مضافاً إليها المحتوى يدوياً

يمكنك تحديد مجموعة من المعايير كقالب للملفات التنفيذية التي ترغب في السماح ببدونها 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 مضافاً إليها المحتوى يدوياً:

1. في **العمليات** ← القائمة المنسدلة **تطبيقات الطرف الثالث**، حدد **فئات التطبيق**.

يتم عرض صفحة بقائمة فئات التطبيقات.

2. انقر على زر **إضافة**.

يبدأ تشغيل فئة المعالج الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. في صفحة تحديد طريقة إنشاء الفئة من المعالج، حدد خيار فئة ذات محتوى مضاف يدوياً. تتم إضافة بيانات الملفات التنفيذية يدوياً إلى الفئة.

4. في صفحة الشروط في المعالج، انقر على زر **إضافة** من أجل إضافة معيار شرط لإدراج الملفات في فئة الإنشاء.

• **من فئة KL** 

إذا تم تحديد هذا الخيار، يمكنك تحديد فئة تطبيق Kaspersky كشرط لإضافة تطبيقات إلى فئة المستخدم. ستنتم إضافة التطبيقات من فئة Kaspersky المحددة إلى فئة تطبيقات المستخدم.

• **تحديد شهادة من المستودع** 

إذا تم تحديد هذا الخيار، فيمكنك تحديد الشهادات من وحدة التخزين. ستنتم إضافة الملفات التنفيذية التي تم توقيعها وفقًا للشهادات المحددة إلى فئة المستخدم.

• **تحديد المسار إلى تطبيق (بدعم الأفتعة)** 

إذا تم تحديد هذا الخيار، فيمكنك تحديد المسار المؤدي إلى المجلد الموجود على الجهاز العميل الذي يحتوي على الملفات التنفيذية المراد إضافتها إلى فئة تطبيقات المستخدم.

• **محرك الأقراص القابل للإزالة** 

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.

• **تجزئة أو بيانات تعريفية أو شهادة:**

• **تحديد من قائمة الملفات التنفيذية** 

إذا تم تحديد هذا الخيار، فيمكنك استخدام قائمة الملفات التنفيذية على الجهاز العميل لتحديد التطبيقات وإضافتها إلى الفئة.

• **تحديد من سجل التطبيقات** 

في حال تحديد هذا الخيار، يتم عرض سجل التطبيقات. يمكنك تحديد تطبيق من السجل وتحديد بيانات تعريف الملف التالية:

- 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.

• **التحديد اليدوي** 

إذا تم تحديد هذا الخيار ، يجب عليك تحديد تجزئة الملف أو بيانات تعريفه أو شهادته كشرط لإضافة تطبيقات إلى فئة المستخدم.

تجزئة الملف

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 حفظ المعلومات حول قيم التجزئة المحسوبة في قاعدة بيانات خادم الإدارة. لا يؤدي تخزين قيم التجزئة إلى زيادة حجم قاعدة البيانات بقدر كبير.

SHA-256 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 SHA-256. 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 إصدارات Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو إصدارات أحدث، فحدد خانة الاختيار حساب SHA-256 للملفات في هذه الفئة (مدعوم بواسطة Kaspersky Endpoint Security 10 Service Pack 2 for Windows وأي إصدارات أحدث). لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA-256 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 for Windows في شبكتك، فحدد حساب MD5 للملفات في هذه الفئة (مدعوم بواسطة إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows). 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 SHA-256 لملفات الفئة.
- في حالة استخدام الأجهزة المختلفة في شبكتك لكل من الإصدارات الأقدم والأحدث من Kaspersky Endpoint Security 10، فقم بتحديد خانة الاختيار حساب SHA-256 للملفات في هذه الفئة وخانة الاختيار حساب MD5 للملفات في هذه الفئة.

بيانات وصفية

في حال تحديد هذا الخيار ، يمكنك تحديد بيانات تعريف الملف مثل اسم الملف وإصدار الملف والبائع. سيتم إرسال بيانات التعريف إلى خادم الإدارة. سيتم إضافة الملفات التنفيذية التي تحتوي على نفس بيانات التعريف إلى فئة التطبيق.

الشهادة

إذا تم تحديد هذا الخيار ، فيمكنك تحديد الشهادات من وحدة التخزين. سيتم إضافة الملفات التنفيذية التي تم توقيعها وفقًا للشهادات المحددة إلى فئة المستخدم.

• من ملف أو من حزمة MSI / مجلد مؤرشف

إذا تم تحديد هذا الخيار ، يمكنك تحديد ملف مثبت MSI كشرط لإضافة تطبيقات إلى فئة المستخدم. سيتم إرسال البيانات الوصفية لمثبت 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 صفحة الاستثناءات في المعالج، انقر على زر إضافة من أجل إضافة معيار شرط حصري لاستثناء الملفات من الفئة التي تم إنشاؤها.

7. في صفحة معيار الشرط، 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.

إنشاء فئة تطبيق تتضمن ملفات تنفيذية من أجهزة محددة

يمكنك استخدام الملفات التنفيذية من الأجهزة المحددة كقالب 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.

لإنشاء فئة تطبيق تتضمن ملفات تنفيذية من أجهزة محددة:

1. في **العمليات** ← القائمة المنسدلة **تطبيقات الطرف الثالث**، حدد **فئات التطبيق**.
يتم عرض صفحة بقائمة فئات التطبيقات.
2. انقر على زر **إضافة**.
يبدأ تشغيل فئة المعالج الجديدة. انتقل عبر المعالج باستخدام زر التالي.
3. في صفحة **تحديد طريقة إنشاء الفئة**، حدد اسم الفئة وحدد خيار **فئة تتضمن ملفات تنفيذية من الأجهزة المحددة**. تتم معالجة هذه الملفات التنفيذية تلقائيًا ويتم إضافة مقاييسها إلى الفئة.
4. انقر فوق **إضافة**.
5. في النافذة التي تفتح، حدد جهازًا أو أجهزة سيتم استخدام ملفاتها التنفيذية في إنشاء فئة التطبيق.
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 حفظ المعلومات حول قيم التجزئة المحتسبة في قاعدة بيانات خادم الإدارة. لا يؤدي تخزين قيم التجزئة إلى زيادة حجم قاعدة البيانات بقدر كبير.

SHA-256 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 الإصدارات الأحدث لحساب SHA-256. 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 إصدارات Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو إصدارات أحدث، فحدد خانة الاختيار **حساب SHA-256 للملفات في هذه الفئة (مدعوم بواسطة Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** (إصدارات أحدث). لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA-256 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 للملفات الفئة.
 - إذا تم تثبيت أي إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows في شبكتك، فحدد **حساب MD5 للملفات في هذه الفئة (مدعوم بواسطة إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**. 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 SHA-256 للملفات الفئة.
- في حالة استخدام الأجهزة المختلفة في شبكتك لكل من الإصدارات الأقدم والأحدث من Kaspersky Endpoint Security 10، فقم بتحديد خانة الاختيار **حساب SHA-256 للملفات في هذه الفئة** وخانة الاختيار **حساب MD5 للملفات في هذه الفئة**.
- يتم تحديد خانة الاختيار **حساب SHA-256 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.

• [مزمنة البيانات مع مستودع خادم الإدارة](#)

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.

• [نوع الملف](#)

يمكنك في هذا القسم تحديد نوع الملف المستخدم في إنشاء فئة التطبيق.

كل الملفات. يتم أخذ جميع الملفات في الاعتبار عند إنشاء الفئة. يتم تحديد هذا الخيار افتراضيًا.

الملفات الموجودة فقط خارج فئات التطبيق. لا يتم الأخذ في الاعتبار عند إنشاء الفئة إلا الملفات خارج فئات التطبيقات.

• [المجلدات](#)

يمكنك في هذا القسم تحديد المجلدات من الجهاز المحدد (الأجهزة المحددة) التي تحتوي على ملفات مستخدمة لإنشاء فئة التطبيق.

كل المجلدات. يتم أخذ جميع المجلدات في الاعتبار لإنشاء الفئة. يتم تحديد هذا الخيار افتراضيًا.

المجلد المحدد. لا يتم الأخذ في الاعتبار لإنشاء الفئة إلا المجلد المحدد. في حالة تحديدها لهذا الخيار، يجب أن تحدد المسار الخاص بالمجلد.

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.

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 المجلد المحدد:

1. في العمليات ← القائمة المنسدلة تطبيقات الطرف الثالث، حدد فئات التطبيق.
يتم عرض صفحة بقائمة فئات التطبيقات.
2. انقر على زر إضافة.
يبدأ تشغيل فئة المعالج الجديدة. انتقل عبر المعالج باستخدام زر التالي.
3. في صفحة تحديد طريقة إنشاء الفئة، حدد اسم الفئة وحدد خيار فئة تحتوي على ملفات تنفيذية من مجلد محدد. تتم معالجة الملفات التنفيذية الخاصة بالتطبيقات والتي تم نسخها إلى المجلد المحدد تلقائيًا، ويتم إضافة مقاييسها إلى الفئة.
4. حدد المجلد الذي سيتم استخدام الملفات التنفيذية الموجودة فيه لإنشاء فئة التطبيق.
5. حدد الإعدادات التالية:

• تضمين مكتبات الروابط الديناميكية (DLL) في هذه الفئة

تشمل فئة التطبيق مكتبات الروابط الديناميكية (ملفات بتنسيق DLL)، ويسجل 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.

• تضمين بيانات البرنامج النصي في هذه الفئة

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 حساب SHA-256 للملفات في هذه الفئة (مدعوم بواسطة Kaspersky Endpoint Security 10 Service Pack 2 for Windows والإصدارات الأحدث) / حساب MD5 للملفات في هذه الفئة (مدعوم بواسطة إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows)

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 حفظ المعلومات حول قيم التجزئة المحسوبة في قاعدة بيانات خادم الإدارة. لا يؤدي تخزين قيم التجزئة إلى زيادة حجم قاعدة البيانات بقدر كبير.

SHA-256 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 SHA-256. 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 إصدارات Kaspersky Endpoint Security 10 Service Pack 2 for Windows أو إصدارات أحدث، فحدد خانة الاختيار حساب SHA-256 للملفات في هذه الفئة (مدعوم بواسطة Kaspersky Endpoint Security 10 Service Pack 2 for Windows وأي إصدارات أحدث). لا ننصحك بإضافة أي فئات تم إنشاؤها وفقًا لمعيار مجموع تجزئة SHA-256 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 للملفات الفئة.

- إذا تم تثبيت أي إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows في شبكتك، فحدد حساب MD5 للملفات في هذه الفئة (مدعوم بواسطة إصدارات أقدم من Kaspersky Endpoint Security 10 Service Pack 2 for Windows). 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 SHA-256 للملفات الفئة.

في حالة استخدام الأجهزة المختلفة في شبكتك لكل من الإصدارات الأقدم والأحدث من Kaspersky Endpoint Security 10، فقم بتحديد خانة الاختيار حساب SHA-256 للملفات في هذه الفئة وخانة الاختيار حساب MD5 للملفات في هذه الفئة.

يتم تحديد خانة الاختيار حساب SHA-256 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.

• فرض فحص المجلد للتغييرات

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 تحقيقات من المجلد. يحاول الخادم الوصول إلى الملفات إذا تم تعديلها أو إضافتها أو حذفها. يتم تعطيل هذا الخيار افتراضيًا.

بعد انتهاء المعالج، يتم إنشاء فئة تطبيق مخصصة. يتم عرضه في قائمة فئات التطبيق. يمكنك استخدام فئة التطبيق في تكوين التحكم في التطبيقات.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى [التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows](#) وإلى [Kaspersky Security for Virtualization Light Agent](#).

عرض قائمة فئات التطبيق

يمكنك عرض قائمة فئات التطبيقات التي تم إنشاؤها وإعدادات كل فئة تطبيق.

لعرض قائمة فئات التطبيقات،

في تبويب العمليات، في القائمة المنسدلة تطبيقات الطرف الثالث، حدد فئات التطبيق.

يتم عرض صفحة بقائمة فئات التطبيقات.

لعرض خصائص فئة تطبيق،

انقر على اسم فئة التطبيق.

يتم عرض نافذة خصائص فئة التطبيق. يتم تجميع الخصائص في عدة علامات تبويب.

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 الأجهزة ← السياسات وملفات التعريف.

سيتم عرض صفحة بقائمة السياسات.

2. انقر على سياسة Kaspersky Endpoint Security for Windows.

سنتفتح نافذة إعدادات السياسة.

3. حدد تبويب إعدادات التطبيق، قسم عناصر التحكم في الأمان، القسم الفرعي .

يتم عرض نافذة التحكم في التطبيقات بإعدادات التحكم في التطبيقات.

4. بدل زر التبديل من أجل تفعيل خيار التحكم في التطبيقات.

5. إذا كنت ترغب في اختبار قواعد التحكم في التطبيقات، بدل زر التبديل من أجل تفعيل خيار وضع الاختبار.

إذا كنت ترغب في تطبيق قواعد التحكم في التطبيقات، بدل زر التبديل من أجل تعطيل خيار وضع الاختبار.

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 الكمبيوتر بعد تحديد خيار التحكم في 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 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 حظر وضع التحكم في التطبيقات، حدد وضع قائمة الرفض أو قائمة السماح.

يتم تحديد وضع قائمة الرفض افتراضياً.

9. انقر على رابط إعدادات قوائم القواعد.

سنتفتح نافذة قوائم الرفض وقوائم السماح كي تتيح لك إضافة فئة تطبيق. يكون تبويب قائمة الرفض محدداً إذا كان وضع قائمة الرفض محدداً، ويكون تبويب قائمة السماح محدداً إذا كان وضع قائمة السماح محدداً.

10. في نافذة قوائم الرفض وقوائم السماح، انقر على زر إضافة.

يتم فتح نافذة قاعدة التحكم في التطبيقات.

11. انقر على الرابط يُرجى اختيار فئة.

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 موافق.

ستغلق نافذة فئة التطبيقات.

14. في نافذة قاعدة التحكم في التطبيقات، في قسم المواضيع وحقوقها، أنشئ قائمة المستخدمين ومجموعات المستخدمين لتطبيق قاعدة التحكم في التطبيقات.

15. انقر على زر موافق لحفظ الإعدادات ولإغلاق نافذة قاعدة التحكم في التطبيقات.

16. انقر على زر موافق لحفظ الإعدادات ولإغلاق نافذة قوائم الرفض وقوائم السماح.

17. انقر على زر موافق لحفظ الإعدادات ولإغلاق نافذة التحكم في التطبيقات.

18. انقر على زر إغلاق (X) لإغلاق النافذة التي بها إعدادات سياسة Kaspersky Endpoint Security for Windows.

يتم تكوين التحكم في التطبيقات. بعد نشر السياسة إلى أجهزة العميل، يتم إدارة بدء تشغيل الملفات التنفيذية.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى [التعليمات عبر الإنترنت من Kaspersky Endpoint Security for Windows](#) وإلى [Kaspersky Security for Virtualization Light Agent](#).

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 حظر بدء تشغيل التطبيق إلى المدير (حدث تحذيري). 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 المراقبة والإبلاغ ← تحديدات الأحداث.

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 تعيين إلى فئة.

يبدأ تشغيل فئة المعالج الجديدة. انتقل عبر المعالج من خلال استخدام الزر التالي.

4. في صفحة المعالج، حدد الإعدادات ذات الصلة:

- في الصفحة الإجراء بشأن الملف التنفيذي المتعلق بالحدث، حدد أحد الخيارات التالية:

• إضافة إلى فئة تطبيق جديدة ⑤

حدد هذا الخيار إذا كنت ترغب في إنشاء فئة تطبيق جديدة بناءً على الملفات التنفيذية ذات الصلة بالحدث.

يتم تحديد هذا الخيار افتراضياً.

إذا كنت قد حددت هذا الخيار، حدد اسم فئة جديدة.

• إضافة إلى فئة تطبيق حالي ⑤

حدد هذا الخيار إذا كنت ترغب في إضافة ملفات تنفيذية متعلقة بالحدث إلى فئة تطبيق موجودة.

لا يتم تحديد هذا الخيار افتراضياً.

إذا كنت قد حددت هذا الخيار، حدد فئة التطبيق المضاف إليها المحتوى يدوياً التي ترغب في إضافة ملفات تنفيذية إليها.

- في القسم نوع القاعدة، حدد واحداً من الخيارات التالية:

• قواعد الإضافة إلى التضمينات

• قواعد الإضافة إلى الاستثناءات

- في قسم حدد المعلمة المستخدمة كشرط، حدد أحد الخيارات التالية:

• تفاصيل الشهادة (أو تجزئات SHA-256 للملفات التي لا تحتوي على شهادة) ⑤

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 SHA-256 فريدة خاصة به. عندما تحدد وظيفة تجزئة SHA-256، 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 SHA-256 للملفات بدون شهادة).

يتم تحديد هذا الخيار افتراضياً.

• تفاصيل الشهادة (سيتم تخطي الملفات التي لا يوجد لديها شهادة) ⑤

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.

• SHA-256 فقط (سيتم تخطي الملفات التي لا تحتوي على تجزئة) ⑤

كل ملف لديه وظيفة تجزئة SHA-256 فريدة خاصة به. عندما تحديد وظيفة تجزئة SHA-256، ينتهي ملف مقابل واحد على سبيل المثال، إصدار التطبيق المحدد، إلى الفئة.
حدد هذا الخيار إذا كنت ترغب بإضافة فقط تفاصيل وظيفة تجزئة SHA-256 الخاصة بالملف التنفيذي.

• MD5 فقط (الوضع المتوقع، لإصدار Kaspersky Endpoint Security 10 Service Pack 1 فقط) 9

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 موافق.

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.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى التعليمات عبر الإنترنت من [Kaspersky Endpoint Security for Windows](#) وإلى [Kaspersky Security for Virtualization Light Agent](#).

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 **تنزيل التحديثات إلى مستودع مهمة خادم الإدارة لأول مرة**.

لإنشاء حزمة تثبيت لتطبيق جهة خارجية من قاعدة بيانات Kaspersky:

1. في Kaspersky Security Center Web Console، افتح **الاكتشاف والنشر** ← **التوزيع والتعيين** ← **حزم التثبيت**.

2. انقر على زر **إضافة**.

3. في صفحة معالج الحزمة الجديدة التي تفتح، حدد خيار **تحديد تطبيق من قاعدة بيانات Kaspersky لإنشاء حزمة تثبيت** ثم انقر على **التالي**.

4. في قائمة التطبيقات التي تفتح، حدد التطبيق ذي الصلة ثم انقر على **التالي**.

5. حدد لغة الترجمة ذات الصلة في القائمة المنسدلة ثم انقر على **التالي**.

لا يتم عرض هذه الخطوة إلا إذا كان التطبيق يعرض خيارات عدة لغات.

6. إذا طلب منك الموافقة على اتفاقية ترخيص للتثبيت، في صفحة **اتفاقية ترخيص المستخدم النهائي** التي تفتح، انقر على الرابط لقراءة اتفاقية الترخيص على الموقع الإلكتروني للبائع ثم حدد خانة الاختيار **أؤكد أنني قرأت وفهمت وأوافق على شروط وأحكام اتفاقية ترخيص المستخدم النهائي** هذه بالكامل.

7. في صفحة **اسم حزمة التثبيت الجديدة** التي تفتح، في حقل **اسم الحزمة**، أدخل اسم حزمة التثبيت ثم انقر على **التالي**.

انتظر حتى يتم رفع حزمة التثبيت التي تم إنشاؤها حديثاً إلى خادم الإدارة. عندما يعرض معالج الحزمة الجديدة الرسالة التي تخبرك بنجاح عملية إنشاء الحزمة، انقر على **إنهاء**.

تظهر حزمة التثبيت التي تم إنشاؤها حديثاً في قائمة حزم التثبيت. يمكنك تحديد هذه الحزمة عند إنشاء مهمة تثبيت التطبيق عن بُعد

عرض وتعديل إعدادات حزمة تثبيت 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 Kaspersky Security Center Web Console، افتح [الاكتشاف والنشر](#) ← [التوزيع والتعيين](#) ← [حزم التثبيت](#).
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 [حفظ](#).

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 الإجزاء من الإعدادات المدرجة بالأعلى بشكل افتراضي حتى يمكنك إضافة الأعمدة المقابلة عن طريق النقر على زر [عامل التصفية وتحديد](#) أسماء الأعمدة ذات الصلة من القائمة.

• تبويب عام:

- حقل الإدخال الذي يحتوي على اسم حزمة التثبيت الذي يمكن تحريره يدويًا

• [التطبيق](#)

اسم تطبيق الجهة الخارجية الذي تم إنشاء حزمة التثبيت له.

• [الإصدار](#)

رقم إصدار تطبيق الجهة الخارجية الذي تم إنشاء حزمة التثبيت له.

• [الحجم](#)

حجم حزمة تثبيت الجهة الخارجية (بالكيلو بايت).

• [تم الإنشاء](#)

تاريخ ووقت إنشاء حزمة تثبيت الجهة الخارجية.

• [المسار](#) ⑤

مسار مجلد الشبكة الذي يوجد فيه حزمة تثبيت الجهة الخارجية.

• [تبويب إجراء التثبيت:](#)

• [تثبيت مكونات النظام العام المطلوبة](#) ⑤

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:

• [الاسم](#) ⑤

اسم الشبكة الفرعية.

• [الوصف](#) ⑤

وصف التحديث.

• [المصدر](#) ⑤

مصدر التحديث، أي ما إذا كان قد تم إصداره بواسطة Microsoft أو بواسطة مطور آخر تابع لجهة خارجية.

• [النوع](#) ⑤

نوع التحديث، أي ما إذا كان مخصصًا لبرنامج تشغيل أو تطبيق.

• [الفئة](#) ⑤

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 وفقًا على MSRC](#) ⑤

مستوى أهمية التحديث المحدد في مركز استجابة خبراء الأمان من Microsoft (MSRC).

• [مستوى الأهمية](#) ⑤

مستوى أهمية التحديث كما تحدده Kaspersky.

• [مستوى أهمية التصحيح \(للتصحيات التي تستهدف تطبيقات Kaspersky\)](#) ⑤

مستوى أهمية التصحيح إذا كان مخصصًا لتطبيق Kaspersky.

• [مقالة](#) ⑤

معرف المقالة في "قاعدة المعارف" التي تصف التحديث.

• **نشرة** ④

معرف نشرة الأمان التي تصف التحديث.

• **غير معين للثبيت (الإصدار الجديد)** ④

يعرض ما إذا كان التحديث بحالة "غير مخصص للثبيت" أم لا.

• **يتم تثبيته** ④

يعرض ما إذا كان التحديث بحالة "للتثبيت" أم لا.

• **يجري التثبيت** ④

يعرض ما إذا كان التحديث بحالة "جاري التثبيت" أم لا.

• **تم التثبيت** ④

يعرض ما إذا كان التحديث بحالة "مثبت" أم لا.

• **فشل** ④

يعرض ما إذا كان التحديث بحالة "تعذر" أم لا.

• **إعادة التشغيل مطلوبة** ④

يعرض ما إذا كان التحديث بحالة "إعادة التشغيل مطلوبة" أم لا.

• **مُسجَّل** ④

يعرض تاريخ ووقت تسجيل التحديث.

• **مثبت في الوضع التفاعلي** ④

يعرض ما إذا كان التحديث يتطلب التفاعل مع المستخدم أثناء التثبيت.

• **تم الإلغاء** ④

يعرض التاريخ والوقت اللذين تم فيهما إبطال التحديث.

• **حالة اعتماد التحديث** ④

يعرض ما إذا قد تمت الموافقة على التحديث للثبيت أم لا.

• **المراجعة** ④

يعرض رقم المراجعة الحالي للتحديث.

• **معرف التحديث**

يعرض معرف التحديث.

• **إصدار التطبيق**

يعرض رقم الإصدار الذي سيتم تحديث التطبيق إليه.

• **تم الإبدال**

يعرض التحديثات الأخرى التي يمكن أن تحل محل التحديث.

• **الإبدال**

يعرض التحديثات الأخرى التي يمكن أن يحل محلها التحديث.

• **يجب قبول بنود اتفاقية الترخيص**

يعرض ما إذا كان التحديث يتطلب قبول شروط اتفاقية ترخيص المستخدم النهائي أم لا.

• **عنوان URL الخاص بالوصف**

يعرض اسم بائع التحديث.

• **مجموعة التطبيقات**

يعرض اسم عائلة التطبيقات التي ينتمي إليها التحديث.

• **التطبيق**

يعرض اسم التطبيق الذي ينتمي إليه التحديث.

• **لغة الترجمة**

يعرض لغة ترجمة التحديث.

• **غير معين للتثبيت (الإصدار الجديد)**

يعرض ما إذا كان التحديث بحالة "غير مخصص للتثبيت (إصدار جديد)".

• **يتطلب تثبيت المتطلبات الأساسية**

يعرض ما إذا كان التحديث بحالة "يتطلب متطلبات أساسية للتثبيت".

• **وضع التنزيل**

يعرض وضع تنزيل التحديث.

• هو تصحيح

يعرض ما إذا كان التحديث عبارة عن تصحيح أم لا.

• غير مثبت

يعرض ما إذا كان التحديث بحالة "غير مثبت" أم لا.

• علامة تبويب إعدادات تعرض إعدادات حزمة التثبيت - مع عرض أسمائها وأوصافها وقيمها - والمستخدم كمعلومات في سطر الأوامر أثناء التثبيت. إذا كانت الحزمة لا توفر تلك الإعدادات، يتم عرض الرسالة المقابلة. يمكنك تعديل قيم هذه الإعدادات.

• علامة تبويب سجل المراجعة تعرض مراجعات حزمة التثبيت وتحتوي على الأعمدة التالية:

• المراجعة

يعرض رقم مراجعة حزمة التثبيت.

• الوقت

يعرض وقت إنشاء المراجعة.

• المستخدم

يعرض اسم حساب المستخدم الذي تم إنشاء المراجعة باسمه.

• الإجراء

قوائم الإجراء أو الإجراءات المتخذة تجاه حزمة التثبيت في المراجعة.

• الوصف

يعرض الوصف النصي المضاف إلى المراجعة.

علامات التطبيقات

يصف هذا القسم علامات التطبيقات، ويوفر تعليمات حول إنشائها وتعديلها وكذلك لوضع علامات على التطبيقات الخارجية.

حول علامات التطبيقات

يتيح لك Kaspersky Security Center وضع علامة على تطبيقات الأطراف الخارجية (أي التطبيقات من صناعة شركات أخرى غير Kaspersky). 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 و Google Chrome و Mozilla Firefox وغيرها).

إنشاء علامة تطبيق

إنشاء علامة تطبيق:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **علامات التطبيق**.
2. انقر فوق **إضافة**.
ستفتح نافذة علامة جديدة.
3. أدخل اسم العلامة.
4. انقر فوق **موافق** لحفظ التغييرات.
تظهر العلامة الجديدة في قائمة علامات التطبيقات.

إعادة تسمية علامة تطبيق

لإعادة تسمية علامة تطبيق:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **علامات التطبيق**.
2. حدد خانة الاختيار الموجودة بجوار العلامة التي ترغب في إعادة تسميتها ثم انقر على **تحرير**.
ستفتح نافذة الخصائص.
3. قم بتغيير اسم العلامة.
4. انقر فوق **موافق** لحفظ التغييرات.
تظهر العلامة المحدثة في قائمة علامات التطبيقات.

تعيين علامات لتطبيق

لتخصيص علامة أو عدة علامات لتطبيق:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **سجل التطبيقات**.
2. انقر على اسم التطبيق الذي ترغب في تخصيص العلامات له.
3. حدد علامة التبويب **العلامات**.
تعرض علامة التبويب جميع علامات التطبيق الموجودة على خادم الإدارة. بالنسبة للعلامات المخصصة للتطبيق المحدد، يتم تحديد خانة الاختيار في عمود **تعيين علامة**.
4. بالنسبة للعلامات التي ترغب في تخصيصها، حدد خانة الاختيار في عمود **تعيين علامة**.

5. انقر على **حفظ** لحفظ التغييرات.

يتم تخصيص العلامات للتطبيق.

إزالة علامات معينة من تطبيق

لإزالة علامة أو عدة علامات من تطبيق:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **سجل التطبيقات**.

2. انقر على اسم التطبيق الذي ترغب في إزالة العلامات منه.

3. حدد علامة التبويب **العلامات**.

تعرض علامة التبويب جميع علامات التطبيق الموجودة على خادم الإدارة. بالنسبة للعلامات المخصصة للتطبيق المحدد، يتم تحديد خانة الاختيار في عمود **تم تعيين علامة**.

4. بالنسبة للعلامات التي ترغب في إزالتها، حدد خانة الاختيار في عمود **تم تعيين علامة**.

5. انقر على **حفظ** 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 **العمليات** ← **تطبيقات الطرف الثالث** ← **علامات التطبيق**.

2. من القائمة، حدد علامة التطبيق التي ترغب في حذفها.

3. انقر فوق الزر **حذف**.

4. في النافذة التي تفتح، انقر على **موافق**.

سيتم حذف علامة التطبيق. يتم إزالة العلامة المحذوفة بشكل تلقائي من جميع التطبيقات التي تخصها 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 لتناسب 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

تعرف 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 انتشار الفيروسات.

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 حالة الحماية

○ قم بإنشاء ومراجعة تقرير عن حالة الحماية

○ قم بإنشاء ومراجعة تقرير الأخطاء.

6 تحديد مواقع أجهزة العميل غير المحمية

تعليمات للمساعدة:

○ راجع عنصر الواجهة أجهزة جديدة.

○ قم بإنشاء ومراجعة تقرير نشر الحماية

7 التحقق من حماية أجهزة العميل

تعليمات للمساعدة:

○ إنشاء التقارير ومراجعتها من فئتي حالة الحماية وإحصائيات التهديد

○ بدء تحديد الحدث حرج ومراجعه

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 استخدام المفتاح إلى جزء المعلومات وراجع.

○ قم بإنشاء ومراجعة تقرير استخدام مفتاح التفعيل

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 14 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.

توفر تحديثات 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، وحالات الخلل الوظيفي، وتحذيرات، ومعلومات عن الأحداث
- حسب الوقت—الأحداث الأخيرة
- حسب النوع—طلبات المستخدم وأحداث التدقيق

يمكنك إنشاء أقسام الأحداث المحددة من قبل المستخدم بناءً على الإعدادات المتوفرة بغرض تكوينها في واجهة Kaspersky Security Center 14 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 جزء المعلومات في Kaspersky Security Center 14 Web Console في قسم **المراقبة والإبلاغ** عن طريق النقر على **لوحة المعلومات**.

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 14 Web Console به مجموعة افتراضية من عناصر الواجهة للفئات التالية:

- حالة الحماية
- النشر
- تحديث
- إحصائيات التهديد
- غير ذلك

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 المراقبة والإبلاغ ← لوحة المعلومات.
 2. انقر على زر إضافة تطبيق الويب المصغر أو استعادته.
 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 زر إضافة.
- 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 المراقبة والإبلاغ ← لوحة المعلومات.
 2. انقر على أيقونة الإعدادات (⚙️) الموجود بجوار عنصر الواجهة الذي ترغب في إخفائه.
 3. حدد إخفاء التطبيق المصغر.
 4. في النافذة تحذير التي تفتح، انقر فوق موافق.
- يتم إخفاء عنصر الواجهة المحدد. يمكنك لاحقاً [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 المراقبة والإبلاغ ← لوحة المعلومات.
 2. انقر على أيقونة الإعدادات (⚙️) الموجود بجوار عنصر الواجهة الذي ترغب في نقله.
 3. حدد نقل.
 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 رسماً بيانياً، يمكنك تغيير تمثيلها إلى مخطط شريطي أو مخطط خطي. يمكنك لبعض عناصر الواجهة تغيير حجمها: صغير أو متوسط أو كبير.

لتغيير تمثيل عنصر الواجهة:

1. في القائمة الرئيسية، انتقل إلى المراقبة والإبلاغ ← لوحة المعلومات.
2. انقر على أيقونة الإعدادات (⚙️) الموجود بجوار عنصر الواجهة الذي ترغب في تحريره.
3. قم بأحد الإجراءات التالية:

- لعرض عنصر الواجهة كمخطط شريطي، حدد نوع المخطط: **أشرطة**.
- لعرض عنصر الواجهة كمخطط خطي، حدد نوع المخطط: **سطور**.
- لتغيير المنطقة التي يشغلها التطبيق المصغر، حدد إحدى القيم:

• **مضغوط**

• **مضغوط (شريط فقط)**

• **متوسط (مخطط دائري مجوف)**

• **متوسط (مخطط شريطي)**

• **الحد الأقصى**

يتم تغيير تمثيل عنصر الواجهة المحدد.

تغيير إعدادات عنصر الواجهة

لتغيير إعدادات عنصر واجهة:

1. في القائمة الرئيسية، انتقل إلى المراقبة والإبلاغ ← لوحة المعلومات.
2. انقر على أيقونة الإعدادات (⚙️) الموجود بجوار عنصر الواجهة الذي ترغب في تغييره.
3. حدد إعدادات العرض.
4. في نافذة إعدادات عنصر الواجهة التي تفتح، قم بتغيير إعدادات عنصر الواجهة كما هو مطلوب.
5. انقر على **حفظ** لحفظ التغييرات.

يتم تغيير إعدادات عنصر الواجهة المحدد.

تعتمد مجموعة الإعدادات على عنصر الواجهة المعين. يوجد أدناه بعض الإعدادات الشائعة:

- **نطاق تطبيق الويب المصغر** (مجموعة الكائنات التي يعرض عنصر الواجهة معلومات لها)، مثل مجموعة الإدارة أو تحديد جهاز.

- **حدد المهمة (المهمة التي يعرض عنصر الواجهة معلومات لها).**
- **الفاصل الزمني (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.**
- **تعيين الحالة إلى حرجة إذا وتعيين الحالة إلى تحذير إذا (القواعد التي تحدد لون إشارة حركة المرور).**

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: أدونات 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: أدونات 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 القسم **المستخدمون والأدوار** ← **المستخدمون**. 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 إلى **المستخدمون والأدوار** ← **المستخدمون**.
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 **المراقبة والإبلاغ ← لوحة المعلومات**:

- **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 أقيمت الخيار معطلاً، فسُعرض 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 سَتُعرض فقط لوحة المعلومات المعدة مسبقاً 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

يصف هذا القسم كيفية استخدام التقارير وإدارة قوائم التقارير المخصصة واستخدام قوائم 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 14 Web Console في قسم **المراقبة والإبلاغ** عن طريق النقر على **التقارير**.

بشكل افتراضي، التقارير تشمل معلومات لأخر 30 يومًا.

Kaspersky Security Center به مجموعة افتراضية من التقارير للفئات التالية:

- **حالة الحماية**
- **النشر**
- **التحديث**
- **إحصاءات التهديدات**

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 المراقبة والإبلاغ ← التقارير.
2. انقر فوق إضافة.
3. يبدأ "معالج قالب التقرير الجديد". انتقل عبر المعالج من خلال استخدام زر التالي.
3. في الصفحة الأولى من المعالج، أدخل اسم التقرير وحدد نوع التقرير.
4. في صفحة النطاق للمعالج، 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 صفحة فترة إعداد التقرير 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 موافق لإغلاق المعالج.

7. قم بأحد الإجراءات التالية:

- انقر على زر حفظ وتشغيل لحفظ قالب التقرير الجديد ولتشغيل تقرير بناءً عليه. يتم حفظ قالب التقرير. يتم إنشاء التقرير.
- انقر على زر حفظ 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 المراقبة والإبلاغ ← التقارير.

2. حدد خانة الاختيار الموجودة بجوار قالب التقارير التي ترغب في عرض خصائصه وتحريرها.
كحل بديل، يمكنك أولاً إنشاء التقرير ثم النقر على زر تحرير.

3. انقر على زر فتح خصائص قالب التقرير.

سنفتح نافذة تحرير التقرير <اسم التقرير> مع تحديد تبويب عام.

4. قم بتحرير خصائص قالب التقرير:

• تبويب عام:

• اسم قالب التقرير

• أقصى عدد من الإدخالات المراد عرضها ④

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 وفقاً 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 المتاحة 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 جداً من الإدخالات. إذا كانت هذه هي الحالة، فقد تجد صعوبة في قراءتها وتحليلها جميعاً. وقد تنفذ مساحة الذاكرة في جهازك أيضاً أثناء إنشاء مثل هذا التقرير، وبالتالي لن تتمكن من عرض التقرير.

يتم تمكين هذا الخيار افتراضياً. القيمة الافتراضية هي 1000.

• مجموعة

انقر على زر إعدادات لتغيير مجموعة أجهزة العميل التي تم إنشاء التقرير من أجلها. قد لا يكون هذا الزر متاحاً لبعض أنواع التقارير. الإعدادات الفعلية تعتمد على الإعدادات المحددة أثناء إنشاء قالب التقرير.

• الفاصل الزمني

انقر على زر إعدادات لتعديل فترة التقرير. قد لا يكون هذا الزر متاحاً 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

• تضمين بيانات من خوادم الإدارة الثانوية والافتراضية ④

إذا تم تمكين هذا الخيار، فإن التقرير يقوم بتضمين معلومات من خوادم الإدارة الثانوية والظاهرية التابعة الخاضعة ل خادم 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 افتراضياً.

• أعلى إلى مستوى التداخل ④

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.

• فصل انتظار البيانات (بالدقائق) 5

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 بيانات ذاكرة التخزين المؤقت من خوادم الإدارة الثانوية)، أو لا يوجد (غير متوفر) بخلاف ذلك. القيمة الافتراضية هي 5 (ثوان).

• بيانات ذاكرة التخزين المؤقت من خوادم الإدارة الثانوية 5

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 أيضاً 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 افتراضياً.

• تكرار تحديث التخزين المؤقت (بالساعات) 5

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 5

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 افتراضياً.

• تبويب الحقول

حدد الحقول التي سيتم عرضها في التقرير، واستخدم زر **نقل لأعلى** وزر **نقل لأسفل** لتغيير ترتيب هذه الحقول. استخدم زر **إضافة** أو زر **تحديد** إذا ما كانت المعلومات في التقرير يجب أن تبقى مرتبة ومفترقة لكل من الحقول. في قسم **عوامل تصفية حقول التفاصيل**، يمكنك أيضاً النقر على زر **تحويل عوامل تصفية** 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 **تحويل عوامل تصفية** على اليمين. انقر على زر **تحويل عوامل تصفية** لتأكيد التحويل. يمكنك الآن تحديد عامل تصفية محوّل بشروط من قسم **حقول التفاصيل** 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). أيضاً لن يحتوي التقرير المحوّل على أي بيانات من خوادم الإدارة الثانوية التي تقوم بتشغيل مثل هذه الإصدارات غير المتوافقة.

5. انقر على **حفظ** لحفظ التغييرات.

6. انقر على زر إغلاق (X) لإغلاق نافذة تحرير التقرير > اسم التقرير <.

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 المراقبة والإبلاغ ← التقارير.
 2. حدد خانة الاختيار الموجودة بجوار التقرير الذي ترغب في تصديره إلى ملف.
 3. انقر على الزر تصدير التقرير.
 4. في النافذة التي تفتح، قم بتغيير اسم ملف التقرير في حقل الاسم. بشكل افتراضي، يتوافق اسم الملف مع اسم قالب التقرير المحدد.
 5. حدد نوع ملف التقرير: XML أو HTML أو PDF.
 6. انقر على الزر تصدير التقرير.
- 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 المراقبة والإبلاغ ← التقارير.
 2. انقر على اسم قالب التقرير الذي ترغب في استخدامه لإنشاء تقرير.
- يتم إنشاء وعرض تقرير باستخدام القالب المحدد.
- ويعرض التقرير البيانات التالية:
- في تبويب الملخص:
 - 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 تمثيلاً.
 - جدول موحد يحتوي على مؤشرات التقرير المعدودة.
 - في تبويب التفاصيل، 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 **المراقبة والإبلاغ** ← **التقارير**.
2. [اختياري] حدد خانة الاختيار الموجودة بجوار قوالب التقارير التي ترغب في إنشاء مهمة تسليم تقرير لها.
3. انقر على زر **مهمة تسليم تقرير جديد**.
4. يبدأ تشغيل معالج إضافة مهمة. انتقل عبر المعالج من خلال استخدام زر **التالي**.
5. في الصفحة الأولى من المعالج، أدخل اسم المهمة. الاسم الافتراضي هو **تسليم التقارير (>ن)** حيث <ن> هو رقم تسلسل المهمة.
6. في صفحة إعدادات المهمة في المعالج، حدد الإعدادات التالية:
 - a. قوالب التقارير التي سيتم تسليمها بالمهمة. إذا حددتها في الخطوة الثانية، يمكنك تخطي هذه الخطوة.
 - b. تنسيق التقرير HTML أو XLS أو PDF.
 - c. سواء كان سيتم إرسال التقارير عبر البريد الإلكتروني أو مع إعدادات الإخطار بالبريد الإلكتروني.
 - d. سواء كان سيتم حفظ التقارير إلى مجلد، وسواء إذا ما كان سيتم استبدال تقارير محفوظة مسبقاً في هذا المجلد، وسواء إذا ما كان سيتم استخدام حساب معين للوصول إلى المجلد (المجلد مشترك).
7. إذا كنت ترغب في تعديل إعدادات المهام الأخرى بعد إنشاء المهمة، في صفحة **إنهاء عملية إنشاء المهمة في المعالج**، قم بتفعيل خيار **فتح تفاصيل المهمة عند اكتمال الإنشاء**.
8. انقر على زر **إنشاء لإنشاء المهمة** وعلق المعالج. يتم إنشاء مهمة تسليم التقرير. إذا قمت بتفعيل خيار **فتح تفاصيل المهمة عند اكتمال الإنشاء**، ستفتح نافذة إعدادات المهمة.

حذف قوالب التقارير

لحذف قالب أو عدة قوالب تقارير:

1. في القائمة الرئيسية، انتقل إلى **المراقبة والإبلاغ** ← **التقارير**.
 2. حدد خانة الاختيار الموجودة بجوار قوالب التقارير التي ترغب في حذفها.
 3. انقر فوق الزر **حذف**.
 4. في النافذة التي تفتح انقر على زر **موافق 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.

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، وحالات الخلل الوظيفي، وتحذيرات، ومعلومات عن الأحداث
- حسب الوقت—الأحداث الأخيرة
- حسب النوع—طلبات المستخدم وأحداث التدقيق

يمكنك إنشاء أقسام الأحداث المحددة من قبل المستخدم بناءً على الإعدادات المتوفرة بغرض تكوينها في واجهة Kaspersky Security Center 14 Web Console.

تتوفر تحديدات الأحداث في Kaspersky Security Center 14 Web Console في قسم المراقبة والإبلاغ عن طريق النقر على تحديدات الأحداث.

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
- عمليات الخلل الوظيفي
- التحذيرات
- رسائل المعلومات
- 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).

لكل من التحديدات 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 [المراقبة والإبلاغ](#) ← [تحديدات الأحداث](#).
 2. انقر فوق [إضافة](#).
 3. في نافذة [تحديد حدث جديد](#) التي تفتح، حدد إعدادات تحديد الحدث الجديد. افعل هذا في قسم أو أكثر من الأقسام في النافذة.
 4. انقر على [حفظ](#) لحفظ التغييرات.
ستفتح نافذة التأكيد.
 5. لعرض نتيجة تحديد الحدث، أبق على خانة الاختيار [الانتقال إلى نتيجة الاختيار محددة](#).
 6. انقر على [حفظ](#) لتأكيد إنشاء تحديد الحدث.
- إذا احتفظت بخانة الاختيار [الانتقال إلى نتيجة الاختيار 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 [المراقبة والإبلاغ](#) ← [تحديدات الأحداث](#).
2. حدد خانة الاختيار الموجودة بجوار تحديد الحدث الذي ترغب في تحريره.
3. انقر على زر [خصائص](#).
ستفتح نافذة إعدادات تحديد حدث.
4. قم بتحرير خصائص تحديد الحدث.

لتحديدات الأحداث المحددة مسبقاً، لا يمكنك إلا تحرير خصائص علامات التبويب التالية: عام (باستثناء اسم التحديد) والوقت وحقوق الوصول.

للتحديدات التي يحددها المستخدم، يمكنك تحرير جميع الخصائص.

5. انقر على **حفظ** لحفظ التغييرات.

يظهر تحديد الحدث الذي تم تحريره في القائمة.

عرض قائمة تحديد الحدث

لعرض تحديد حدث:

1. في القائمة الرئيسية، انتقل إلى **المراقبة والإبلاغ** ← **تحديدات الأحداث**.
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 **إعادة تكوين الفرز والبدء**.

b. في نافذة **إعادة تكوين الفرز لتحديد الحدث 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.

عرض تفاصيل حدث

لعرض تفاصيل حدث:

1. **ابدأ تحديد حدث**.

2. انقر على وقت الحدث المطلوب.

سنفتح نافذة **خصائص الحدث**.

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

لتصدير الأحداث إلى ملف:

1. [ابدأ تحديد حدث](#).

2. حدد خانة الاختيار الموجودة بجوار الحدث المطلوب.

3. انقر على زر **تصدير إلى ملف**.

يتم تصدير الحدث المحدد إلى ملف.

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 **سجل المراجعة**.

يتم فتح تاريخ مراجعة الكائن.

حذف الأحداث

لحذف حدث أو عدة أحداث:

1. [ابدأ تحديد حدث](#).

2. حدد خانة الاختيار الموجودة بجوار الأحداث المطلوبة.

3. انقر فوق الزر **حذف**.

يتم حذف الأحداث المحددة ولا يمكن استردادها.

حذف تحديدات الحدث

لا يمكنك حذف إلا تحديثات الأحداث من تحديد المستخدم. لا يمكن حذف تحديثات الأحداث المحددة مسبقًا.

لحذف تحديد حدث أو عدة تحديثات:

1. في القائمة الرئيسية، انتقل إلى المراقبة والإبلاغ ← تحديثات الأحداث.
 2. حدد خانة الاختيار الموجودة بجوار تحديثات الحدث التي ترغب في حذفها.
 3. انقر على حذف.
 4. في النافذة التي تفتح، انقر على موافق.
- 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 لمدة 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، فترة التخزين الطويلة لحدث تتيح لك إجراء مهام المراقبة وإعداد التقارير لفترة أطول من الوقت.

لتحديد فترة التخزين لحدث في قاعدة بيانات خادم الإدارة:

1. حدد الأجهزة ← السياسات وملفات التعريف.
2. قم بأحد الإجراءات التالية:
 - لتكوين فترة التخزين لأحداث عميل الشبكة أو لتطبيق Kaspersky مُدار، انقر على اسم السياسة المقابلة. تفتح صفحة خصائص السياسة.
 - لتكوين أحداث خادم الإدارة، في أعلى الشاشة، انقر على أيقونة الإعدادات (⚙️) الموجودة بجوار اسم خادم الإدارة المطلوب. إذا كان لديك سياسة لخادم الإدارة، يمكنك النقر على اسم هذه السياسة بدلاً من ذلك. ستفتح صفحة خصائص خادم الإدارة (أو صفة خصائص سياسة خادم الإدارة).
3. حدد تبويب تكوين الحدث.
4. حدد قسم خلل وظيفي أو تحذير أو معلومات.
5. في قائمة أنواع الأحداث في الجزء الأيمن، انقر على رابط الحدث الذي ترغب في تغيير فترة تخزينه. في قسم تسجيل الحدث في النافذة التي تفتح، يتم تفعيل خيار تخزين في قاعدة البيانات الخاصة بخادم الإدارة لمدة (بالأيام).
6. في خانة التحرير أسفل زر التبديل هذا، أدخل عدد أيام تخزين الحدث.

7. إذا كنت لا ترغب في تخزين حدث في قاعدة بيانات خادم الإدارة، قم بتعطيل خيار تخزين في قاعدة البيانات الخاصة بخادم الإدارة لمدة (بالأيام).

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.

8. انقر على موافق.

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.

أنواع الأحداث

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 الأجهزة المحمولة التي تعمل بنظام iOS MDM، وخادم الأجهزة المحمولة Exchange. أنواع الأحداث التي تظهر في تطبيقات Kaspersky غير مدرجة في هذا القسم.

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 مدة التخزين للأحداث:

• وحدة تحكم الإدارة: [تعيين مدة التخزين لحدث](#)

• Kaspersky Security Center 14 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**: معرف 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.

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	<p>يقوم Kaspersky Security Center بالتحقق مما إذا تم تجاوز قيود الترخيص أم لا بمعدل مرة يوميًا.</p> <p>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.</p> <p>حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none">• استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا.• تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). <p>يحدد Kaspersky Security Center القواعد المُستخدمة لإنشاء أحداث عند تجاوز تقييد الترخيص.</p>	180 يومًا
انتشار الفيروسات	26 (للحماية من تهديدات الملفات)	GNRL_EV_VIRUS_OUTBREAK	<p>تحدث الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة زمنية قصيرة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none">• يمكنك تكوين الحد في خصائص خادم الإدارة.• قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة التي	180 يومًا

	سيتم تشغيلها عند وقوع هذا الحدث.			
180 يوماً	<p>تحدث الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة زمنية قصيرة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • يمكنك تكوين الحد في خصائص خادم الإدارة. • قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة البيئي سيتم تشغيلها عند وقوع هذا الحدث. 	GNRL_EV_VIRUS_OUTBREAK	27 (للحماية من تهديدات البريد)	انتشار الفيروسات
180 يوماً	<p>تحدث الأحداث من هذا النوع عند تجاوز عدد الكائنات الضارة التي تم اكتشافها على العديد من الأجهزة المُدارة للحد خلال فترة زمنية قصيرة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • يمكنك تكوين الحد في خصائص خادم الإدارة. • قم بإنشاء سياسة أكثر صرامة يتم تفعيلها أو قم بإنشاء المهمة البيئي سيتم تشغيلها عند وقوع هذا الحدث. 	GNRL_EV_VIRUS_OUTBREAK	28 (الجدار الحماية)	انتشار الفيروسات
180 يوماً	<p>تحدث الأحداث من هذا النوع في حالة وجود أي جهاز مُدار مرئياً على الشبكة، ولكنه غير متصل بخادم الإدارة لفترة زمنية محددة.</p> <p>تعرف على ما يمنع التشغيل السليم لعميل الشبكة على الجهاز. تتضمن الأسباب المحتملة حدوث مشكلات في الشبكة وإزالة عميل الشبكة من الجهاز.</p>	KLSRV_HOST_OUT_CONTROL	4111	أصبح الجهاز غير مُدار
180 يوماً	<p>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.</p>	KLSRV_HOST_STATUS_CRITICAL	4113	حالة الجهاز حرج
180 يوماً	<p>تقع الأحداث من هذا النوع عندما يضيف برنامج Kaspersky رمز التنشيط أو ملف المفتاح الذي تستخدمه في قائمة الرفض.</p> <p>تواصل مع الدعم الفني للحصول على المزيد من التفاصيل.</p>	KLSRV_LICENSE_BLACKLISTED	4124	تمت إضافة ملف المفتاح إلى قائمة الرفض
180 يوماً	<p>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.</p>	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	4130	وضع الوظائف المحدودة

	<p>في ما يلي أسباب وقوع الحدث والاستجابات المناسبة له:</p> <ul style="list-style-type: none"> • لقد انتهت فترة الترخيص. يقدم ترخيص لاستخدام وضع الوظائف الكاملة لـ Kaspersky Security Center (إضافة رمز تنشيط صالح أو ملف المفتاح لخدم 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	<p>تحدث أحداث من هذا النوع عندما يقترب تاريخ انتهاء صلاحية <u>الترخيص التجاري</u>.</p> <p>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 و 15 يوم 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.</p> <p>عند انتهاء صلاحية الترخيص التجاري، يوفر Kaspersky Security Center <u>الوظائف الأساسية فقط</u>.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • تأكد من إضافة <u>مفتاح ترخيص احتياطي</u> إلى خادم الإدارة. • إذا كنت تستخدم <u>اشترِ الآن</u>، فتأكد من تجديده. يتم تجديد الاشتراك غير المحدود تلقائيًا في حالة الدفع المسبق لموفر الخدمة في المواعيد المحددة. 	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	4129	ستنتهي فترة صلاحية الترخيص قريبًا
180 يومًا	<p>تحدث الأحداث من هذا النوع عند انتهاء صلاحية شهادة خادم الإدارة لإدارة الجهاز المحمول.</p> <p>تحتاج إلى <u>تحديث الشهادة منتهية الصلاحية</u>.</p> <p>يمكنك تكوين التحديثات التلقائية للشهادات بتحديد <u>إعادة إصدار الشهادة تلقائيًا إن أمكن</u> خانة الاختيار في <u>إعدادات إصدار الشهادة</u>.</p>	KLSRV_CERTIFICATE_EXPIRED	4132	انتهت صلاحية الشهادة
180 يومًا	<p>تحدث الأحداث من هذا النوع في حالة إبطال <u>التحديثات المستمرة</u> (يتم عرض</p>	KLSRV_SEAMLESS_UPDATE_REVOKED	4142	تم إبطال تحديثات

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.

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

يوضح الجدول أدناه أنواع أحداث خادم إدارة Kaspersky Security Center التي تدرج ضمن مستوى أهمية **خلل وظيفي**.

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. <u>يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المرخصة.</u> تشمل مجموعة التطبيقات المرخصة على التطبيقات التي تفي بالمعايير المحددة بواسطة.	180 يومًا
فشل استقصاء قطاع السحابة	4143	KLSRV_KL_CLOUD_SCAN_ERROR	تحدث الأحداث من هذا النوع عندما يفشل خادم الإدارة في <u>استقصاء مقطع شبكة</u> في بيئة سحابية. اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقًا لذلك.	غير مخزنة
فشل نسخ	4123	KLSRV_UPD_REPL_FAIL	تحدث الأحداث من هذا النوع عند القيام	180 يومًا

	<p>بنسخ تحديثات البرنامج إلى مجلد (مجلدات) إضافية مشتركة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • 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 (المجلدات) أم لا. • تحقق من الاتصال بالإنترنت لأنه قد يكون السبب في حدوث هذا الحدث. اتبع التعليمات للقيام بتحديث قواعد البيانات <u>والوحدات النمطية للبرامج</u>. 			التحديثات إلى المجلد المحدد
180 يومًا	<p>تحدث الأحداث من هذا النوع عند نفاذ مساحة القرص في الجهاز المثبت عليه خادم الإدارة.</p> <p>قم بتحرير مساحة القرص على الجهاز.</p>	KLSRV_DISK_FULL	4107	لا توجد مساحة فارغة على القرص
180 يومًا	<p>تحدث الأحداث من هذا النوع في حال عدم توافر <u>المجلد المشترك لخادم الإدارة</u>.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • 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. 	KLSRV_SHARED_FOLDER_UNAVAILABLE	4108	المجلد المشترك غير متاح
180 يومًا	<p>تحدث الأحداث من هذا النوع في حال أصبحت قاعدة بيانات خادم الإدارة غير متاحة.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • 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. 	KLSRV_DATABASE_UNAVAILABLE	4109	قاعدة بيانات خادم الإدارة غير متوفرة
180 يومًا	<p>تحدث الأحداث من هذا النوع في حالة عدم توافر مساحة فارغة في قاعدة بيانات خادم الإدارة.</p>	KLSRV_DATABASE_FULL	4110	لا توجد مساحة فارغة في قاعدة

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، وفقاً 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 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 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.

أحداث التحذير لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية تحذير.

أحداث التحذير لخادم الإدارة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	الوصف	مدة التخزين الافتراضية.
تم تجاوز حد الترخيص	4098	KLSRV_EV_LICENSE_CHECK_100_110	يقوم Kaspersky Security Center بالتحقق مما إذا تم تجاوز قيود الترخيص أم لا بمعدل مرة يوميًا.	90 يومًا

	<p>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 <u>وحدات الترخيص</u> المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد يشكل من 100% إلى 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص.</p> <p>حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا. • تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). <p>يحدد Kaspersky Security Center <u>القواعد المُستخدمة لإنشاء أحداث</u> عند تجاوز تقييد الترخيص.</p>			
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يظهر الجهاز المُدار عدم النشاط لبعض الوقت.</p> <p>يحدث هذا غالبًا عند إيقاف تشغيل الجهاز المُدار.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • 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 14 Web Console. • حدد الفاصل الزمني الذي يتم بعده إزالة الجهاز تلقائيًا من المجموعة باستخدام وحدة تحكم الإدارة أو باستخدام Kaspersky Security Center 14 Web Console. 	KLSRV_EVENT_HOSTS_NOT_VISIBLE	4103	ظل الجهاز غير نشط على الشبكة لوقت طويل
90 يومًا	تحدث الأحداث من هذا النوع عندما يعتبر خادم الإدارة جهازين مُدارين	KLSRV_EVENT_HOSTS_CONFLICT	4102	تعارض في أسماء الجهاز

	<p>أو أكثر كجهاز واحد.</p> <p>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.</p> <p>لتجنب هذه المشكلة، قم بتبديل عميل الشبكة إلى <u>وضع استنساخ القرص</u> على جهاز مرجعي قبل استنساخ محرك الأقراص الثابتة لهذا الجهاز.</p>			
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يتم تعيين الحالة تحذير للجهاز المُدار. يمكنك <u>تكوين الشروط</u> التي يتم من خلالها تغيير حالة الجهاز إلى تحذير.</p>	KLSRV_HOST_STATUS_WARNING	4114	حالة الجهاز تحذير
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما يصل عدد عمليات التثبيت لتطبيقات الطرف الثالث المضمنة في <u>مجموعة التطبيقات المرخصة</u> إلى 90% من الحد الأقصى للقيمة المسموح بها <u>المحددة في خصائص مفتاح الترخيص</u>.</p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • 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. <p>يمكنك <u>إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية</u> باستخدام الوظائف الخاصة بمجموعات التطبيقات المرخصة.</p>	KLSRV_INVLICPROD_FILLED	4127	سيتم تجاوز حد عمليات التثبيت لإحدى مجموعات التطبيقات المرخصة قريبًا
90 يومًا	<p>تحدث الأحداث من هذا النوع عندما تفشل إعادة إصدار شهادة إدارة الأجهزة المحمولة تلقائيًا.</p> <p>قد تكون الأسباب والردود المناسبة على الحدث فيما يلي:</p> <ul style="list-style-type: none"> • تم بدء إعادة الإصدار التلقائي للشهادة التي تم تعطيل خيار <u>إعادة إصدار الشهادة تلقائيًا إن أمكن</u>. قد يكون هذا بسبب حدوث خطأ أثناء إنشاء الشهادة. قد يلزم إعادة إصدار الشهادة يدويًا. • إذا كنت تستخدم <u>تكاملاً مع بنية تحتية للمفتاح العام</u>، فقد يكون 	KLSRV_CERTIFICATE_REQUESTED	4133	تم طلب شهادة

	السبب هو عدم وجود سمة SAM-Account-Name للحساب المستخدم للتكامل مع PKI وإصدار الشهادة. راجع خصائص الحساب.			
90 يومًا	تحدث الأحداث من هذا النوع عندما يزيل المسؤول أي نوع من الشهادات (عامة، بريد، VPN) لإدارة الجهاز 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.	KLSRV_CERTIFICATE_REMOVED	4134	تمت إزالة الشهادة
غير مخزنة	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.	KLSRV_APN_CERTIFICATE_EXPIRED	4135	انتهت صلاحية شهادة أسماء نقاط الوصول
غير مخزنة	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.	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	4136	ستنتهي صلاحية شهادة أسماء نقاط الوصول قريبًا
90 يومًا	تحدث الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Google 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 Google Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات").	KLSRV_GCM_DEVICE_ERROR	4138	فشل إرسال رسالة FCM إلى الجهاز المحمول
90 يومًا	تحدث الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Google Firebase (Cloud Messaging, FMC) لتوصيل الأجهزة المحمولة المدارة	KLSRV_GCM_HTTP_ERROR	4139	حدث خطأ في HTTP أثناء إرسال رسالة FCM إلى خادم FCM

	<p>بنظام التشغيل Android ويعود خادم FMC إلى طلب خادم الإدارة برمز HTTP غير 200 (موافق). قد تكون الأسباب والردود المناسبة على الحدث فيما يلي:</p> <ul style="list-style-type: none"> • مشكلات من جانب خادم FMC. اقرأ رمز HTTP في تفاصيل وصف الحدث واستجب وفقاً لذلك. لمزيد من المعلومات حول رموز HTTP المستلمة من خادم FMC والأخطاء ذات الصلة، يُرجى الرجوع إلى وثائق خدمة Google Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات"). • مشاكل من جانب الخادم الوكيل (إذا كنت تستخدم خادمًا وكيلًا). اقرأ كود HTTP في تفاصيل الحدث واستجب وفقاً لذلك. 			
90 يومًا	<p>تحدث الأحداث من هذا النوع بسبب أخطاء غير متوقعة من جانب خادم الإدارة عند العمل مع بروتوكول Google Firebase Cloud Messaging HTTP. اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقاً لذلك. إذا لم تتمكن من إيجاد حل لمشكلة ما بنفسك، فنوصيك بالاتصال بالدعم الفني لـ Kaspersky.</p>	KLSRV_GCM_GENERAL_ERROR	4140	فشل إرسال رسالة FCM إلى خادم FCM
90 يومًا	<p>تحدث الأحداث من هذا النوع عند نفاد مساحة القرص في الجهاز المثبت عليه خادم الإدارة. قم بتحرير مساحة القرص على الجهاز.</p>	KLSRV_NO_SPACE_ON_VOLUMES	4105	توجد مساحة فارغة قليلة على القرص الصلب
90 يومًا	<p>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، وفقاً لـ DBMS التي تستخدمها، والاستجابات المناسبة للحدث.</p> <p>إنك تستخدم خادم SQL Server Express Edition DBMS:</p> <ul style="list-style-type: none"> • في وثيقة SQL Server Express، قم بفحص حد حجم قاعدة البيانات للإصدار الذي تستخدمه. من المحتمل أن قاعدة بيانات خادم الإدارة الخاصة بك 	KLSRV_NO_SPACE_IN_DATABASE	4106	توجد مساحة فارغة قليلة في قاعدة بيانات خادم الإدارة

	<p>على وشك الوصول إلى حد حجم قاعدة البيانات.</p> <ul style="list-style-type: none"> • <u>يمكنك تقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.</u> • 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. <p>إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition:</p> <ul style="list-style-type: none"> • <u>لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.</u> • <u>يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.</u> استعرض المعلومات عند <u>تحديد DBMS.</u> 			
90 يومًا	<p>تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي.</p> <p>اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الثانوي واستجب وفقًا لذلك.</p>	KLSRV_EV_SLAVE_SRV_DISCONNECTED	4116	تمت مقاطعة الاتصال بخادم الإدارة الثانوي
90 يومًا	<p>تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي.</p> <p>اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الرئيسي واستجب وفقًا لذلك.</p>	KLSRV_EV_MASTER_SRV_DISCONNECTED	4118	تم قطع الاتصال بخادم الإدارة الأساسي
90 يومًا	<p>تحدث أحداث من هذا النوع عندما يسجل خادم الإدارة تحديثات جديدة لبرنامج Kaspersky المثبت على الأجهزة المدارة التي تتطلب الموافقة ليتم تثبيتها.</p> <p>وافق على التحديثات أو ارفضها باستخدام وحدة تحكم الإدارة أو باستخدام <u>Kaspersky Security Center Web Console</u>.</p>	KLSRV_SEAMLESS_UPDATE_REGISTERED	4141	تم تسجيل تحديثات جديدة للوحدات النمطية لبرنامج Kaspersky
غير مخزنة	<p>تحدث الأحداث من هذا النوع عند بدء حذف الأحداث القديمة من قاعدة بيانات خادم الإدارة بعد <u>الوصول إلى سعة قاعدة بيانات خادم الإدارة.</u></p>	KLSRV_EVP_DB_TRUNCATING	4145	تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وبدأت

	<p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • <u>قم بتغيير الحد الأقصى لعدد الأحداث المخزنة في قاعدة بيانات خادم الإدارة.</u> • <u>يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.</u> 			عملية حذف الأحداث
غير مخزنة	<p>تحدث الأحداث من هذا النوع عند حذف الأحداث القديمة من قاعدة بيانات خادم الإدارة بعد <u>الوصول إلى سعة قاعدة بيانات خادم الإدارة.</u></p> <p>يمكنك الاستجابة للحدث من خلال الطرق التالية:</p> <ul style="list-style-type: none"> • <u>قم بتغيير الحد الأقصى المسموح به لعدد الأحداث المخزنة في قاعدة بيانات خادم الإدارة.</u> • <u>يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.</u> 	KLSRV_EVP_DB_TRUNCATED	4146	تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وتم حذف الأحداث

الأحداث المعلوماتية لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center التي تندرج ضمن مستوى أهمية معلومات.

الأحداث المعلوماتية لخادم الإدارة

مدة التخزين الافتراضية.	نوع الحدث	معرف نوع الحدث	اسم العرض لنوع الحدث
30 يومًا	KLSRV_EV_LICENSE_CHECK_90	4097	تم استنفاد أكثر من 90% من هذا المفتاح
30 يومًا	KLSRV_EVENT_HOSTS_NEW_DETECTED	4100	تم اكتشاف جهاز جديد
30 يومًا	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	4101	تمت إضافة جهاز إلى المجموعة تلقائيًا
30 يومًا	KLSRV_INVISIBLE_HOSTS_REMOVED	4104	تمت إزالة الجهاز من المجموعة: غير نشط على الشبكة لمدة طويلة
30 يومًا	KLSRV_INVLICPROD_EXPIRED_SOON	4128	سيتم تجاوز حد عمليات التثبيت قريبًا (تم استهلاك أكثر من 95%) لأحدى مجموعات التطبيقات المرخصة
30 يومًا	KLSRV_APS_FILE_APPEARED	4131	تم العثور على ملفات سترسل إلى Kaspersky للتحليل
30 يومًا	KLSRV_GCM_DEVICE_REGID_CHANGED	4137	تم تغيير معرف مثيل FCM على هذا الجهاز المحمول
30 يومًا	KLSRV_UPD_REPL_OK	4122	تم نسخ التحديثات بنجاح إلى المجلد المحدد
30 يومًا	KLSRV_EV_SLAVE_SRV_CONNECTED	4115	تم إنشاء الاتصال بخادم الإدارة الثانوي
30 يومًا	KLSRV_EV_MASTER_SRV_CONNECTED	4117	تم إنشاء الاتصال بخادم الإدارة الأساسي
30 يومًا	KLSRV_UPD_BASES_UPDATED	4144	تم تحديث قواعد البيانات
30 يومًا	KLAUD_EV_SERVERCONNECT	4147	تدقيق: تم إنشاء اتصال بخادم الإدارة
30 يومًا	KLAUD_EV_OBJECTMODIFY	4148	تدقيق: تم تعديل الكائن

30 يومًا	KLAUD_EV_TASK_STATE_CHANGED	4150	تدقيق: تم تغيير حالة الكائن
30 يومًا	KLAUD_EV_ADMGROUP_CHANGED	4149	تدقيق: تم تعديل إعدادات المجموعة
30 يومًا	KLAUD_EV_SERVERDISCONNECT	4151	التدقيق: تم إنهاء الاتصال بخادم الإدارة
30 يومًا	KLAUD_EV_OBJECTPROPMODIFIED	4152	التدقيق: تم تعديل خصائص الكائن
30 يومًا	KLAUD_EV_OBJECTACLMODIFIED	4153	التدقيق: تم تعديل أذونات المستخدم

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 تدرج ضمن مستوى خطورة **خلل وظيفي**.

أحداث الخلل الوظيفي لعميل الشبكة

مدة التخزين الافتراضية.	الوصف	نوع الحدث	معرف نوع الحدث	اسم العرض لنوع الحدث
30 يومًا	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.	KLNAG_EV_PATCH_INSTALL_ERROR	770	خطأ في تثبيت التحديث
30 يومًا	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.	KLNAG_EV_3P_PATCH_INSTALL_ERROR	7697	فشل تثبيت تحديث برامج الجهة الخارجية
30 يومًا	تحدث الأحداث من هذا النوع في حالة عدم نجاح تحديثات Windows. يمكنك تكوين تحديثات Windows في سياسة عميل الشبكة .	KLNAG_EV_WUA_INSTALL_ERROR	7717	فشل تثبيت تحديثات Windows

اقرأ وصف الحدث. ابحث عن الخطأ في قاعدة معارف Microsoft. واتصل بالدعم الفني لـ Microsoft إذا تعذر عليك حل المشكلة بنفسك.

أحداث تحذير عميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center التي تدرج ضمن مستوى الخطورة تحذير.

أحداث تحذير عميل الشبكة

مدة التخزين الافتراضية.	نوع الحدث	معرف نوع الحدث	اسم العرض لنوع الحدث
30 يومًا	KLNAG_EV_PATCH_INSTALL_WARNING	7701	ظهر تحذير أثناء تثبيت تحديث الوحدة النمطية للبرامج
30 يومًا	KLNAG_EV_3P_PATCH_INSTALL_WARNING	7696	اكتمل تثبيت تحديث برامج الجهة الخارجية مع وجود تحذير
30 يومًا	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	7698	تم تأجيل تثبيت تحديث برامج الجهة الخارجية
30 يومًا	GNRL_EV_APP_INCIDENT_OCCURED	549	وقع حادث
30 يومًا	KSNPROXY_STARTED_CON_CHK_FAILED	7718	بدأ وكيل KSN. فشل فحص مدى توفر KSN

الأحداث المعلوماتية لعميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center التي تدرج ضمن مستوى الخطورة معلومات.

الأحداث المعلوماتية لعميل الشبكة

مدة التخزين الافتراضية.	نوع الحدث	معرف نوع الحدث	اسم العرض لنوع الحدث
30 يومًا	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	7699	تم تثبيت تحديث الوحدات النمطية للبرامج بنجاح
30 يومًا	KLNAG_EV_PATCH_INSTALL_STARTING	7700	بدأ تثبيت تحديث الوحدة النمطية للبرامج
30 يومًا	KLNAG_EV_INV_APP_INSTALLED	7703	تم تثبيت التطبيق
30 يومًا	KLNAG_EV_INV_APP_UNINSTALLED	7704	تم إلغاء تثبيت التطبيق
30 يومًا	KLNAG_EV_INV_OBS_APP_INSTALLED	7705	تم تثبيت التطبيق المراقب
30 يومًا	KLNAG_EV_INV_OBS_APP_UNINSTALLED	7706	تم إلغاء تثبيت التطبيق المراقب
30 يومًا	KLNAG_EV_INV_CMPTR_APP_INSTALLED	7707	تم تثبيت التطبيق التابع لجهة خارجية
30 يومًا	KLNAG_EV_DEVICE_ARRIVAL	7708	تمت إضافة جهاز جديد
30 يومًا	KLNAG_EV_DEVICE_REMOVE	7709	تمت إزالة الجهاز
30 يومًا	KLNAG_EV_NAC_DEVICE_DISCOVERED	7710	تم اكتشاف جهاز جديد
30 يومًا	KLNAG_EV_NAC_HOST_AUTHORIZED	7711	تم اعتماد الجهاز
30 يومًا	KLUSRLOG_EV_FILE_READ	7712	مشاركة سطح المكتب لـ Windows: تمت قراءة الملف
30 يومًا	KLUSRLOG_EV_FILE_MODIFIED	7713	مشاركة سطح المكتب لـ Windows:

تم تعديل الملف			
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**.

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

30 يوماً	INSTALLAPPLICATION_COMMAND_FAILED	فشل في تثبيت التطبيق
30 يوماً	APPLYREDEMPTIONCODE_COMMAND_FAILED	فشل في تعيين رمز الاسترداد للتطبيق
30 يوماً	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	فشل في طلب قائمة التطبيقات المُدارة
30 يوماً	REMOVEAPPLICATION_COMMAND_FAILED	فشل في إزالة التطبيق المُدار
30 يوماً	SETROAMINGSETTINGS_COMMAND_FAILED	تم رفض إعدادات التجوال
30 يوماً	PRODUCT_FAILURE	حدث خطأ في تشغيل التطبيق
30 يوماً	MALFORMED_COMMAND	تحتوي نتيجة الأمر على بيانات غير صالحة
30 يوماً	SEND_PUSH_NOTIFICATION_FAILED	فشل في إرسال إشعار الدفع
30 يوماً	SEND_COMMAND_FAILED	فشل في إرسال الأمر
30 يوماً	DEVICE_NOT_FOUND	لم يتم العثور على الجهاز

أحداث التحذير ل خادم 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 تحذير.

أحداث التحذير ل خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

مدة التخزين الافتراضية.	نوع الحدث	اسم العرض لنوع الحدث
30 يوماً	INACTICE_DEVICE_TRY_CONNECTED	تم اكتشاف محاولة توصيل جهاز محمول مقفل
30 يوماً	MDM_PROFILE_WAS_REMOVED	تم إزالة ملف التعريف
30 يوماً	CLIENT_CERT_ALREADY_IN_USE	تم اكتشاف محاولة إعادة استخدام شهادة عميل.
30 يوماً	FOUND_INACTIVE_DEVICE	تم اكتشاف جهاز غير مفعّل.
30 يوماً	NEED_REDEMPTION_CODE	رمز الاسترداد مطلوب.
30 يوماً	UMDM_PROFILE_WAS_REMOVED	تم تضمين ملف التعريف في سياسة تمت إزالتها من الجهاز.

الأحداث المعلوماتية ل خادم 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 معلومات.

الأحداث المعلوماتية ل خادم الأجهزة المحمولة التي تعمل بنظام iOS MDM

مدة التخزين الافتراضية.	نوع الحدث	اسم العرض لنوع الحدث
30 يوماً	NEW_DEVICE_CONNECTED	تم توصيل جهاز محمول جديد.
30 يوماً	PROFILELIST_COMMAND_SUCCESSFULL	تم طلب قائمة بملفات التعريف بنجاح.
30 يوماً	INSTALLPROFILE_COMMAND_SUCCESSFULL	تم تثبيت ملف التعريف بنجاح.
30 يوماً	REMOVEPROFILE_COMMAND_SUCCESSFULL	تمت إزالة ملف التعريف بنجاح.
30 يوماً	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	تم طلب قائمة بملفات تعريف التزويد بنجاح.
30 يوماً	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	تم تثبيت ملف تعريف التزويد بنجاح.
30 يوماً	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	تم إزالة ملف تعريف التزويد بنجاح.

30 يوماً	CERTIFICATELIST_COMMAND_SUCCESSFULL	تم طلب قائمة بالشهادات الرقمية بنجاح.
30 يوماً	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	تم طلب قائمة بالتطبيقات المثبتة بنجاح.
30 يوماً	DEVICEINFORMATION_COMMAND_SUCCESSFULL	تم طلب المعلومات العامة بشأن الجهاز المحمول بنجاح.
30 يوماً	SECURITYINFO_COMMAND_SUCCESSFULL	تم طلب معلومات الأمان بنجاح.
30 يوماً	DEVICELOCK_COMMAND_SUCCESSFULL	تم قفل الجهاز المحمول بنجاح.
30 يوماً	CLEARPASSCODE_COMMAND_SUCCESSFULL	تمت إعادة تعيين كلمة المرور بنجاح.
30 يوماً	ERASEDEVICE_COMMAND_SUCCESSFULL	تم مسح البيانات من الجهاز المحمول.
30 يوماً	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	تم تثبيت التطبيق بنجاح.
30 يوماً	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	تم تعيين رمز الاسترداد الخاص بالتطبيق بنجاح.
30 يوماً	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	تم طلب قائمة التطبيقات المُدارة بنجاح.
30 يوماً	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	تمت إزالة التطبيق المدار بنجاح.
30 يوماً	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	تم تطبيق إعدادات التجوال بنجاح.

أحداث خادم الأجهزة المحمولة Exchange

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بخادم الأجهزة المحمولة Exchange.

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة Exchange

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة Exchange في Kaspersky Security Center التي تشمل مستوى الخطورة **خلل وظيفي**.

أحداث الخلل الوظيفي الخاصة بخادم الأجهزة المحمولة Exchange

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
فشل في مسح البيانات من الجهاز المحمول	WIPE_FAILED	30 يوماً
يتعذر حذف معلومات حول اتصال الجهاز المحمول بصندوق البريد.	DEVICE_REMOVE_FAILED	30 يوماً
فشل تطبيق سياسة ActiveSync على صندوق البريد.	POLICY_APPLY_FAILED	30 يوماً
خطأ في تشغيل التطبيق.	PRODUCT_FAILURE	30 يوماً
فشل تعديل حالة وظائف ActiveSync.	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 يوماً

الأحداث المعلوماتية الخاصة بخادم الأجهزة المحمولة Exchange

يوضح الجدول أدناه أحداث خادم الأجهزة المحمولة Exchange في Kaspersky Security Center التي تشمل مستوى الخطورة **معلومات**.

الأحداث المعلوماتية الخاصة بخادم الأجهزة المحمولة Exchange

اسم العرض لنوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم توصيل جهاز محمول جديد.	NEW_DEVICE_CONNECTED	30 يوماً
تم مسح البيانات من الجهاز المحمول.	WIPE_SUCCESSFULL	30 يوماً

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 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 نافذة التطبيق الرئيسية، انقر فوق أيقونة **الإعدادات** (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **عام**، حدد القسم **حظر الأحداث المتكررة**.

3. في قسم **حظر الأحداث المتكررة**:

- إذا كنت ترغب في إلغاء حظر تلقي الأحداث المتكررة:

a. حدد الأحداث المتكررة التي تريد إلغاء حظرها، ثم انقر فوق زر **استبعاد**.

b. انقر على زر **حفظ**.

- إذا كنت ترغب في حظر تلقي أحداث متكررة:

a. حدد الأحداث المتكررة التي تريد حظرها، ثم انقر فوق زر **حظر**.

b. انقر على زر **حفظ**.

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 نافذة التطبيق الرئيسية، انقر فوق أيقونة **الإعدادات** (⚙️) بجوار اسم خادم الإدارة المطلوب.
تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **عام**، حدد القسم **حظر الأحداث المتكررة**.

3. في قسم **حظر الأحداث المتكررة** حدد أنواع الأحداث المتكررة التي تريد إزالة الحظر لها.

4. انقر على زر **إزالة من الحظر**.

بهذا تم حذف الحدث المتكرر من قائمة الأحداث الجماعية. سيستلم خادم الإدارة أحداثاً من هذا النوع.

تلقي الأحداث من Microsoft Exchange Servers – Kaspersky Security

يتم نقل المعلومات المتعلقة بالأحداث أثناء تشغيل التطبيقات المُدارة، مثل Kaspersky Endpoint Security for Windows، من الأجهزة المُدارة وتسجيلها في قاعدة بيانات خادم الإدارة. بشكل افتراضي، لا يتم تسجيل الأحداث من Kaspersky Security for Microsoft Exchange Servers في قاعدة بيانات خادم الإدارة. إذا تم تثبيت Kaspersky Security – Microsoft Exchange Servers على الأجهزة المُدارة في مؤسستك وتريد تلقي الأحداث من هذا التطبيق، فقم بتمكين تسجيل الحدث لهذا التطبيق باستخدام الأداة المساعدة klsclflag.

لتمكين تسجيل الحدث – Kaspersky Security – Microsoft Exchange Servers:

1. على جهاز خادم الإدارة، قم بتشغيل موجه أوامر Windows ضمن حساب له حقوق المسؤول.

2. قم بتغيير دليلك الحالي إلى مجلد تثبيت Kaspersky Security Center (عادةً، C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).\n

3. قم بتشغيل الأمر التالي:

```
klsclflag.exe -fset -pv klsrver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
```

تم تمكين تسجيل الحدث – Kaspersky Security – Microsoft Exchange Servers.

بالنسبة إلى Kaspersky Security – Microsoft Exchange Servers، فلا يمكنك تعيين مدة التخزين للأحداث أو تحديد الأحداث التي يجب حفظها في مستودع خادم الإدارة. يمكنك **تعيين الحد الأقصى لعدد الأحداث التي يمكن حفظها في المستودع**. يتم تطبيق هذا الإعداد على الأحداث الواردة من جميع تطبيقات Kaspersky.

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 [المراقبة والإبلاغ](#) ← قسم [الإخطارات](#). 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 [الإخطارات حسب مستوى الخطورة المحددة في المراقبة والإبلاغ](#) ← قسم [لوحة المعلومات](#). 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 مسبقاً:

1. في القائمة الرئيسية، انتقل إلى المراقبة والإبلاغ ← الإخطارات.
يتم تحديد فئة جميع الإخطارات في الجزء الأيسر، ويتم عرض جميع الإخطارات في الجزء الأيمن.
2. حدد إحدى الفئات في الجزء الأيسر:

• النشر

• الأجهزة

• الحماية

• تحديثات (يشمل هذا الإخطارات عن تطبيقات Kaspersky المتوفرة للتنزيل والإخطارات عن تحديثات قاعدة بيانات مكافحة الفيروسات التي تم تنزيلها).

• منع الاستغلال

• خادم الإدارة (يشمل هذا الأحداث التي تتعلق بخادم الإدارة فقط)

• الروابط المفيدة يشمل هذا روابطاً إلى موارد Kaspersky، مثل الدعم الفني من Kaspersky ومدونة Kaspersky وصفحة تجديد الترخيص وموسوعة تكنولوجيا المعلومات من Kaspersky)

• أخبار Kaspersky (يشمل هذا معلومات عن إصدارات تطبيقات Kaspersky)

يتم عرض قائمة بإخطارات الفئة المحددة. تحتوي القائمة على ما يلي:

- الأيقونة المتعلقة بموضوع الإخطار: النشر (P)، الحماية (P)، التحديثات (P)، إدارة الجهاز (P)، منع الاستغلال (P)، خادم الإدارة (P).
 - مستوى أهمية الإشعار. يتم عرض إخطارات مستويات الأهمية التالية: الإخطارات الحرجة (P)، وإخطارات التحذير (P)، وإخطارات المعلومات. يتم تجميع الإخطارات في القائمة بمستويات الأهمية.
 - الإخطار. يحتوي هذا على وصف الإخطار.
 - الإجراء. يحتوي هذا على رابط لإجراء سريع ننصح باتخاذها. يمكنك على سبيل المثال بالنقر على هذا الرابط [التقدم إلى المستودع](#) وتشبث 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.
 - تم تسجيل الحالة. 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 14 Web Console، انقر على أيقونة العلم (P).

إذا كان أيقونة العلم به نقطة حمراء، يوجد إخطارات لم يتم مراجعتها.

ستفتح نافذة تسرد الإخطارات. بشكل افتراضي، يكون تبويب جميع الإخطارات محدداً ويتم تجميع الإخطارات بمستوى الأهمية: حرج أو تحذير أو معلومات.

2. حدد تبويب النظام.

يتم عرض قائمة إخطارات مستويات الأهمية حرج (P) وتحذير (P). قائمة الإخطارات تشمل ما يلي:

- تحديد بالألوان. الإخطارات الحرجة تكون باللون الأحمر. الإخطارات التحذيرية تكون باللون الأصفر.
- الأيقونة التي تشير إلى موضوع الإخطار: النشر (P)، الحماية (P)، التحديثات (P)، إدارة الجهاز (P)، منع الاستغلال (P)، خادم الإدارة (P).

• 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 وتخس 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. في علامة تبويب المزيد.

- يتم عرض قائمة إخطارات مستويات الأهمية معلومات.
- تنظيم القائمة هو نفسه للقائمة في تبويب النظام (راجع الوصف أعلاه). الاختلاف الوحيد هو غياب تحديد الألوان.
- يمكنك تصفية الإخطارات بالفاصل الزمني للتاريخ عند تسجيلها على خادم الإدارة. استخدم خانة الاختيار **عرض عامل التصفية لإدارة عامل التصفية**.

لعرض الإخطارات على الشاشة في عنصر الواجهة:

1. في قسم لوحة المعلومات، حدد إضافة تطبيق الويب المصغر أو استعادته.

2. في النافذة التي تفتح، انقر على فئة غير ذلك وحدد عنصر الواجهة الإخطارات حسب مستوى الخطورة المحددة ثم انقر على إضافة.

- سيظهر عنصر الواجهة الآن في تبويب لوحة المعلومات. 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 أخرى: **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 (P)، الحماية (M)، التحديثات (U)، إدارة الجهاز (D)، منع الاستغلال (E)، خادم الإدارة (S).
- 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 الإخطارات لقسم المراقبة والإبلاغ.

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 لجهاز ما، يأخذ Kaspersky Security Center في الاعتبار علامة رؤية الجهاز على الشبكة (انظر الجدول أدناه). 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

القيم المتوفرة	وصف الشرط	الشرط
<ul style="list-style-type: none"> زر التبديل قيد التشغيل. زر التبديل متوقف. 	عمل الشبكة مثبت على الجهاز، إلا أن تطبيق الأمان غير مثبت.	تطبيق الأمان غير مثبت
أكثر من 0.	تم العثور على بعض الفيروسات على الجهاز عن طريق تنفيذ إحدى مهام اكتشاف الفيروسات، على سبيل المثال مهمة فحص الفيروسات، ويتجاوز عدد الفيروسات التي تم العثور عليها القيمة المحددة.	تم اكتشاف العديد من الفيروسات
<ul style="list-style-type: none"> متوقف. متوقف مؤقتًا. قيد التشغيل. 	الجهاز مرئي على الشبكة، إلا أن مستوى الحماية في الوقت الحقيقي يختلف عن المستوى الذي حدده المسؤول (في الشرط) لحالة الجهاز.	يختلف مستوى الحماية في الوقت الحقيقي عن المستوى الذي تم تعيينه من قبل المسؤول
أكثر من يوم واحد.	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لم يتم تشغيل مهمة فحص الفيروسات خلال الفاصل الزمني المحدد. لا ينطبق الشرط إلا على الأجهزة التي تمت إضافتها إلى قاعدة بيانات خادم الإدارة قبل 7 أيام أو أكثر.	لم يتم إجراء فحص الفيروسات منذ وقت طويل
أكثر من يوم واحد.	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.	قواعد البيانات قديمة
أكثر من يوم واحد.	يتم تثبيت عميل الشبكة على الجهاز، ولكن لم يتم اتصال الجهاز بخادم الإدارة خلال الفاصل الزمني المحدد نظرًا لإيقاف تشغيل الجهاز.	لم يتم الاتصال منذ فترة طويلة
أكثر من 0 عناصر.	يتجاوز عدد الكائنات التي لم تتم معالجتها في المجلد تهديدات نشطة القيمة المحددة.	تم اكتشاف تهديدات نشطة
أكثر من 0 دقائق.	الجهاز مرئي على الشبكة، إلا إن أحد التطبيقات يتطلب إعادة تشغيل الجهاز لمدة أطول من الفاصل الزمني المحدد ولأحد الأسباب المحددة.	إعادة التشغيل مطلوبة
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	الجهاز مرئي على الشبكة، إلا إن مخزون البرنامج المنفذ عبر عميل الشبكة قد اكتشف تطبيقات غير متوافقة مثبتة على الجهاز.	تم تثبيت تطبيقات غير متوافقة
<ul style="list-style-type: none"> حرج. مرتفع. متوسط. تجاهل إذا تعذر إصلاح الثغرات الأمنية. تجاهل إذا تم تعيين تحديث للثغرات. 	الجهاز مرئي على الشبكة و عميل الشبكة مثبت على الجهاز، إلا أن مهمة البحث عن الثغرات الأمنية والتحديثات المطلوبة قد اكتشفت وجود ثغرات أمنية بمستوى الخطورة المحدد في التطبيقات المثبتة على الجهاز.	تم اكتشاف ثغرات أمنية بالبرنامج
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	الجهاز مرئي على الشبكة، إلا إن الترخيص قد انتهى.	انتهت صلاحية الترخيص

أكثر من 0 أيام.	الجهاز مرئي على الشبكة، إلا أن الترخيص سينتهي على الجهاز خلال فترة أقل من عدد الأيام المحدد.	ستنتهي فترة صلاحية الترخيص قريباً
أكثر من يوم واحد.	الجهاز مرئي على الشبكة، إلا أنه لم يتم تشغيل مهمة إجراء مزامنة Windows Update خلال الفاصل الزمني المحدد.	لم يتم إجراء البحث عن تحديثات تحديث Windows منذ وقت طويل
<ul style="list-style-type: none"> 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. 	عميل الشبكة مثبت على الجهاز، إلا إن نتيجة تشفير الجهاز مساوية للقيمة المحددة.	حالة تشفير غير صالحة
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	إعدادات الجهاز المحمول تختلف عن الإعدادات المحددة في سياسة Kaspersky Endpoint Security for Android أثناء التحقق من قواعد الامتثال.	لا تتوافق إعدادات الجهاز المحمول مع السياسة
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	تم العثور على بعض الأحداث التي لم تتم معالجتها على الجهاز. يمكن إنشاء الحوادث إما تلقائياً من خلال تطبيقات Kaspersky المُدارة المثبتة على الجهاز العميل أو يدوياً من قبل المسؤول.	تم اكتشاف حوادث لم تتم معالجتها
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	تم تحديد حالة الجهاز بواسطة التطبيق المدار.	حالة الجهاز المحددة بواسطة التطبيق
أكثر من 0 ميجابايت	مساحة القرص الشاغرة على الجهاز أقل من القيمة المحددة أو أنه يتعدى 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.	نفدت مساحة قرص الجهاز
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	أثناء اكتشاف الأجهزة، تم التعرف على الجهاز بأنه مرئي على الشبكة، لكن فشلت أكثر من ثلاث محاولات للمزامنة مع خادم الإدارة.	أصبح الجهاز غير مُدار

أكثر من 0 دقائق.	الجهاز مرئي على الشبكة، إلا إنه قد تم تعطيل تطبيق الأمان على الجهاز لمدة أطول من الفاصل الزمني المحدد.	تم تعطيل الحماية
<ul style="list-style-type: none"> زر التبديل متوقف. زر التبديل قيد التشغيل. 	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لا يعمل.	تطبيق الأمان ليس 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 قواعد البيانات قديمة 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، فيم شرط قواعد البيانات قديمة لتخصيص الحالة تتغير إلى حرجة أو تحذير أو لا تتغير.

عندما يقوم Kaspersky Security Center بتعيين حالة إلى جهاز، يتم أخذ علامة الرؤية في الاعتبار بالنسبة لبعض الشروط (راجع عمود وصف الحالة). على سبيل المثال: إذا تم تعيين الحالة حرج إلى جهاز مُدار بسبب عدم استيفاء شرط قواعد البيانات قديمة ثم بعد ذلك تم تعيين علامة الرؤية للجهاز، يتم تعيين حالة موافق إلى الجهاز.

تكوين تبديل حالات الجهاز

يمكنك تغيير الشروط لتعيين الحالة حرجة أو تحذير لجهاز ما.

لتمكين تغيير حالة الجهاز إلى حرجة:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← التسلسل الهرمي للمجموعات.
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 حالة الجهاز.
4. في الجزء الأيسر، حدد حرج.
5. في الجزء الأيمن في قسم تعيين الحالة إلى حرجة إذا، 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 تحرير.

8. حدد القيمة المطلوبة للحالة المحددة.

لا يمكن تعيين القيم لكل حالة.

9. انقر على موافق.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار على حرج .

لتمكين تغيير حالة الجهاز إلى تحذير:

1. في القائمة الرئيسية، انتقل إلى الأجهزة ← التسلسل الهرمي للمجموعات.
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 حالة الجهاز.
4. في الجزء الأيسر، حدد تحذير.
5. في الجزء الأيمن في قسم تعيين الحالة إلى تحذير إذا، 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 تحرير.
 8. حدد القيمة المطلوبة للحالة المحددة.
لا يمكن تعيين القيم لكل حالة.
 9. انقر على موافق.
- عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار على 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 أعلى الشاشة، انقر على أيقونة الإعدادات (⚙️) بجوار اسم خادم الإدارة المطلوب.
ستفتح نافذة خصائص خادم الإدارة مع تحديد تبويب عام.
2. انقر على قسم الإخطار، وفي الجزء الأيمن حدد تبويب طريقة الإخطار التي تريدها:

- [البريد الإلكتروني](#) ⓘ

تبويب البريد الإلكتروني يتيح لك تكوين إخطار الحدث 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.

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 إعلانات البريد الإلكتروني.

في حال تمكين خيار **استخدام مصادقة ESMTP**، يمكنك تحديد إعدادات مصادقة ESMTP في اسم المستخدم وكلمة المرور. يكون هذا الخيار معطلاً بشكل افتراضي، وتكون إعدادات مصادقة ESMTP غير متوفرة

يمكنك تحديد إعدادات TLS للاتصال بخادم SMTP:

• لا تستخدم TLS

يمكنك تحديد هذا الخيار إذا كنت تريد تعطيل تشفير رسائل البريد الإلكتروني.

• استخدم TLS إن 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.

• استخدم TLS دوماً وتحقق من صحة شهادة الخادم

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 للاتصال TLS.

إذا قمت بتحديد قيمة **استخدم TLS دوماً وتحقق من صحة شهادة الخادم** 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 أيضاً تحديد شهادة لمصادقة العميل على خادم SMTP.

يمكنك تحديد شهادات لاتصال TLS بالنقر فوق رابط **تحديد الشهادات** :

• 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 أيضاً 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.

■ حاوية 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 **الموضوع**، حدد موضوع البريد الإلكتروني. يمكنك ترك هذا الحقل فارغًا.

في القائمة المنسدلة **قالب الموضوع**، حدد قالب موضوعك. متغير يحدده القالب المحدد يُوضع تلقائيًا في حقل **الموضوع**. يمكنك إنشاء موضوع بريد إلكتروني باختيار عدة قوالب للموضوع.

في حقل **عنوان البريد الإلكتروني للمرسل**: إذا لم يتم تحديد هذا الإعداد، فسيتم استخدام عنوان المستلم بدلاً من ذلك. **تحذير**: لا نوصي باستخدام **عنوان بريد إلكتروني وهمي**، حدد عنوان البريد الإلكتروني للمرسل. إذا تركت هذا الحقل فارغًا، سيتم استخدام عنوان المستلم افتراضيًا. لا يُنصح باستخدام عناوين بريد إلكتروني وهمية.

يحتوي حقل **رسالة إخطار** على نص قياسي يحتوي على معلومات حول الحدث الذي يرسله التطبيق عند وقوع حدث. يتضمن هذا النص معلومات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة عن طريق إضافة بعض **المعلومات 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 **تكوين حد الإخطارات الرقمي** يتيح لك تحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مدار الفاصل الزمني المحدد.

النقر على زر **إرسال رسالة اختبار** يتيح لك التحقق مما إذا قمت بتكوين الإخطارات بطريقة صحيحة: يرسل التطبيق إخطار اختبار إلى عناوين البريد الإلكتروني التي حددتها.

• رسالة SMS

توييب رسالة SMS يتيح لك تكوين إرسال إخطارات بمختلف الأحداث عبر رسالة نصية قصيرة إلى هاتف محمول. يتم إرسال الرسائل النصية القصيرة عبر بوابة البريد.

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.

في حال تمكين خيار استخدام مصادقة ESMTP، يمكنك تحديد إعدادات مصادقة ESMTP في حقل اسم المستخدم وكلمة المرور. يكون هذا الخيار معطلاً بشكل افتراضي، وتكون إعدادات مصادقة ESMTP غير متوفرة

يمكنك تحديد إعدادات TLS للاتصال بخادم SMTP:

• لا تستخدم TLS

يمكنك تحديد هذا الخيار إذا كنت تريد تعطيل تشفير رسائل البريد الإلكتروني.

• استخدم TLS إن 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.

• استخدم TLS دوماً وتحقق من صحة شهادة الخادم

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 للاتصال TLS.

إذا قمت بتحديد قيمة استخدم TLS دوماً وتحقق من صحة شهادة الخادم 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 أيضاً تحديد شهادة لمصادقة العميل على خادم SMTP.

يمكنك تحديد ملف شهادة خادم SMTP بالنقر فوق رابط تحديد الشهادات :

يمكنك استلام ملف قائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى خادم الإدارة. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم SMTP موقعة أيضاً 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 المستلمون (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 حقل الموضوع، حدد موضوع البريد الإلكتروني.

في القائمة المنسدلة قالب الموضوع، حدد قالب موضوعك. متغير وفق القالب المحدد يُوضع في حقل الموضوع. يمكنك إنشاء موضوع بريد إلكتروني باختيار عدة قوالب للموضوع.

في حقل عنوان البريد الإلكتروني للمرسل: إذا لم يتم تحديد هذا الإعداد، فسيتم استخدام عنوان المستلم بدلاً من ذلك. تحذير: لا نوصي باستخدام عنوان بريد إلكتروني وهمي، حدد عنوان البريد الإلكتروني للمرسل. إذا تركت هذا الحقل فارغاً، سيتم استخدام عنوان المستلم افتراضياً. لا يُنصح باستخدام عناوين بريد إلكتروني وهمية.

في حقل أرقام هواتف مستلمي رسائل SMS، حدد أرقام الهواتف المحمولة لمستلمي إشعار SMS.

في حقل رسالة إخطار، حدد نصاً يحتوي على معلومات حول الحدث الذي يرسله التطبيق عند وقوع حدث. يمكن أن يشمل هذا النص معلومات 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 %100 CPU".

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: يرسل التطبيق إشعاراً تجريبياً 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. في حقل **الملف التنفيذي الذي سيتم تشغيله على خادم الإدارة عند وقوع حدث**، حدد المجلد واسم الملف الذي سيتم تشغيله. قبل تحديد الملف، **قم بإعداد الملف وحدد العناصر النائية** التي تحدد تفاصيل الحدث التي سيتم إرسالها في رسالة الإشعار. يجب أن يكون المجلد والملف اللذين تحددتهما موجودين على خادم الإدارة. انقر على **رابط تكوين حد الإخطارات الرقمي** يتيح لك تحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مدار الفاصل الزمني المحدد.

3. حدد إعدادات الإخطار في التثبيت.

4. انقر فوق الزر **موافق** 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 **تكوين الحدث** 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 العملية عبر تشغيل الملف التنفيذي. يجب أن يحتوي الملف التنفيذي على ملف تنفيذي آخر مع العناصر النائية للحدث ليتم ترحيله إلى المسؤول.

العناصر النائية لوصف حدث

وصف عنصر نائب	عنصر نائب
مستوى أهمية الحدث	%الخطورة%
اسم الجهاز الذي وقع عليه الحدث	%الكمبيوتر%
المجال	%المجال%
الحدث	%الحدث%
وصف الحدث	%DESCR%
الموقت الذي تم إنشاؤه	%RISE_TIME%
اسم المهمة	%KLCSAK_EVENT_TASK_DISPLAY_NAME%
عميل شبكة Kaspersky Security Center	%KL_PRODUCT%
رقم إصدار عميل الشبكة	%KL_VERSION%
عنوان IP	%HOST_IP%
عنوان IP للاتصال	%HOST_CONN_IP%

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 يشغل 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 (المراقبة والإبلاغ ← أخبار Kaspersky) يبيّنك 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 Security Center 14 Web Console، Kaspersky 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 **المراقبة والإبلاغ** ← **إعلامات Kaspersky**.

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 **المراقبة والإبلاغ** وأقسامه الفرعية.

4. انقر على زر **موافق**.

بهذا تم تحديد إعدادات أخبار Kaspersky.

تعطيل أخبار Kaspersky

قسم [أخبار Kaspersky](#) (المراقبة والإبلاغ ← أخبار Kaspersky) يبيّنك 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 نافذة التطبيق الرئيسية، انقر فوق أيقونة **الإعدادات** (⚙️) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **عام**، حدد القسم **إعلامات Kaspersky**.

3. بدل زر **التبديل** إلى وضع **الأخبار المتعلقة بالأمان معطل**.

4. انقر على زر **حفظ**.

بهذا تم تعطيل أخبار Kaspersky.

يتم تعطيل الأخبار التسويقية افتراضياً. أنت لا تتلقى أخبار تسويقية إلا إذا قمت بتمكين (KSN) Kaspersky Security Network. يمكنك تعطيل هذا النوع من الأخبار عن طريق تعطيل KSN.

لتعطيل الأخبار التسويقية:

1. في نافذة التطبيق الرئيسية، انقر فوق أيقونة **الإعدادات** (⚙️) بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **عام**، حدد قسم **إعدادات KSN**.

3. قم بتعطيل خيار عند تمكين هذا الخيار، يرسل Kaspersky Security Center إحصائياته إلى KSN كي يحللها محلو Kaspersky.

4. انقر على زر **حفظ**.

بهذا تم تعطيل الأخبار التسويقية.

عرض معلومات حول اكتشافات التهديدات

يمكنك تمكين أو تعطيل عرض المعلومات حول التنبيهات.

لتمكين أو تعطيل عرض قسم **التنبيهات** في القائمة الرئيسية:

1. في القائمة الرئيسية، انتقل إلى إعدادات حسابك وحدد **خيارات الواجهة**.

2. في نافذة **خيارات الواجهة** التي تفتح، قم بتمكين خيار **عرض تنبيهات EDR** أو تعطيله.

3. انقر فوق **حفظ**.

تعرض الوحدة القسم الفرعي **تنبيهات** في القسم **المراقبة والإبلاغ** من القائمة الرئيسية. في القسم الفرعي **التنبيهات**، يمكنك عرض معلومات حول اكتشاف التهديدات على أجهزة نقطة النهاية. إذا أضفت مفتاح ترخيص لـ **EDR الأمثل** ، فسيعرض Kaspersky Security Center 14 Web Console القسم الفرعي **التنبيهات تلقائيًا** في القسم **المراقبة والإبلاغ** من القائمة الرئيسية. يمكنك أيضًا **إضافة تطبيق مصغر** يعرض معلومات حول التنبيهات. وإذا ثبت أيضًا المكون الإضافي EDR الأمثل، فيمكنك عرض معلومات التفصيلية حول التهديدات المكتشفة بالنقر فوق رابط **المزيد من التفاصيل**.

تسجيل نشاط Kaspersky Security Center 14 Web Console

تسجيل نشاط Kaspersky Security Center 14 Web Console يمكن أن يساعد في تقصي أسباب خلل برنامج. عند الاتصال بالدعم الفني لـ Kaspersky بشأن عطل في Kaspersky Security Center 14 Web Console ، يمكن لمختصي الدعم الفني في Kaspersky طلب ملفات سجل Kaspersky Security Center 14 Web Console منك. تُخزن ملفات سجل Kaspersky Security Center 14 Web Console في المجلد `<Kaspersky Security Center 14 Web Console installation folder>/logs` طوال الوقت الذي تستخدم فيه التطبيق. لا يتم إرسال ملفات السجل إلى أخصائي الدعم الفني من تلقائيًا.

لتفعيل تسجيل نشاط Kaspersky Security Center 14 Web Console،

حدد خانة اختيار **تفعيل تسجيل أنشطة Kaspersky Security Center 14 Web Console** في النافذة إعدادات اتصال Kaspersky Security Center 14 Web Console في **معالج إعدادات 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

• **اسم المكون** هو اسم مكون Kaspersky Security Center أو اسم مكون الإدارة الإضافي لـ Kaspersky Security Center 14 Web Console.

• **اسم الجهاز** هو اسم الجهاز الذي يعمل عليه **اسم المكون**.

• **رقم مراجعة الملف** هو رقم ملف السجل الذي تم إنشاؤه لـ **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 ميغا بايت. يتم إنشاء مل سجل جديد عند الوصول إلى أقصى حجم. يتم وضع الرقم 1 في نهاية **رقم مراجعة الملف** لملف السجل.

• **YYYY MM و DD** 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 Kaspersky آخر، مثل Kaspersky Endpoint Detection and Response و Kaspersky Managed Detection and Response.

تكوين الوصول إلى KATA/KEDR Web Console

Kaspersky Anti Targeted Attack (KATA) و Kaspersky Endpoint Detection and Response (KEDR) هما جزآن عمليان في [Kaspersky Anti Targeted Attack Platform](#). يمكنك إدارة هذه الأجزاء العملية من خلال Web Console لمنصة Kaspersky Anti Targeted Attack Platform. إذا كنت تستخدم كلاً من Kaspersky Security Center 14 Web Console و Kaspersky Anti Targeted Attack Platform (KATA / KEDR Web Console)، فيمكنك تكوين الوصول إلى KATA / KEDR Web Console مباشرة من واجهة Kaspersky Security Center 14 Web Console.

لتكوين الوصول إلى KATA / KEDR Web Console:

1. في القائمة المنسدلة إعدادات وحدة التحكم، حدد **التكامل**.
سنتفتح نافذة إعدادات وحدة التحكم.

2. حدد **تبويب التكامل**.

3. في علامة التبويب **التكامل**، قم باختيار قسم **KATA**.

4. أدخل رابط URL الخاص بـ KATA/KEDR Web Console في حقل عنوان URL إلى KATA/KEDR Web Console.

5. انقر على زر **حفظ**.

يتم إضافة القائمة المنسدلة إدارة متقدمة إلى الجزء العلوي من نافذة التطبيق الرئيسية. يمكنك استخدام هذه القائمة في فتح KATA / KEDR Web Console. بعد أن تنقر على **الأمان عبر الإنترنت المتقدم**، سيفتح تبويب جديد في المستعرض الذي تستخدمه بالرابط الذي حددته.

جارٍ إنشاء اتصال في الخلفية

لتمكن Kaspersky Security Center 14 Web Console من أداء مهامها في الخلفية، فيجب عليك إنشاء اتصال في الخلفية بين Kaspersky Security Center Web Console و XADM الإدارة. يمكنك إنشاء هذا الاتصال فقط إذا كان حسابك له حق تعديل **قوائم التحكم في الوصول للكانين** مباشرة في المجال الوظيفي **الميزات العامة: أدوات المستخدم**.

إذا قمت بتهيئة المكون الإضافي لبرنامج Kaspersky Endpoint Security لنظام التشغيل Windows 11.9.0، أو إذا قمت بتحديث المكون الإضافي Kaspersky Endpoint Security لنظام التشغيل Windows من إصدار أقدم من 11.7 ولم يتم إنشاء اتصال في الخلفية بعد، فسيعرض إشعار بأنك أنشأت اتصالاً في الخلفية. سيتعين عليك أيضاً منح حساب الخدمة حقوق **الميزات العامة: العمليات في المجال الوظيفي** لخادم الإدارة.

لإنشاء اتصال في الخلفية:

1. في القائمة المنسدلة إعدادات وحدة التحكم، حدد **التكامل**.

سنتفتح نافذة إعدادات وحدة التحكم.

2. حدد **تبويب التكامل**.

3. في علامة التبويب **التكامل**، حدد القسم **التكامل**.

4. قم بتبديل زر التبديل الخاص بإنشاء اتصال في الخلفية إلى الوضع: إنشاء اتصال في الخلفية للتكامل مُمكن.

5. في قسم سيتم بدء الخدمة التي تنشئ اتصالاً في الخلفية على خادم Kaspersky Security Center Web Console المفتوح، انقر على زر موافق.

تم إنشاء الاتصال في الخلفية بين Kaspersky Security Center Web Console وخادم الإدارة. خادم الإدارة ينشئ حساباً 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 تلقائياً بتغيير كلمة مرور حساب الخدمة مرة واحدة كل 30 يوماً لأسباب أمنية. لا يمكنك حذف حساب الخدمة يدوياً. خادم الإدارة يحذف هذا الحساب تلقائياً عند تعطيل اتصال عبر الخدمات. خادم الإدارة ينشئ حساب خدمة واحد لكل وحدة تحكم في الإدارة ويعين جميع حسابات الخدمة لمجموعة الأمان التي تحمل الاسم ServiceNwcGroup. خادم الإدارة ينشئ مجموعة الأمان هذه تلقائياً أثناء عملية تثبيت Kaspersky Security Center. لا يمكنك حذف مجموعة الأمان هذه يدوياً.

تصدير الأحداث إلى أنظمة SIEM

يصف هذا القسم كيفية تكوين تصدير الأحداث إلى أنظمة SIEM.

السيناريو: تكوين تصدير الحدث إلى نظام SIEM

يسمح Kaspersky Security Center بالتكوين بإحدى الطرق التالية: التصدير إلى أي نظام SIEM يستخدم تنسيق Syslog أو التصدير إلى أنظمة QRadar و Splunk و ArcSight SIEM التي تستخدم تنسيقات LEEF و CEF أو تصدير الأحداث إلى أنظمة SIEM مباشرة من قاعدة بيانات Kaspersky Security Center. عند إكمال هذا السيناريو، يرسل خادم الإدارة الأحداث إلى نظام SIEM تلقائياً.

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 14 Web Console: [وضع علامة على أحداث تطبيق Kaspersky للتصدير بتنسيق Syslog](#)، ووضع علامة على الأحداث العامة للتصدير بتنسيق Syslog

- قم بتكوين تصدير الأحداث إلى نظام SIEM باستخدام إحدى الطرق التالية:

- استخدام TCP/IP أو UDP أو TLS من خلال بروتوكولات TCP. تعليمات للمساعدة:

■ وحدة تحكم الإدارة: [تكوين تصدير الأحداث إلى أنظمة SIEM](#)

■ [Kaspersky Security Center 14 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 للتصدير 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 الاستجابة السريعة لأحداث نظام الأمن التي تحدث في الأجهزة المدارة أو مجموعات الأجهزة.

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 بناءً 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.

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 خطيراً بالضرورة، غير أنه يشير إلى مشكلة محتملة في المستقبل. يتم تعيين معظم الأحداث كتحذيرات إذا كان من الممكن استعادة التطبيق بدون فقدان البيانات أو الإمكانات 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 مدة تخزين محددة، يمكنك خلالها عرضه في Kaspersky Security Center أو تعديله. لا يتم حفظ بعض البيانات في قاعدة بيانات خادم الإدارة بشكل افتراضي لأن مدة 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 تنشأها 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 أيضاً وظيفة تجميع البيانات التي تم رصدها لمساعدتك في تجنب فقدان الأحداث الحرجة. إضافة إلى ذلك، تُجري الأنظمة تحليلاً تلقائياً 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 الموافقة على التحديثات [عبر وحدة تحكم الإدارة](#) أو [عبر Kaspersky Security Center 14 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 و LEEF إلى أنظمة QRadar و Splunk و ArcSight.
يمكنك استخدام بروتوكولي CEF و LEEF لتصدير الأحداث العامة. عند تصدير الأحداث عبر بروتوكولات CEF و LEEF، فلن يكون لديك إمكانية تحديد أحداث محددة لتصديرها. وبدلاً من ذلك، يتم تصدير جميع الأحداث العامة. خلافاً لبروتوكول Syslog، لا تعتبر البروتوكولات CEF و LEEF بروتوكولات عامة. تكون البروتوكولات CEF و LEEF مخصصة لأنظمة SIEM المناسبة (QRadar و Splunk و ArcSight). لذا، عند اختيارك لتصدير الأحداث عبر واحد من هذه البروتوكولات، فستستخدم المحلل المطلوب في نظام SIEM.

لتصدير الأحداث عبر بروتوكولات CEF و LEEF، يجب تنشيط ميزة التكامل مع أنظمة SIEM في خادم الإدارة باستخدام [مفتاح ترخيص نشط أو رمز تنشيط صالح](#).

- 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](#)

هذا هو بروتوكول نقل الرسالة، إما أن يكون TCP/IP أو UDP. يجب أن يكون هذا البروتوكول مطابقاً لما حددته في Kaspersky Security Center.

- [المنفذ](#)

رقم المنفذ للاتصال بـ Kaspersky Security Center. يجب أن يكون هذا المنفذ مطابقاً 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 وفقاً 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.

Edit Receiver

If a source type that you need does not exist in the Source Type dropdown list below, go to the [Source Types](#) page to add it.

Name: tcp cef

IP/Host: All

Port: 616

Encoding: UTF-8

Source Type: CEF

Enable:

Save Cancel

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 محلات الرسالة جزءًا من نظام SIEM، إذ تُستخدم لتجزئة محتويات الرسالة في الحقول ذات الصلة، مثل معرف الحدث والخطورة والوصف والمعلومات وما إلى ذلك. يتيح هذا الإجراء لنظام SIEM معالجة الأحداث المستلمة من Kaspersky Security Center حتى يمكن تخزينها في قاعدة بيانات نظام SIEM.

يحتوي كل نظام من أنظمة SIEM على مجموعة من محلات الرسالة القياسية. يوفر Kaspersky أيضًا محلات الرسالة لبعض أنظمة SIEM، على سبيل المثال، QRadar و ArcSight. يمكنك تنزيل هذه الرسائل من مواقع ويب أنظمة SIEM المطابقة. عند تكوين المستلم، يمكنك استخدام أحد محلات الرسالة القياسية أو محلل رسالة من Kaspersky.

وضع علامة على الأحداث للتصدير إلى أنظمة SIEM بتنسيق Syslog

يصف هذا القسم كيفية وضع علامة على الأحداث لتصدير المزيد منها إلى أنظمة SIEM بتنسيق Syslog.

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 **الأجهزة** ← **السياسات وملفات التعريف**.
2. انقر على سياسة التطبيق الذي تريد تحديد الأحداث الخاصة به.
ستفتح نافذة إعدادات السياسة.
3. انتقل إلى قسم **تكوين الحدث**.
4. حدد خانة الاختيار الموجودة بجوار الأحداث التي ترغب في تصديرها إلى نظام SIEM.
5. انقر على الزر **وضع علامة على التصدير إلى نظام SIEM باستخدام Syslog**.

يمكنك أيضاً تحديد حدث للتصدير إلى نظام SIEM في القسم، **تسجيل الحدث** 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 **حفظ**.

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 مسبقاً 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 **الأجهزة** ← **الأجهزة المُدارة**.
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 **التطبيقات**.
4. انقر فوق الرابط الذي يحمل اسم التطبيق المطلوب في قائمة التطبيقات.
5. انتقل إلى قسم **تكوين الحدث**.
6. حدد خانة الاختيار الموجودة بجوار الأحداث التي ترغب في تصديرها إلى SIEM.
7. انقر على الزر **وضع علامة على التصدير إلى نظام SIEM باستخدام Syslog**.

ويمكنك أيضاً وضع علامة على حدث للتصدير إلى نظام SIEM في القسم **تسجيل الحدث** 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 فصاعداً، 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:

- انقر فوق أيقونة الإعدادات (⚙️) المجاورة لاسم خادم الإدارة المطلوب.
- انتقل إلى الأجهزة ← السياسات وملفات التعريف، ثم انقر فوق رابط السياسة.

2. في النافذة التي تفتح، انقر فوق علامة التبويب تكوين الحدث.

3. انقر على وضع علامة على التصدير إلى نظام SIEM باستخدام Syslog.

ويمكنك أيضاً وضع علامة على حدث للتصدير إلى نظام SIEM في القسم تسجيل الحدث، 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 فصاعداً، 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 مسبقاً، ولا يمكنك تحديد أحداث لتصديرها.

لتصدير الأحداث عبر بروتوكولات CEF وLEEF، يجب تنشيط ميزة التكامل مع أنظمة SIEM في خادم الإدارة باستخدام [مفتاح ترخيص نشط أو رمز تنشيط صالح](#).

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 (Log Event Extended Format) - تنسيق حدث مخصص لـ IBM Security QRadar SIEM. 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.

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.

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 المعيار [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

توضح هذه المقالة كيفية تكوين تصدير الأحداث إلى أنظمة SIEM.

لتكوين التصدير إلى أنظمة SIEM في Kaspersky Security Center 14 Web Console:

1. في القائمة المنسدلة إعدادات وحدة التحكم، حدد التكامل.

سنتفتح نافذة إعدادات وحدة التحكم.

2. حدد تبويب التكامل.

3. في تبويب التكامل، حدد قسم SIEM.

4. انقر على الرابط إعدادات.

يفتح قسم إعدادات التصدير.

5. قم بتحديد الإعدادات التالية في القسم إعدادات التصدير:

• [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 نظام SIEM](#)

رقم المنفذ المستخدم لإنشاء اتصال بين Kaspersky Security Center و خادم نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center وفي إعدادات المستلم لنظام SIEM الخاص بك.

• البروتوكول 9

حدد البروتوكول الذي سيستخدم لنقل الرسائل إلى نظام SIEM. يمكنك تحديد إما بروتوكول TCP/IP، أو UDP أو TLS من خلال بروتوكول TCP.

حدد إعدادات TLS التالية إذا قمت بتحديد TLS عبر بروتوكول TCP:

• مصادقة الخادم

في حقل مصادقة الخادم، يمكنك تحديد قيم الشهادات الموثوق بها أو بصمات أصابع SHA:

- **شهادات موثوقة.** يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى Kaspersky Security Center. يتحقق Kaspersky Security Center مما إذا كانت شهادة خادم نظام SIEM موقعة أيضًا من قبل مرجع مصدق موثوق أم لا. لإضافة شهادة موثوقة، انقر فوق الزر **تصفح ملف شهادات CA**، ثم قم بتحميل الشهادة.
- **بصمات SHA.** يمكنك تحديد بصمات الإبهام SHA-1 لشهادات نظام SIEM في Kaspersky Security Center. لإضافة بصمة إبهام SHA-1، أدخلها في حقل **بصمات الإبهام**، ثم انقر فوق الزر **إضافة**.

باستخدام إعداد **إضافة مصادقة العميل**، 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.

• أضف اسم الموضوع/الاسم البديل للموضوع

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 **أضف اسم الموضوع/الاسم البديل للموضوع**. إذا تطابق أي من أسماء الموضوعات المحددة مع اسم موضوع شهادة نظام SIEM، فسيتحقق Kaspersky Security Center من صحة شهادة خادم نظام SIEM.

• إضافة مصادقة العميل

لمصادقة العميل، يمكنك إدخال شهادتك أو إنشائها في Kaspersky Security Center.

- **أدخل شهادة.** 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 شهادة PEM.** قم بتحميل ملف بشهادة في الحقل **ملف مع شهادة**، وملف بمفتاح خاص في الحقل **ملف مع مفتاح**. 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 **التحقق من كلمة المرور أو الشهادة**. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- **X.509 شهادة PKCS12.** قم بتحميل ملف واحد يحتوي على شهادة ومفتاحها الخاص في الحقل **ملف مع شهادة**. عند تحميل الملف، حدد كلمة المرور لفك تشفير المفتاح الخاص في حقل **التحقق من كلمة المرور أو الشهادة**. يمكن أن تحتوي كلمة المرور على قيمة فارغة إذا لم يتم تشفير المفتاح الخاص.

- **إنشاء مفتاح.** 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.

• تنسيق البيانات 9

يمكنك تحديد تنسيقات Syslog أو CEF أو LEEF، وفقاً لمتطلبات نظام SIEM.

إذا قمت بتحديد تنسيق Syslog، فيجب عليك تحديد:

• الحد الأقصى لرسالة الحدث بالبايت

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 التنسيق Syslog في حقل البروتوكول.

6. عليك تبديل الخيار إلى الوضع تصدير الأحداث إلى قاعدة بيانات نظام SIEM تلقائيًا مُمْكَّن.

7. انقر على زر حفظ.

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 هذه آراء الجمهور في وثيقة 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 لإنشاء استعلام SQL بواسطة أداة klsq2 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 الممثل واسم قاعدة البيانات، في [القسم المقابل](#).

إنشاء استعلام SQL باستخدام أداة klsq2 المساعدة

يوضح هذا القسم كيفية تنزيل أداة klsq2 المساعدة واستخدامها، وكيفية إنشاء استعلام SQL باستخدام هذه الأداة المساعدة. عندما تقوم بإنشاء استعلام SQL بواسطة أداة klsq2 المساعدة، لا يتعين عليك توفير اسم قاعدة البيانات ومعلمات الوصول، لأن الاستعلام يتعامل مع الرؤية العامة لـ Kaspersky Security Center بشكل مباشر.

لتنزيل أداة klsq2 المساعدة واستخدامها:

1. تنزيل klakdb.chm/utility من الموقع الإلكتروني لـ Kaspersky.

2. انسخ ملف klsq2.zip الذي تم تنزيله وفك ضغطه في أي مجلد على الجهاز المثبت عليه خادم إدارة Kaspersky Security Center.

تشتمل حزمة klsql2.zip على الملفات التالية:

- klsql2.exe
- src.sql
- start.cmd

3. افتح ملف src.sql في أي محرر نصوص.

4. في ملف src.sql، اكتب الاستعلام الذي تريده. ثم احفظ الملف.

5. في الجهاز المثبت عليه خادم إدارة Kaspersky Security Center، في سطر الأوامر، اكتب الأمر التالي لتشغيل استعلام SQL من الملف src.sql واحفظ النتائج على الملف result.xml:

```
klsql2 -i src.sql -o result.xml
```

6. افتح الملف result.xml الذي تم إنشاؤه حديثاً لعرض نتائج الاستعلام.

يمكنك تحرير الملف src.sql وإنشاء أي استعلام للرؤى العامة. بعد ذلك، من سطر الأوامر، قم بتنفيذ استعلامك واحفظ النتائج على ملف.

مثال لاستعلام SQL في أداة klsql2 المساعدة

يعرض هذا القسم مثالاً لاستعلام SQL، الذي يتم إنشاؤه بواسطة أداة klsql2 المساعدة.

يوضح المثال التالي استعادة الأحداث التي حدثت في الأجهزة خلال السبعة أيام الماضية، وعرض للأحداث التي طُلبت وقت حدوثها، ويتم عرض الأحداث الأخيرة أولاً.

مثال:

```
تحديد
e.nId , /* معرّف الحدث */
e.tmRiseTime /* الوقت، وقت وقوع الحدث.
e.strEventType /* الاسم الداخلي لنوع الحدث */
e.wstrEventTypeDisplayName /* الاسم المعروف للحدث */
e.wstrDescription /* الوصف المعروف للحدث */
e.wstrGroupName /* اسم المجموعة حيث يوجد الجهاز */
h.wstrDisplayName /* الاسم المعروف للجهاز الذي وقع عليه الحدث */
+ '.' + ((CAST(((h.nIp / 16777216) & 255) AS varchar(4
+ '.' + ((CAST(((h.nIp / 65536) & 255) AS varchar(4
+ '.' + ((CAST(((h.nIp / 256) & 255) AS varchar(4
*/CAST(((h.nIp) & 255) AS varchar(4)) as strIp عنوان IP للجهاز الذي وقع عليه
الحدث */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
(())WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE
ORDER BY e.tmRiseTime DESC
```

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.

إذا تم استلام الأحداث المرسلّة 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.

Time (Event Time)	Device	Logger	deviceVendor	deviceProduct	deviceVersion
2017/01/24 17:27:11 MSK	mikrotik_admin.avp.ru [tcp.cel]	Local	KasperskyLab	SecurityCenter	10.4.343
2017/01/24 17:26:41 MSK	mikrotik_admin.avp.ru [tcp.cel]	Local	KasperskyLab	SecurityCenter	10.4.343

مثال للأحداث

العمل باستخدام Kaspersky Security Center 14 Web Console في بيئة السحابة

يوفر هذا القسم معلومات حول ميزة Kaspersky Security Center 14 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.

معالج تكوين بيئة سحابة Kaspersky Security Center 14 Web Console

لتكوين Kaspersky Security Center باستخدام هذا المعالج، يجب أن تمتلك ما يلي:

- بيانات اعتماد محددة لبيئة السحابة:

- [دور IAM الذي تم منحه حق استقضاء قطاع السحابة](#) أو [حساب مستخدم IAM الذي تم منحه حق استقضاء قطاع السحابة](#) (للمعمل مع Amazon Web Services)

- [معرف تطبيق Azure](#)، وكلمة المرور، والاشتراك (للمعمل في بيئة السحابة لـ Microsoft Azure)

- [البريد الإلكتروني لعميل Google](#) ومعرف المشروع والمفتاح الخاص (للمعمل مع Google Cloud)

- المكون الإضافي في Kaspersky Endpoint Security for Linux (مكون Web Console الإضافي)

- المكون الإضافي في Kaspersky Endpoint Security for Windows (مكون Web Console الإضافي)

- عمل الشبكة لنظام التشغيل Windows

• عميل الشبكة لنظام التشغيل Linux

• حزمة التثبيت لـ Kaspersky Endpoint Security for Linux

• حزمة التثبيت لـ Kaspersky Security for Windows Server

سيبدأ تشغيل معالج 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 معالج تكوين بيئة السحابة يدويًا في أي وقت.

لبدء تشغيل معالج تكوين بيئة السحابة يدويًا،

في القائمة الرئيسية، انتقل **الاكتشاف والنشر** ← **التوزيع والتعيين** ← **معالج تكوين بيئة السحابة**.

سيبدأ المعالج.

يستمر متوسط جلسة العمل مع هذا المعالج 15 دقيقة تقريبًا.

الخطوة 1. قراءة المعلومات حول المعالج

اقرأ عن معالج تكوين بيئة السحابة في صفحة الترحيب ثم انقر على **التالي** للمتابعة.

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 **التالي** 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:

• **بيئة السحابة**

حدد بيئة السحابة التي تقوم فيها بنشر AWS Kaspersky Security Center أو Azure. إذا كنت تخطط للعمل مع أكثر من بيئة سحابية واحدة، حدد بيئة واحدة ثم قم بتشغيل المعالج مرة أخرى.

• اسم الاتصال ⑤

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفاً. 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:

• تم تعيين دور AWS IAM لمثيل EC2

حدد هذا الخيار إذا كان لديك دور IAM بالحقوق المطلوبة لخادم الإدارة.

• مستخدم AWS IAM

حدد هذا الخيار إذا كان لديك مفتاح وصول AWS IAM. أدخل بيانات مفاتيحك:

• معرف مفتاح الوصول ⑤

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 للتحويل بدلاً من دور IAM.

• المفتاح السري ⑤

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 للتحويل بدلاً من دور IAM.

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **إظهار**.

Azure

إذا قمت بتحديد Azure لتكون نوع قطاع السحابة، حدد الإعدادات التالية للاتصال الذي سيتم استخدامه لاستقصاء قطاع السحابة بعد ذلك:

• معرف تطبيق Azure ⑤

لقد قمت [بانشاء](#) 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 أولاً بحذف اتصال Azure الموجود.

• [معرفة 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.

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر إظهار.

• [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 إظهار.

Google Cloud

إذا حددت Google Cloud ليكون نوع قطاع السحابة، حدد الإعدادات التالية للاتصال الذي سيتم استخدامه لاستقصاء قطاع السحابة بعد ذلك:

• [عنوان البريد الإلكتروني للعميل](#)

البريد الإلكتروني للعميل هو عنوان البريد الإلكتروني الذي استخدمته لتسجيل مشروعك في Google Cloud.

• [مُعرّف المشروع](#)

معرّف المشروع هو المعرف الذي استلمته عند تسجيل مشروعك في Google Cloud.

• [المفتاح الخاص](#)

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 إظهار.

يتم حفظ الاتصال الذي حددته في إعدادات التطبيق.

معالج تكوين بيئة السحابة يسمح لك بتحديد قطاع واحد فقط. يمكنك بعد ذلك تحديد المزيد من الاتصالات لإدارة قطاعات السحابة الأخرى.

انقر على التالي للمضي قدماً.

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:

• [مزامنة مجموعات الإدارة مع بنية 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، فسيقوم المعالج بإنشاء مهمة لتثبيت تطبيقات أمان 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 أدوات لتثبيت التطبيقات على مثيلات EC2 أو على الأجهزة الظاهرية لـ Azure، يمكنك تكوين مهمة [التثبيت عن بُعد](#) يوميًا 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 يوميًا في وقت لاحق.

إذا قمت بتحديد خيار نشر الحماية، سيصبح قسم [إعادة تشغيل الأجهزة](#) متاحًا. في هذا القسم، يجب عليك اختبار 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:

• [لا تقم بإعادة التشغيل](#)

في حالة تحديد هذا الخيار، لن يتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

• [إعادة التشغيل](#)

في حالة تحديد هذا الخيار، فستتم إعادة تشغيل الجهاز بعد تثبيت تطبيق الأمان.

انقر على التالي للمضي قدمًا.

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 لصالح Kaspersky Security Center

حدد إعدادات ترحيل المعلومات حول عمليات Kaspersky Security Center إلى قاعدة معارف Kaspersky Security Network (KSN). حدد أحد الخيارات التالية:

• [أوافق على استخدام شبكة Kaspersky Security Network](#)

سيقوم Kaspersky Security Center والتطبيقات المدارة المثبتة على الأجهزة العملية بنقل تفاصيل عملياته تلقائيًا إلى [Kaspersky Security Network](#). تتضمن 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.

يمكن كذلك عرض اتفاقيات KSN للتطبيقات المدارة. 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 التالي للمضي قدماً.

الخطوة 6. إنشاء تكوين أولي للحماية

يمكنك التحقق من قائمة بالسياسات والمهام التي تم إنشاؤها.

انتظر حتى يكتمل إنشاء السياسات والمهام ثم انقر على التالي للمتابعة. في آخر صفحة من المعالج، انقر على زر إنهاء للخروج.

استنقصاء مقطع الشبكة عبر Kaspersky Security Center 14 Web Console

يتم استلام معلومات حول بنية الشبكة (والأجهزة فيها) عن طريق خادم الإدارة من خلال الاستنقصاء 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 المدارة. إذا قمت بتكوين الأجهزة التي سيتم نقلها إلى مجموعات الإدارة تلقائيًا، سيتم تضمين الأجهزة التي تم اكتشافها في مجموعات الإدارة.

للسماح لخادم الإدارة باستنقصاء 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 الاستنقصاء لكل قطاع سحابة.

إضافة اتصالات لاستقصاء قطاع السحابة

لإضافة اتصال لاستقصاء قطاع السحابة لقائمة الاتصالات المتاحة:

1. في القائمة الرئيسية، انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **السحابة**.
2. في النافذة التي تفتح، انقر على **خصائص**.
3. في نافذة إعدادات التي تفتح، انقر على **إضافة**.
سنفتح نافذة إعدادات قطاع السحابة.
4. حدد اسم بيئة السحابة للاتصال الذي سيتم استخدامه لإجراء المزيد من الاستقصاءات على قطاع السحابة:

• **بيئة السحابة**

حدد بيئة السحابة التي تقوم فيها بنشر AWS Kaspersky Security Center أو Azure. إذا كنت تخطط للعمل مع أكثر من بيئة سحابية واحدة، حدد بيئة واحدة ثم قم بتشغيل المعالج مرة أخرى.

• **اسم الاتصال**

أدخل اسم للاتصال. لا يمكن أن يتضمن الاسم أكثر من 256 حرفاً. لا يُسمح إلا بحروف Unicode كما سيتم استخدام هذا الاسم بوصفه اسم مجموعة إدارة أجهزة السحابة. إذا كنت تخطط للعمل مع أكثر من بيئة سحابية 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:

• **استخدام دور AWS IAM**

حدد هذا الخيار إذا قمت بالفعل بإنشاء دور IAM لخادم الإدارة لـ **استخدم خدمات AWS**.

• **بيانات اعتماد حساب مستخدم AWS IAM**

حدد هذا الخيار إذا كان لديك **حساب مستخدم IAM** لديه **الأذونات المطلوبة** ويمكنك إدخال معرف مفتاح والمفتاح السري.

إذا حددت أنك تملك بيانات اعتماد حساب مستخدم AWS IAM، حدد ما يلي:

• **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 للتحويل بدلاً من دور IAM.

• **المفتاح السري**

المفتاح السري الذي تلقينته مع معرف مفتاح الوصول [عند إنشاء 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 للتحويل بدلاً من دور IAM.

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **إظهار**.

• إذا حددت Azure، فحدد الإعدادات التالية:

• **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 أولاً 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** متاحاً. انقر مع الاستمرار فوق هذا الزر لإظهار الحروف التي أدخلتها.

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **إظهار**.

• **اسم حساب تخزين Azure**

لقد قمت بإنشاء اسم [حساب تخزين Azure](#) لاستخدام Kaspersky Security Center.

• **مفتاح الوصول إلى مخزن Azure**

لقد حصلت على كلمة المرور (المفتاح) عند إنشاء حساب تخزين Azure لاستخدام Kaspersky Security Center.
يكون المفتاح متاحاً في القسم "نظرة عامة على حساب تخزين Azure"، في القسم الفرعي "المفاتيح".

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **إظهار**.

إذا حددت Google Cloud، فحدد الإعدادات التالية:

• **عنوان البريد الإلكتروني للعميل**

البريد الإلكتروني للعميل هو عنوان البريد الإلكتروني الذي استخدمته لتسجيل مشروعك في Google Cloud.

• **مُعزف المشروع**

معرف المشروع هو المعرف الذي استلمته عند تسجيل مشروعك في Google Cloud.

• [المفتاح الخاص](#) 5

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 إظهار.

6. يمكنك إذا كنت ترغب النقر على [تعيين جدول الاستقصاء 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 أدونات استقصاء قطاع سحابة قد تم نقلها إلى مستخدم آخر يملك بيانات اعتماد مختلفة.

لحذف اتصال:

1. في القائمة الرئيسية، انتقل إلى [الاكتشاف والنشر](#) ← [اكتشاف](#) ← [السحابة](#).

2. في النافذة التي تفتح، انقر على [خصائص](#).

3. في نافذة [إعدادات](#) التي تفتح، انقر على اسم القطاع الذي ترغب في حذفه.

4. انقر على [حذف](#).

5. في النافذة التي تفتح انقر على زر [موافق](#) 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 14 Web Console

يتم تنفيذ استقصاء قطاع السحابة وفقًا لجدول. يمكنك إعداد تكرار الاستقصاء.

يتم إعداد تكرار الاستقصاء تلقائيًا في غضون 5 دقائق بواسطة معالج 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 الاكتشاف والنشر ← اكتشاف ← السحابة.

2. في النافذة التي تفتح، انقر على خصائص.

3. في نافذة إعدادات التي تفتح، انقر على اسم القطاع الذي ترغب في تكوين جدول استقصاء له. سيفتح هذا نافذة إعدادات قطاع السحابة.

4. في النافذة إعدادات قطاع السحابة، انقر على زر تعيين جدول الاستقصاء. يؤدي ذلك إلى فتح نافذة الجدول.

5. في نافذة الجدول، حدد الإعدادات التالية:

• **البداية المُجدول**

خيارات جدول الاستقصاء:

• **كل N أيام**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالأيام، بدايةً من الوقت والتاريخ المحددين. بشكل افتراضي، يعمل الاستقصاء كل يوم، بدايةً من التاريخ والوقت الحاليين للنظام.

• **كل N دقيقة**

يعمل الاستقصاء بشكلٍ منتظم، حسب الفاصل الزمني المحدد بالدقائق، بدايةً من الوقت المحدد. بشكلٍ افتراضي، يعمل الاستقصاء كل خمس دقائق، بدايةً 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 6:00:00 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 6:00:00 مساءً.

• **موعد البدء (بالدقائق)**

حدد قيمة ن (لدقائق أو أيام).

• **بدءاً من**

حدد متى يبدأ أول استقصاء.

• **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 على **حفظ** لحفظ التغييرات.

يتم تكوين جدول الاستقصاء للقطاع وحفظه.

عرض نتائج استقصاء قطاع السحابة عبر Kaspersky Security Center 14 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 **الاكتشاف والنشر** ← **اكتشاف** ← **السحابة**.

يعرض هذا قطاعات السحابة المتوفرة للاستقصاء.

عرض خصائص الأجهزة السحابية عبر Kaspersky Security Center 14 Web Console

يمكنك عرض خصائص كل جهاز سحابة.

لعرض خصائص جهاز السحابة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **الأجهزة المُدارة**.

2. انقر على اسم الجهاز الذي ترغب في عرض خصائصه.

سنفتح نافذة خصائص مع قسم عام محدد.

3. إذا كنت ترغب في عرض الخصائص المحددة لأجهزة السحابة، حدد قسم **النظام** 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 المثليل 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 القاعدة المتحركة

أثناء تشغيل معالج تكوين بيئة السحابة، سيتم إنشاء القاعدة مزمنة 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 الاكتشاف والنشر ← التوزيع والتعيين ← قواعد النقل. يفتح هذا قائمة بقواعد النقل.

2. في قائمة قواعد النقل، حدد المزامنة مع السحابة. يفتح هذا نافذة خصائص القاعدة.

3. يمكنك عند الضرورة تحديد الإعدادات التالية في تبويب حالات القاعدة في تبويب قطاعات السحابة:

• الجهاز موجود ضمن 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 9

إذا تم تمكين هذا الخيار، فستنقل 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 تفرع لاحق. يتم تمكين هذا الخيار افتراضيًا.

• إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثًا 9

إذا تم تمكين هذا الخيار، في حالة عدم اشتغال 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 المُدارة/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 9

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 بتفعيل خيار مزامنة مجموعات الإدارة مع بنية السحابة عند استخدام معالج تكوين بيئة السحابة، يتم إنشاء قاعدة المزامنة مع السحابة مع تفعيل خيار إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثًا وخيار حذف المجموعات الفرعية التي لم يتم العثور على تطابق لها في قطاعات السحابة. إذا لم يتم تفعيل خيار مزامنة مجموعات الإدارة مع بنية السحابة، سيتم إنشاء قاعدة المزامنة مع السحابة بحيث تكون هذه الخيارات معطلة (تم إلغاء تحديدها). إذا كان عمالك مع Kaspersky Security Center يتطلب أن تتوافق بنية المجموعات الفرعية في المجموعة الفرعية الأجهزة المُدارة/السحابة مع بنية قطاعات السحابة، قم بتمكين خيار إنشاء مجموعات فرعية مقابلة لحاويات الأجهزة المكتشفة حديثًا وخيار حذف المجموعات الفرعية التي لم يتم العثور على تطابق لها في قطاعات السحابة في خصائص القاعدة ثم قم بفرض القاعدة.

4. في القائمة المنسدلة تم اكتشاف الجهاز باستخدام واجهة برمجة التطبيقات، حدد إحدى القيم التالية:

- لا. لا يمكن اكتشاف الجهاز باستخدام AWS API أو Azure API أو Google API، أي أنه يوجد خارج بيئة السحابة أو يوجد في بيئة السحابة ولكن لا يمكن اكتشافه باستخدام 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، أي أن الجهاز موجود بالفعل في بيئة Google cloud.
- دون قيمة. يتعدى تطبيق هذا المعيار.

5. إن لزم الأمر، قم بإعداد خصائص قاعدة أخرى في الأقسام الأخرى.

تم تكوين قاعدة النقل.

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 الأجهزة ← المهام.

2. انقر فوق إضافة.

يبدأ تشغيل معالج إضافة مهمة.

3. في الصفحة الأولى من المعالج في قائمة التطبيق، حدد 14 Kaspersky Security Center، وفي قائمة نوع المهمة حدد النسخ الاحتياطي لبيانات خادم الإدارة.

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 إنشاء 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 تلقيتته مع معرف مفتاح الوصول عند إنشاء 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 للتحويل 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 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 5

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 أولاً بحذف اتصال Azure الموجود.

• اسم خادم Azure SQL Server 5

يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

• مجموعة مورد خادم Azure SQL Server 5

يكون الاسم ومجموعة الموارد متاحان في خصائص خادم Azure SQL Server الخاص بك.

• مفتاح وصول تخزين Azure 5

يكون متاحًا في خصائص حساب التخزين الخاص بك، في قسم مفاتيح الوصول. يمكنك استخدام أي من المفاتيح (المفتاح 1 أو المفتاح 2).

يتم إنشاء المهمة وعرضها في قائمة المهام. إذا كنت تفعل خيار فتح تفاصيل المهمة عند اكتمال الإنشاء، 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 بُعد للتنفيذ عن بُعد للعمليات التالية على أجهزة العميل:

- 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.

يتم إجراء التشخيص عن بُعد باستخدام خادم الإدارة.

فتح نافذة التشخيص عن بُعد

لإجراء التشخيص عن بُعد على جهاز عميل، عليك أولاً فتح نافذة التشخيص عن بُعد.

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، فانتقل إلى الأجهزة ← الأجهزة المُدارة.
- إذا كان الجهاز ينتمي إلى مجموعة الأجهزة غير المخصصة، انتقل إلى الاكتشاف والنشر ← الأجهزة غير المخصصة.

2. انقر على اسم الجهاز المطلوب.

3. في نافذة خصائص الجهاز التي تفتح، حدد تبويب خيارات متقدمة.

4. في النافذة التي تفتح، انقر على تشخيصات عن بُعد.

يؤدي هذا إلى فتح نافذة تشخيصات عن بُعد لجهاز عميل.

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 التشخيص عن بُعد، انقر على تشخيصات عن بُعد.

3. في نافذة الحالات والسجلات التي تفتح، حدد قسم تطبيقات Kaspersky.

يؤدي هذا إلى فتح قائمة تطبيقات Kaspersky المثبتة على الجهاز.

4. في قائمة التطبيقات، حدد التطبيق الذي ترغب في تمكين التتبع أو تعطيله له.

يتم عرض قائمة خيارات التشخيص عن بُعد.

5. إذا كنت ترغب في تفعيل التتبع:

a. في قسم التتبع من القائمة، انقر على تمكين التتبع.

b. في النافذة تعديل مستوى التتبع التي تفتح، نوصي بإبقاء القيم الافتراضية للإعدادات. عند الضرورة، سيقوم أخصائي الدعم الفني بإرشادك خلال عملية التكوين. تتوفر الإعدادات التالية:

• مستوى التتبع 5

يحدد مستوى التتبع مقدار التفاصيل التي يحتويها ملف التتبع.

• [التتبع القائم على التدوير](#) 5

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 فوق **حفظ**.

يتم تفعيل التتبع للتطبيق المحدد. في بعض الحالات، يجب إعادة تشغيل تطبيق الأمان والمهمة التابعة له ليتم تمكين التتبع.

6. إذا كنت ترغب في تعطيل التتبع للتطبيق المحدد، انقر على **تعطيل التتبع**.

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 تتبع Xperf وتكوينه:

1. [افتح نافذة التشخيص عن بُعد لجهاز عميل](#).

2. في نافذة التشخيص عن بُعد، انقر على **تشخيصات عن بُعد**.

3. في نافذة الحالات والسجلات التي تفتح، حدد قسم **تطبيقات Kaspersky**.

يؤدي هذا إلى فتح قائمة تطبيقات Kaspersky المثبتة على الجهاز.

4. في قائمة التطبيقات، حدد Kaspersky Endpoint Security for Windows.

يتم عرض قائمة خيارات التشخيص عن بُعد لـ Kaspersky Endpoint Security for Windows.

5. في قسم **تتبع Xperf** من القائمة، انقر على **تمكين تتبع Xperf**.

إذا كان تتبع Xperf ممكنًا بالفعل/ يتم عرض زر **تعطيل تتبع Xperf** بدلاً من ذلك.

6. في نافذة **تغيير مستوى تتبع Xperf** التي تفتح، واستنادًا إلى طلب أخصائي الدعم الفني، افعل أحد الإجراءات التالية:

a. حدد أحد مستويات التتبع التالية:

• [مستوى سطحي](#) 5

يحتوي ملف التتبع من هذا النوع على الحد الأدنى لمقدار المعلومات حول النظام.

يتم تحديد هذا الخيار افتراضيًا.

• [مستوى عميق](#) 5

يحتوي ملف التتبع من هذا النوع على معلومات مفصلة مقارنة بملفات التتبع من النوع البسيط، وقد يطالبك أخصائي الدعم الفني بتحديدته 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:

• النوع الرئيسي ٩

يتم استقبال معلومات التتبع أثناء تشغيل تطبيق Kaspersky Endpoint Security. يتم تحديد هذا الخيار افتراضياً.

• النوع القائم على إعادة التشغيل ٩

يتم استقبال معلومات التتبع عند بدء تشغيل نظام التشغيل على الجهاز المُدار. يكون نوع التتبع هذا فعالاً عند حدوث المشكلة التي تؤثر على أداء النظام بعد تشغيل الجهاز وقبل بدء تشغيل Kaspersky Endpoint Security.

قد تتم مطالبتك أيضاً بتمكين الخيار **حجم ملف التدوير بالميجابايت** 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 فوق **حفظ**.

تم تمكين تتبع Xperf وتكوينه.

لتعطيل تتبع Xperf:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.

2. في نافذة التشخيص عن بُعد، انقر على **تشخيصات عن بعد**.

3. في نافذة **الحالات والسجلات** التي تفتح، حدد قسم **تطبيقات Kaspersky**.

يؤدي هذا إلى فتح قائمة تطبيقات Kaspersky المثبتة على الجهاز.

4. في قائمة التطبيقات، حدد **Kaspersky Endpoint Security for Windows**. يتم عرض خيارات التتبع لـ Kaspersky Endpoint Security for Windows.

5. في قسم **تتبع Xperf** من القائمة، انقر على **تعطيل تتبع Xperf**.

إذا كان تتبع Xperf معطلاً بالفعل، سيتم عرض زر **تمكين تتبع Xperf** بدلاً من ذلك.

تم تعطيل تتبع Xperf.

تنزيل ملفات التتبع لتطبيق

لتنزيل ملف التتبع لتطبيق:

1. افتح نافذة التشخيص عن بُعد لجهاز عميل.

2. في نافذة التشخيص عن بُعد، انقر على **تشخيصات عن بعد**.

3. في نافذة **الحالات والسجلات** التي تفتح، حدد قسم **تطبيقات Kaspersky**.

يؤدي هذا إلى فتح قائمة تطبيقات Kaspersky المثبتة على الجهاز.

في قسم **التتبع**، انقر على زر **ملفات التتبع**.

يفتح هذا نافذة **سجلات تتبع الجهاز** حيث يتم عرض قائمة بملفات التتبع.

4. في قائمة ملفات التتبع، حدد الملف الذي تريده.

5. قم بأحد الإجراءات التالية:

• قم بتنزيل الملف المحدد عن طريق النقر على تنزيل ملف بالكامل.

• قم بتنزيل جزء من الملف المحدد:

a. انقر على تنزيل جزء.

b. في النافذة التي تفتح، حدد الاسم وجزء الملف المراد تنزيله، وفقاً لاحتياجاتك.

c. انقر على تنزيل.

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 التشخيص عن بُعد التي تفتح، انقر على تشخيصات عن بعد.

3. في نافذة الحالات والسجلات التي تفتح، تأكد أن قسم سجلات نظام التشغيل محدد.

4. في قسم ملفات التتبع، انقر على زر سجلات Windows Update أو زر سجلات التثبيت عن بُعد، اعتماداً على ملفات التتبع التي ترغب في حذفها. يفتح هذا قائمة بملفات التتبع.

5. في قائمة ملفات التتبع، حدد الملف الذي ترغب في حذفه.

6. انقر على زر إزالة.

يتم حذف ملف التتبع المحدد.

تنزيل إعدادات التطبيق

لتنزيل إعدادات تطبيق من جهاز عميل:

1. [افتح نافذة التشخيص عن بُعد لجهاز عميل.](#)

2. في نافذة التشخيص عن بُعد التي تفتح، انقر على تشخيصات عن بعد.

3. في نافذة الحالات والسجلات التي تفتح، تأكد أن سجلات نظام التشغيل محدد في الجزء الأيمن.

- في قسم معلومات النظام، انقر على زر ملف التنزيل لتنزيل معلومات النظام عن الجهاز العميل.
- في قسم إعدادات التطبيق، انقر على زر ملف التنزيل لتنزيل معلومات عن إعدادات التطبيقات المثبتة على الجهاز. يتم تنزيل المعلومات إلى الموقع التي تحدده كملف.

تنزيل سجلات الأحداث

لتنزيل سجل الأحداث من جهاز بعيد:

1. [افتح نافذة التشخيص عن بُعد لجهاز عميل.](#)

2. في نافذة التشخيص عن بُعد، انقر على سجلات الجهاز.

3. في نافذة جميع سجلات الجهاز، حدد السجل ذي الصلة:

4. قم بأحد الإجراءات التالية:

• قم بتنزيل السجل المحدد عن طريق النقر على تنزيل ملف بالكامل.

• قم بتنزيل جزء من السجل المحدد:

a. انقر على تنزيل جزء.

b. في النافذة التي تفتح، حدد الاسم وجزء الملف المراد تنزيله، وفقاً لاحتياجاتك.

c. انقر على تنزيل.

يتم تنزيل سجل الحدث المحدد أو جزئه إلى الموقع الذي تحدده.

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 التشخيص عن بُعد، انقر على تشخيصات عن بعد.

3. في نافذة الحالات والسجلات التي تفتح، حدد قسم تطبيقات Kaspersky.

يؤدي هذا إلى فتح قائمة تطبيقات Kaspersky المثبتة على الجهاز.

4. في قائمة التطبيقات، حدد التطبيق الذي ترغب في بدئه أو إيقافه أو إعادة تشغيله.

5. حدد إجراءً بالنقر على أحد الأزرار التالية:

• إيقاف التطبيق

لا يتوفر هذا الزر إلا إذا كان التطبيق قيد التشغيل حاليًا.

• إعادة تشغيل التطبيق

لا يتوفر هذا الزر إلا إذا كان التطبيق قيد التشغيل حاليًا.

• بدء التطبيق

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 رسالة تفيد أنه سيتم فقد الاتصال الحالي للجهاز بخادم الإدارة.

تشغيل التشخيصات عن بُعد لأحد التطبيقات وتنزيل النتائج

لبدء التشخيصات لأحد التطبيقات على جهاز بعيد وتنزيل نتائجها:

1. [افتح نافذة التشخيص عن بُعد لجهاز عميل.](#)

2. في نافذة التشخيص عن بُعد، انقر على **تشخيصات عن بُعد**.

3. في نافذة **الحالات والسجلات** التي تفتح، حدد قسم **تطبيقات Kaspersky**.

يؤدي هذا إلى فتح قائمة تطبيقات Kaspersky المثبتة على الجهاز.

4. في قائمة التطبيقات، حدد التطبيق الذي ترغب في تشغيل التشخيص عن بُعد له.

يتم عرض قائمة خيارات التشخيص عن بُعد.

5. في قسم **تقرير التشخيص** من القائمة، انقر على زر **تشغيل التشخيصات**.

يؤدي هذا إلى بدء عملية التشخيص عن بُعد وينشئ تقريرًا عن التشخيص. عندما تكتمل عملية التشخيص، يتوفر زر **تنزيل تقرير التشخيص**.

6. نزل التقرير عن طريق النقر على زر **تنزيل تقرير التشخيص**.

يتم تنزيل التقرير إلى الموقع الذي حددته.

تشغيل تطبيق على جهاز عميل

قد تضطر إلى تشغيل تطبيق على الجهاز العميل إذا طلب منك أخصائي دعم 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 التشخيص عن بُعد التي تفتح، انقر على **تشخيصات عن بُعد**.

3. في نافذة **الحالات والسجلات** التي تفتح، حدد قسم **تشغيل تطبيق بعيد**.

4. في نافذة **تشغيل تطبيق بعيد** في قسم **ملفات التطبيق**، اتخذ أحد الإجراءات التالية، وفق ما يطلب من أخصائي Kaspersky فعله:

- حدد ملف مضغوط ZIP يحتوي على التطبيق الذي ترغب في تشغيله على الجهاز العميل عن طريق النقر على زر استعراض.
- حدد تطبيق سطر الأوامر ووسيطاته إذا لزم الأمر.

5. اتبع إرشادات الأخصائي.

تنزيل وحذف الملفات من العزل والنسخ الاحتياطي

يقدم هذا القسم معلومات حول كيفية التنزيل وكيفية حذف الملفات من العزل والنسخ الاحتياطي في Kaspersky Security Center 14 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 النسخ الاحتياطي إلى محرك الأقراص الثابتة:

1. قم بأحد الإجراءات التالية:

- إذا كنت تريد حفظ نسخة من الملف من العزل، فانقل إلى **العمليات** ← **المستودعات** ← **العزل**.
- إذا كنت تريد حفظ نسخة من الملف من النسخ الاحتياطي، فانقل إلى **العمليات** ← **المستودعات** ← **النسخ الاحتياطي**.

2. في النافذة التي تفتح، حدد الملف الذي تريد تنزيله وانقر فوق **تنزيل**.

سيبدأ التنزيل. يتم حفظ نسخة من الملف الذي تم وضعه في العزل على جهاز العميل في المجلد المحدد.

حول إزالة الكائنات من العزل أو النسخ الاحتياطي أو مستودعات التهديدات النشطة

عندما تضع تطبيقات الأمان من Kaspersky المثبتة على أجهزة العميل كائنات في العزل أو النسخ الاحتياطي أو مستودعات التهديدات النشطة، فإنها ترسل المعلومات حول الكائنات المضافة إلى **العزل**، و **النسخ الاحتياطي** أو أقسام **تهديدات نشطة** في Kaspersky Security Center. عند فتح أحد هذه الأقسام، حدد كائنًا من القائمة وانقر على زر **إزالة**، فإن ينفذ Kaspersky Security Center أحد الإجراءات التالية أو كلا الإجراءات:

• يزيل الكائن المحدد من القائمة

• يحذف الكائن المحدد من المستودع

يتم تحديد الإجراءات المطلوب تنفيذه بواسطة تطبيق Kaspersky الذي وضع الكائن المحدد في المستودع. تم تحديد تطبيق Kaspersky في حقل **الإدخال من إضافة**. راجع وثائق تطبيق Kaspersky للحصول على تفاصيل حول الإجراءات الذي سيتم تنفيذه.

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 بصفحتك 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

يمكنك العثور على أمثلة للمطابقة بين بعض سيناريوهات المستخدمين وأساليب OpenAPI في الجدول أدناه.

المطابقة بين سيناريوهات المستخدمين وعينات من أساليب Kaspersky Security Center OpenAPI

سيناريو	الغرض من العينة	عينة
المراقبة وإعداد التقارير	يمكنك استخلاص البيانات ومعالجتها وجمعها باستخدام هيكل بيانات KIAkParams. 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.	سجل KIAkParams
<ul style="list-style-type: none"> • إنشاء تسلسل هرمي من خوادم الإدارة: إضافة خادم إدارة تابع • حذف تسلسل هرمي لخوادم الإدارة 	يمكنك إضافة خادم إدارة كخادم إدارة ثانوي، وإنشاء تسلسل هرمي "أساسي / ثانوي". بالتناوب، يمكنك فصل خادم الإدارة الثانوي من التسلسل الهرمي.	إنشاء وحذف تدرج "أساسي / ثانوي"
إنشاء مجموعات إدارة	يمكنك الاستقصاء عن وحدة Active Directory وتشكيل تسلسل هرمي لمجموعات الأجهزة المكتشفة.	إنشاء التسلسل الهرمي للمجموعة مع هيكل يستند إلى وحدة Active Directory
إنشاء مجموعات إدارة	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 التسلسل الهرمي للمجموعة مع هيكل يستند إلى وحدة Active Directory المخزنة مؤقتًا
تعديل نقاط التوزيع وبوابات الاتصال	يمكنك الاتصال بوكيل الشبكة على الجهاز المطلوب عن طريق استخدام بوابة اتصال ، وبعدها قم بتنزيل ملف بقائمة الشبكات على جهازك.	تنزيل ملفات قائمة الشبكة عبر بوابة الاتصال للجهاز المحدد
ترخيص التطبيقات المُدارة	يمكنك الاتصال بخادم الإدارة الأساسي، وتحميل مفتاح الترخيص المطلوب منه، ونقل هذا المفتاح إلى جميع خوادم الإدارة الثانوية المضمنة في التدرج.	قم بتثبيت مفتاح ترخيص مخزن في مستودع خادم الإدارة الأساسي على خوادم الإدارة الثانوية
إنشاء تقرير وعرضه	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 بحقوق المستخدم النشطة
بدء مهمة يدويًا	يمكنك الاتصال بوكيل الشبكة على الجهاز المطلوب عن طريق استخدام بوابة اتصال ثم تشغيل	إبدأ مهمة لجهاز

	المهمة المطلوبة.	
<p>تكوين حماية الشبكة</p>	<p>يمكنك إنشاء شبكة IP فرعية استنادًا إلى وحدة Active Directory التي تستخدمها.</p> <p>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.</p> <p>بعد الاستقصاء، يشير النموذج إلى Active Directory ويفحص كل جهاز فيه وينشئ شبكة IP الفرعية. لفعل ذلك، يستخدم النموذج أفضة وعناوين IP لجميع الأجهزة.</p>	<p>إنشاء شبكات IP فرعية استنادًا إلى موقع وخدمات Active Directory</p>
<p>تحديث قواعد بيانات Kaspersky وتطبيقاته</p>	<p>يمكنك تعيين الأجهزة المُدارة كنقاط توزيع (كانت معروفة سابقًا باسم وكلاء التحديث).</p>	<p>تسجيل نقاط التوزيع للأجهزة في مجموعة</p>
<p>تكوين خادم الإدارة</p>	<p>يمكنك تنفيذ العديد من الإجراءات على مجموعات الإدارة. يوضح النموذج كيفية فعل ذلك:</p> <ul style="list-style-type: none"> • احصل على معرّف لمجموعة الجذر "الأجهزة المُدارة" • تنقل عبر التسلسل الهرمي للمجموعة • استرجع التسلسل الهرمي الكامل والموسع للمجموعات، جنبًا إلى جنب مع أسمائها وتداخلها 	<p>عد كل المجموعات</p>
<p>مراقبة تنفيذ المهمة</p>	<p>يمكنك معرفة المعلومات التالية:</p> <ul style="list-style-type: none"> • تاريخ تقدم المهمة • حالة المهمة الحالية • عدد المهام في حالات مختلفة <p>يمكنك أيضًا تشغيل مهمة بشكل افتراضي، يقوم النموذج بتشغيل مهمة بعد إخراج الإحصائيات.</p>	<p>عد المهام والاستعلام عن إحصائيات المهام وتشغيل مهمة</p>
<p>إنشاء مهمة</p>	<p>يمكنك إنشاء مهمة. حدد معلمات المهمة التالية في النموذج:</p> <ul style="list-style-type: none"> • النوع • طريقة التشغيل • الاسم • مجموعة الأجهزة التي سيتم استخدام المهمة لها <p>بشكل افتراضي، يقوم النموذج بإنشاء مهمة من النوع "إظهار الرسالة". يمكنك تشغيل هذه المهمة لجميع الأجهزة المُدارة لخادم الإدارة. يمكنك إذا لزم الأمر تحديد معلمات المهمة الخاصة بك.</p>	<p>إنشاء وتشغيل مهمة</p>
<p>عرض معلومات حول مفاتيح الترخيص قيد الاستخدام</p>	<p>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.</p>	<p>عد مفاتيح الترخيص</p>
<p>تحديد الحساب لتشغيل خادم الإدارة</p>	<p>يمكنك إنشاء حساب لمزيد من العمل.</p>	<p>إنشاء العثور على مستخدم داخلي</p>
<p>إنشاء فئة تطبيق</p>	<p>يمكنك إنشاء فئة التطبيق بالمعلومات المطلوبة.</p>	<p>إنشاء فئة مخصصة</p>

مضافاً إليها المحتوى يدوياً		
إدارة حسابات المستخدمين	يمكنك استخدام الفئة SrvView لطلب معلومات مفصلة من خادم الإدارة. يمكنك على سبيل المثال الحصول على قائمة المستخدمين عن طريق استخدام هذا النموذج.	عد المستخدمين باستخدام SrvView

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، Kaspersky Security for Virtualization أو Attack Platform. يمكن أن يكون هذا أيضاً 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؛ وبخاصة 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 مأخذ التوصيل الأمانة (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:

- منفذ TCP 13000—منفذ TLS لخادم الإدارة لاتصال عملاء الشبكة الذين تم نشرهم في شبكة العميل
- منفذ TCP—HTTPS 8061 لنشر الحزم المستقلة باستخدام أدوات وحدة تحكم الإدارة
- منفذ TCP—HTTP 8060 8061 لنشر الحزم المستقلة باستخدام أدوات وحدة تحكم الإدارة
- منفذ TCP—TLS 13292 المطلوب فقط عند وجود أجهزة محمولة تلزم إدارتها

إذا كنت بحاجة إلى تزويد العملاء بالخيارات الأساسية لإدارة الشبكة من خلال Kaspersky Security Center 14 Web Console، فيجب عليك أيضًا فتح منافذ Kaspersky Security Center 14 Web Console التالية:

- منفذ TCP—HTTPS 8081
- منفذ TCP—HTTP 8080

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 المزودين بالخدمات أو العدد الإجمالي للأجهزة المُدارة.

يمكن لخادم إدارة واحد دعم ما يصل إلى 100000 جهاز. يجب عليك وضع احتمالية زيادة عدد الأجهزة المُدارة 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 المسماة والتعامل مع مجموعة الأجهزة المُدارة بالكامل كما لو أنها تتم إدارتها بواسطة خادم إدارة واحد: مثل البحث عن أجهزة، وبناء تحديثات 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 مستويات 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 مباشراً 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.

سيُتخذ على خادم الإدارة إرسال إخطارات إلى المنفذ UDP 15000 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 متاحاً 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:

- توزيع التحديثات (والتي يمكن استردادها إما من خادم الإدارة أو من خوادم Kaspersky). في الحالة الأخيرة، يجب إنشاء مهمة تنزيل التحديثات إلى مستويات 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 لخادم 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 كيوابة اتصال. وفي هذه الحالة، ستكون الأجهزة الموجودة في نطاق نقطة التوزيع هذه متصلة بخادم الإدارة عبر البوابة وليس مباشرة. يمكن 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 لاثنتين 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.

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 المخصص لمجموعات الإدارة للأجهزة المخصصة مع السياسات والمهام، يتميز كل خادم إدارة افتراضي بمجموعته الخاصة من الأجهزة غير المعينة ومجموعات التقارير الخاصة والأحداث المحددة وحزم التثبيت وقواعد النقل... إلخ. 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 14 Web Console.

خوادم الإدارة الافتراضية تشبه إلى حد كبير خوادم الإدارة الثانوية، ولكن مع الفروق التالية:

- يفتقد خادم الإدارة الافتراضي لأغلب الإعدادات العمومية ومناقذ 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 المثبت عليها Kaspersky Endpoint Security for Android™ (يُشار إليها فيما بعد باسم أجهزة KES) بواسطة خادم الإدارة. يدعم Kaspersky Security Center 10 Service Pack 1، بالإضافة إلى الإصدارات الأحدث، المزايا 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 موزعًا. 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 يشغلها المسؤول.
- Kaspersky Security Center 14 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 14 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 المثبت 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 المسمى KLAAdmins

2. في مثبت خادم الإدارة، حدد حسابات المجال التي تم إنشاؤها للخدمات.

تحديد نظام إدارة قواعد البيانات

عند تثبيت خادم الإدارة، يمكنك تحديد نظام إدارة قواعد البيانات الذي سيستخدمه خادم 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 قيود استخدامها.

قيود استخدام نظام إدارة قاعدة البيانات

القيود	نظام إدارة قاعدة البيانات
لا يوصى به إذا كنت تنوي تشغيل خادم إدارة واحد لأكثر من 10,000 جهاز أو استخدام التحكم في التطبيقات.	إصدار SQL Server Express Edition 2012 أو الإصدار الأحدث.
بلا قيود.	إصدار 2012 أو الإصدارات الأحدث من خادم SQL Server المحلي، غير الإصدار Express.
صالح فقط في حالة وجود الجهازين في مجال Windows® نفسه؛ وفي حالة اختلاف المجالات، يجب إنشاء علاقة ثقة ثنائية بينهم.	إصدار 2012 من SQL Server البعيد، غير الإصدار Express، أو الإصدار الأحدث.
لا يوصى به إذا كنت تنوي تشغيل خادم إدارة واحد لأكثر من 10,000 جهاز أو استخدام التحكم في التطبيقات.	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)
لا يوصى به إذا كنت تنوي تشغيل خادم إدارة واحد لأكثر من 50,000 جهاز أو استخدام التحكم في التطبيقات.	MySQL 8.0.20 محلي أو عن بُعد أو إصدار أحدث
لا يوصى به إذا كنت تنوي تشغيل خادم إدارة واحد لأكثر من 20,000 جهاز أو استخدام التحكم في التطبيقات.	MariaDB Server 10.3 المحلي أو البعيد

إذا كنت تستخدم SQL Server 2019 كنظام DBMS ولم يكن لديك التصحيح التراكمي CU12 أو إصدار أحدث، فيجب عليك تنفيذ ما يلي بعد تثبيت Kaspersky Security Center:

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
```

```
ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
```

```
GO
```

3. أعد تشغيل خدمة SQL Server 2019.

وإلا، فإن استخدام SQL Server 2019 قد ينتج عنه أخطاء، مثل "لا توجد ذاكرة كافية على النظام في وعاء الموارد الداخلي" لتشغيل هذا الاستعلام".

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 العملية

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.

الإعدادات اليدوية 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، الرجاء مراعاة أنه يجب عليك النقر على أيقونة القفل فوق الإعداد ذي الصلة للسماح باستخدام القيمة الخاصة به على محطة العمل.

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 لـ 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 قسم Kaspersky Security Network الفرعي، نوصي بتمكين خيار استخدام وكيل KSN. يساعد استخدام هذا الخيار في إعادة توزيع وتحسين حركة المرور على الشبكة. يمكنك أيضًا تمكين استخدام خوادم KSN إذا لم تكن خدمة KSN Proxy متوفرة. قد تتواجد خوادم KSN إما على جانب Kaspersky (عند استخدام شبكة KSN العالمية) أو على جانب أطراف خارجية (عند استخدام شبكة KSN الخاصة).

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.

موضح أدناه إجراءات الإعداد الإضافية، والتي ننصحك بإجرائها في نافذة خصائص السياسة الخاصة بـ Kaspersky Endpoint Security for Windows، في قسم الحماية من التهديدات الأساسية.

قسم الحماية من التهديدات الأساسية، القسم الفرعي "جدار الحماية"

تحقق من قائمة الشبكات الموجودة في خصائص السياسة. قد لا تحتوي القائمة على كل الشبكات.

للتحقق من قائمة الشبكات:

1. من نافذة خصائص السياسة، ابحث عن قسم الحماية من التهديدات الأساسية وحدد القسم الفرعي جدار الحماية.
 2. في قسم الشبكات المتوفرة، انقر فوق الزر الإعدادات.
- يؤدي ذلك إلى فتح النافذة جدار الحماية. تعرض هذه النافذة قائمة بالشبكات الموجودة في علامة التبويب الشبكات.

قسم الحماية من التهديدات الأساسية، القسم الفرعي الحماية من تهديدات الملفات

يمكن أن يؤدي تمكين 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. من نافذة خصائص السياسة، ابحث عن قسم الحماية من التهديدات الأساسية وحدد القسم الفرعي الحماية من تهديدات الملفات.
2. في قسم مستوى الأمان، انقر فوق الزر الإعدادات.
3. من نافذة الحماية من تهديدات الملفات التي تفتح، في علامة التبويب عام، قم بإلغاء تحديد 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.

قسم الإعدادات العامة، القسم الفرعي التقارير وعمليات التخزين

في القسم نقل البيانات إلى خادم الإدارة، يُرجى ملاحظة الإعدادات التالية:

خانة اختيار حول التطبيقات التي تم بدؤها: في حالة تحديد خانة الاختيار هذه، تقوم قاعدة بيانات خادم الإدارة بحفظ معلومات حول كل 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

في حالة وجوب إدارة الحماية ضد الفيروسات في شبكة المؤسسة في الوضع المركزي عبر وحدة تحكم الإدارة، يجب عليك تعطيل عرض واجهة مستخدم Kaspersky Endpoint Security for Windows على محطات العمل (عن طريق إلغاء تحديد خانة الاختيار عرض واجهة التطبيق الموجودة في القسم التفاعل مع المستخدم)، وتمكين الحماية باستخدام كلمة المرور (عن طريق تحديد خانة الاختيار تمكين الحماية بكلمة المرور 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 تبويب حدث حرج :
- تم تعطيل التشغيل التلقائي للتطبيق
- تم رفض الوصول
- تم حظر بدء التطبيق
- التنظيف غير ممكن
- انتهاك اتفاقية الترخيص
- تعذر تحميل الوحدة النمطية للتشفير
- يتعذر تشغيل مهمتين في الوقت نفسه
- تم اكتشاف تهديد نشط. بدء التنظيف المتقدم
- تم اكتشاف هجوم على الشبكة
- لم يتم تحديث كل المكونات
- خطأ في النسخ
- خطأ في تمكين الوضع المحمول
- خطأ في التفاعل مع Kaspersky Security Center
- خطأ في تعطيل الوضع المحمول
- خطأ في تغيير مكونات التطبيق

- خطأ في تطبيق قواعد تشفير / فك تشفير الملف
- يتعذر تطبيق السياسة
- تم إنهاء العملية
- تم حظر نشاط الشبكة
- في علامة التثبيت **الفشل الوظيفي**: إعدادات المهمة غير صالحة. لم يتم تطبيق الإعدادات
- في علامة التثبيت **تحذير**:
- تم تعطيل الدفاع الذاتي
- مفتاح حجز غير صحيح
- قام المستخدم بإلغاء اشتراكه في سياسة التشفير
- في علامة التثبيت "معلومات": يحظر بدء تشغيل التطبيق في وضع الاختبار

الإعداد اليدوي لمهمة تحديث المجموعة لتطبيق Kaspersky Endpoint Security

تنطبق المعلومات الموجودة في هذا القسم الفرعي فقط على Kaspersky Security Center 10 Maintenance Release 1 والإصدارات الأحدث.

إذا كان خادم الإدارة يعمل كمصدر التحديث، فخيار الجدولة الأمثل والموصى به لإصدارات 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**.

بالنسبة لمهمة تحديث مجموعة في Kaspersky Endpoint Security الإصدار 8 يجب عليك تحديد تأخير التشغيل بشكل صريح (ساعة واحدة أو أكثر) وتحديد خانة الاختيار **استخدام التأخير العشوائي التلقائي لبدء مهمة**.

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 7:00 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 6:30 م، فلن يتم تشغيل مهمة فحص الجهاز أبدًا. يجب عليك إعداد الجدول الأكثر ملاءمة 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 لعمل الشبكة. بشكل افتراضي، يتم تعيين الجدول **تشغيل في أيام الثلاثاء الساعة 7:00 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 ملاءمة 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 01:00 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 ملاءمة 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 باستخدام العلامات ومواقع الجهاز في الوحدات التنظيمية لـ **Active Directory** والعضوية في **مجموعات الأمان الخاصة بـ Active Directory** وما إلى ذلك.
- 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 التوافق 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 ينتقلون 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. كما يقدم هذا القسم معلومات حول ملفات تعريف السياسة المدعومة في **Kaspersky Security Center**، بدءًا من الإصدار 10 من Service Pack 1.

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.

لن تكون سياسة الوجود خارج المكتب مدعومة في الإصدارات الأخرى من Kaspersky Security Center. سيتم استخدام ملفات تعريف السياسة بدلاً من سياسات خارج المكتب.

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.

للمساعدة في تجنب مثل هذه المشكلات، فإن Kaspersky Security Center - بدءًا من الإصدار 10 من Service Pack 1 - يدعم ملفات تعريف السياسة. ملف تعريف السياسة هو مجموعة فرعية مسماة 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:

- ملفات التعريف الاسم ذات الأسماء المتشابهة تؤثر 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 نشطاً (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 ضمناً (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 طبقاً 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 أي 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، و عرض 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 و [سجل 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 (وبخاصة في مناطق حقوق الوصول والأحداث والتقارير). يجب العثور على حل آخر، على سبيل المثال، من خلال استخدام ملفات تعريف السياسة، والمهام الخاصة بـ تحديثات 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 المعدة 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 يمكن إنشاء فئات يتم تحديثها تلقائيًا على أساس المجلدات "%windir"، "%My Documents"، و"%ProgramFiles%". 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

يمكن 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 العملية 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 k1backup. تتضمن النسخة الاحتياطية جميع الإعدادات والكائنات الرئيسية المتعلقة بخادم الإدارة، مثل الشهادات، والمفاتيح الأساسية لتشفير محركات الأقراص على الأجهزة المدارة، 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 لتشغل يوميًا في الساعة 4:00 صباحًا. ويتم حفظ النسخ الاحتياطية افتراضيًا في المجلد %Application Data\KasperskySC%\ALLUSERSPROFILE.

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 الغير واضح مستنتب 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 kbackup يعملان على حماية النسخ الاحتياطية 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.

لتقليل حجم النسخ الاحتياطية لأدنى حد، قم بتمكين خيار **ضغط النسخ الاحتياطية** في إعدادات خادم SQL Server.

تتم الاستعادة من نسخة احتياطية باستخدام الأداة المساعدة kbackup 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 (خادم SQL Server أو MySQL أو MariaDB) والإصدار نفسه (أو الأحدث). يمكن أن يكون إصدار خادم الإدارة هو نفسه (بتصحيح مشابه أو أحدث) أو إصدار أحدث.

يوضح هذا القسم السيناريو هات القياسية لإعدادات الاستعادة وكنائنات 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 القائمة **بدء**، قم بتشغيل الأداة المساعدة kbackup وإجراء الاستعادة.

إعدادات خادم الإدارة أو قاعدة البيانات تالفة

إذا تعذر تشغيل خادم الإدارة نتيجة لتلف الإعدادات أو قاعدة البيانات (على سبيل المثال، بعد حدوث تغيير 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 kbackup وإجراء الاستعادة.

أية محاولات لاستعادة خادم الإدارة من خلال برنامج تابع لجهة خارجية ستؤدي حتمًا إلى عدم مزامنة البيانات على عُقد تطبيق Kaspersky Security Center الموزع، 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 الموزع على أجهزة المؤسسة عادةً بتثبيت عميل الشبكة عليها.

وفي Microsoft Windows XP، قد لا يقوم عميل الشبكة بالعمليات التالية بشكل صحيح: تنزيل التحديثات مباشرة من خوادم Kaspersky (كنقطة توزيع) والعمل كوكيل 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 عميل الشبكة المثبت 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 مستخدم الجهاز. الحزم المستقلة هي وحدات نمطية تنفيذية تحتوي على حزم التوزيع الخاصة بالتطبيقات المحددة مع تحديد إعداداتها.
- يدويًا، عن طريق تشغيل مثبتات التطبيق على الأجهزة.

في المنصات بخلاف Microsoft Windows، يتعين عليك تنفيذ التثبيت الأولي لعميل الشبكة على الأجهزة المُدارة 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

- 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 Kaspersky عليها (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 بالمتبث، 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 المتبث.

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 غير التفاعلي للتطبيقات على مجموعات الأجهزة. بشكل عام، يجب على المسؤول تحديد قيم الإعدادات 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 غير التفاعلي 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 بالمتبث أو من المثبتات الموجودة في تنسيق (MSI) Microsoft Windows Installer للتطبيقات القياسية أو المدعومة.

حزم التثبيت التي تم إنشاؤها مرتبة ترتيبًا هرميًا كمجلدات بها مجلدات فرعية وملفات متداخلة. بالإضافة إلى حزمة التوزيع الأصلية، تحتوي حزمة التثبيت على إعدادات قابلة للتعديل (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 إنشاؤها بالفعل). عند إجراء تثبيت التطبيقات عن بُعد باستخدام أدوات Kaspersky Security Center tools، يتم تسليم حزم التثبيت إلى الأجهزة الهدف يمكن أن يؤدي تشغيل متبث 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 تقع 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 إنشاؤه 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 تتفقد 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 كل 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 وفقاً لمحتويات التحديد عند بدء تشغيل المهمة. إذا احتوي تحديد ما على أجهزة تم توصيلها بخوادم الإدارة الثانوية، ستعمل المهمة على هذه الأجهزة أيضاً.

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 مقدماً.

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 عضواً 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 مثبت Microsoft (حزمة MSI) في مجلد مشترك (هو المجلد الذي تحتوي فيه حسابات LocalSystem الخاصة بالأجهزة الهدف على أدونات 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 مستخدم الجهاز إلى النظام)، يتم التحقق من كل التطبيقات المثبتة بحثاً 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 مثبت Windows.

بالإضافة إلى ذلك، عند تحديد طريقة النشر هذه، يجب عليك أيضاً تقييم الحمل على مورد الملف الذي سيتم نسخ الملفات منه إلى الأجهزة الهدف بعد تطبيق سياسة مجموعة Windows. يتعين عليك أيضاً 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. ونظراً 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.

- 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

لقيام بالنشر الأولي لعملاء الشبكة أو التطبيقات الأخرى، يمكنك فرض تثبيت حزم التثبيت المحددة عن طريق استخدام مهمة التثبيت عن بُعد من Kaspersky Security Center – شريطة أن يحتوي كل جهاز على حساب (حسابات) مستخدم لديه حقوق المسؤول المحلي وعلى الأقل جهاز واحد مثبت عليه عميل الشبكة [يعمل كنقطة توزيع](#) في كل شبكة فرعية.

في هذه الحال، يمكنك تحديد أجهزة هدف 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. إذا كان إعداد [تشغيل المهام الفائتة](#) ممكنًا في خصائص المهمة، فيمكن تشغيل المهمة إما فورًا أو بعد تشغيل الأجهزة الهدف أو عند نقلها إلى مجموعة الإدارة الهدف.

يتألف التثبيت الإجباري من تسليم حزم التثبيت إلى نقاط التوزيع، والنسخ التالي للملفات إلى مورد \$admin على كل جهاز من الأجهزة الهدف، التسجيل عن بُعد للخدمات الداعمة على تلك الأجهزة. يتم تنفيذ تسليم حزم التثبيت إلى نقاط التوزيع من خلال ميزة Kaspersky Security Center التي تضمن تفاعل الشبكة. يجب الوفاء بالشروط التالية في هذه الحالة:

- يمكن الوصول إلى الأجهزة المستهدفة من جانب نقطة التوزيع.
- يعمل تحليل الاسم للأجهزة الهدف بشكل صحيح على الشبكة.
- تظل المشاركات الإدارية (\$ admin) ممكنة على الأجهزة الهدف.
- تعمل خدمة نظام الخادم على الأجهزة الهدف (تكون قيد التشغيل بشكل افتراضي).
- إن المنافذ التالية مفتوحة على الأجهزة الهدف للسماح بالوصول عبر أدوات TCP 139، TCP 445، UDP 137، UDP 138. Windows.
- يتم تعطيل وضع مشاركة الملفات البسيطة على الأجهزة المستهدفة التي تعمل بنظام التشغيل Microsoft Windows XP.
- على الأجهزة الهدف، يتم تعيين مشاركة الوصول ونموذج الأمان على النحو التقليدي – مصادقة المستخدمين المحليين على أنفسهم، ولا يمكن أن يكون بأي حال ضيف فقط – مصادقة المستخدمين المحليين على أنهم ضيف.
- يجب أن تكون الأجهزة الهدف أعضاء في المجال، أو يجب إنشاء حسابات موحدة باستخدام حقوق المسؤول على الأجهزة الهدف مقدمًا.

يمكن تعديل الأجهزة الموجودة في مجموعات العمل وفقًا للمتطلبات الموجودة أعلاه باستخدام الأداة المساعدة riprep.exe الموضحة [على الموقع الإلكتروني للدعم الفني في Kaspersky](#).

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.

يُعتبر التثبيت التلقائي طريقة مبسطة لإنشاء مهام للتثبيت الإجباري للتطبيقات. للقيام بذلك، افتح خصائص مجموعة الإدارة، وافتح قائمة حزم التثبيت وحدد الحزم التي يجب تثبيتها على الأجهزة الموجودة في هذه المجموعة. وكننتيجة 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.

للسماح بالثثبيت الإجباري، ينبغي عليك التأكد من أن نقاط التوزيع موجودة في كل شبكة من الشبكات الفرعية المنعزلة التي تستضيف الأجهزة الهدف.

لاحظ أن طريقة التثبيت هذه تضع حملاً كبيراً على الأجهزة التي تعمل كنقاط توزيع. لذا، من المستحسن أن تحدد أجهزة قوية ذات وحدات تخزين عالية الأداء لتعمل كنقاط توزيع. علاوةً على ذلك، يجب أن تتخطى مساحة القرص الخالية في القسم الذي يحتوي على المجلد `%Application Data\KasperskyLab\adminkit%\ALLUSERSPROFILE%` بعدة مرات المساحة الإجمالية لحزم التوزيع الخاصة بالتطبيقات المثبتة.

تشغيل الحزم المستقلة التي أنشأها Kaspersky Security Center

لا يمكن تطبيق الطرق الموضحة أعلاه للنشر الأولي لعمل الشبكة والتطبيقات الأخرى دائماً 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 (مضمن 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 حصرياً مضمن في Kaspersky Security Center 14 Web Console. يمكنك أيضاً 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 المستخدم حالياً، مطالباً 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 أيضاً 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 بعمل عميل 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 يدوياً 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 مثبت 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) مثبتاً 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 قبل 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\FTCITmp`.

لا يمكن حذف الملفات من المجلد `FTCITmp` 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 محسن 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 أي 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 حال استخدام مهمة التثبيت عن بُعد من Kaspersky Security Center، في إضافة معالج المهمة أو في نافذة خصائص المهمة التي تم إنشاؤها (قسم إعادة تشغيل نظام التشغيل)، يمكنك تحديد الإجراء الذي سيتم اتخاذه عندما تكون إعادة التشغيل مطلوبة:

- **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 ملاءمة لمحطات العمل حيث يحتاج المستخدمون لإمكانية تحديد الوقت الأكثر ملاءمة 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 للتحديثات 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). سيقال 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 المثبت

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 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.

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 المخزن 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 لمواجهة الأوامر على الأجهزة الهدف.

إذا كنت تستخدم مثبتات بتنسيق (MSI) Microsoft Windows Installer، 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) أيضاً قواعد التثبيت وتحليل نتائج التثبيت التي توجد في قاعدة البيانات القابلة للتحديث الخاص به.

وإلا، سنتنظر المهمة الافتراضية للملفات التنفيذية اكتمال العملية قيد التشغيل وكل عملياتها الفرعية. بعد اكتمال كل العمليات قيد التشغيل، سنكتمل المهمة بنجاح بعض النظر عن رمز الإرجاع الخاص بالعملية الأولية. لتغيير مثل هذا السلوك في هذه المهمة، قیل إنشاء المهمة، عليك تعديل الملفات ذات التنسيق kpd. يدوياً والتي أنشأها Kaspersky Security Center في مجلد حزمة التثبيت المنشأة حديثاً ومجلداتها الفرعية.

لجعل المهمة لا تنتظر اكتمال العملية قيد التشغيل، قم بتعيين قيم إعداد الانتظار إلى 0 في القسم [SetupProcessResult]:

مثال:
[SetupProcessResult]
Wait=0

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:

مثال:
[SetupProcessResult]
WaitJob=0

لجعل المهمة تكتمل بنجاح أو إرجاع خطأ بناءً على رمز الإرجاع الخاص بالعملية قيد التشغيل، قم بإدراج رموز الإرجاع الناجحة في القسم [SetupProcessResult_SuccessCodes]، على سبيل المثال:

مثال:
[SetupProcessResult_SuccessCodes]
=0
=3010

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:

مثال:
[SetupProcessResult_SuccessCodes]
0= اكتمل التثبيت بنجاح
3010=إعادة التشغيل مطلوبة لإكمال التثبيت
[SetupProcessResult_ErrorCodes]
1602=تم إلغاء التثبيت بواسطة المستخدم
1603=خطأ فادح أثناء التثبيت

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]:

مثال:

مراقبة النشر

لمراقبة نشر Kaspersky Security Center وللتأكد من أن تطبيق الأمان و عميل 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 المثبت 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 المدارة** 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 و عميل الشبكة في الوضع الصامت.

معلومات عامة

أدوات تثبيت مكونات Kaspersky Security Center 14 (خادم الإدارة، و عميل الشبكة، ووحدة تحكم الإدارة) مضمنة في تقنية مثبت Windows Installer. حزمة MSI هي أساس أداة التثبيت. يتيح تنسيق الحزمة استخدام كل الميزات التي يقدمها Windows Installer: وهي قابلية التوسع وتوفير 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 و عميل 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
```

الملف ss_install.xml هو مثيل للتنسيق الداخلي لمعلومات مثبت Kaspersky Security Center. تحتوي حزمة التوزيع على الملف ss_install.xml مع المعلومات الافتراضية.

الرجاء عدم تعديل الملف ss_install.xml يدويًا. يمكن تعديل هذا الملف عبر أدوات Kaspersky Security Center عند تحرير معلمات حزم التثبيت في وحدة تحكم الإدارة.

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. لتجنب التعارض بين المعلمات المحددة عبر خصائص MSI والمعلومات المحددة في ملف الاستجابة، يمكنك تعطيل ملف الاستجابة عن طريق تعيين الخاصية DONT_USE_ANSWER_FILE=1. مثال على تشغيل مثبت عميل الشبكة باستخدام حزمة msi يتم كما يلي.

يتطلب تثبيت عميل الشبكة في الوضع غير التفاعلي قبول بنود اتفاقية ترخيص المستخدم النهائي. استخدم معلمة EULA=1، إذا قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها.

مثال:

```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1  
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

يمكنك أيضًا تحديد معلمات التثبيت الخاصة بحزمة msi عن طريق إعداد ملف الاستجابة مقدمًا (الملف ذي الامتداد .mst). يظهر هذا الأمر كما يلي:

مثال:

```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

يمكنك تحديد ملفات استجابة متعددة في أمر واحد.

تكوين التثبيت الجزئي عبر setup.exe

عند تشغيل تثبيت التطبيقات عبر setup.exe، يمكنك إضافة القيم الخاصة بأي خصائص MSI إلى حزمة MSI.

يظهر هذا الأمر كما يلي:

مثال:

```
"v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2/
```

معلومات تثبيت خادم الإدارة

يوضح الجدول الموجود أدناه خصائص MSI التي يمكنك تكوينها عند تثبيت خادم الإدارة. جميع المعلومات اختيارية، ماعدا الخاصة باتفاقية ترخيص المستخدم النهائي (EULA) و PRIVACYPOLICY (سياسة الخصوصية).

معلومات تثبيت خادم الإدارة في الوضع غير التفاعلي

القيم المتوفرة	الوصف	خاصية MSI
<ul style="list-style-type: none">1- لقد قرأت شروط <u>اتفاقية ترخيص المستخدم النهائي</u> بشكل كامل واستوعبتها وقبلتها.قيمة أخرى أو بلا قيمة— لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت).	الموافقة على شروط اتفاقية الترخيص (مطلوب)	EULA
<ul style="list-style-type: none">1- أنني أدرك وأوافق على التعامل مع بياناتي ونقلها (بما في ذلك، نقلها إلى البلدان الثالثة) كما هو موضح في <u>سياسة الخصوصية</u>. أؤكد على أنني قد قرأت سياسة الخصوصية وفهمتها بالكامل.قيمة أخرى أو بلا قيمة— لا أوافق على بنود سياسة الخصوصية (لا يتم إجراء التثبيت).	الموافقة على شروط سياسة الخصوصية (مطلوب)	PRIVACYPOLICY

<ul style="list-style-type: none"> • قياسي. • مخصص. 	نوع تثبيت خادم الإدارة	INSTALLATIONMODETYPE
قيمة السلسلة.	مجلد تثبيت التطبيق	INSTALLDIR
<p>CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, .Microsoft_VC100_CRT_x86</p> <p>قائمة الحد الأدنى من المكونات الكافية للتثبيت الصحيح لخادم الإدارة:</p> <p>ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, .Microsoft_VC100_CRT_x86</p>	قائمة بالمكونات التي سيتم تثبيتها (مفصولة بفاصلة)	ADDLOCAL
<ul style="list-style-type: none"> • NRT_1_100 – من 1 إلى 100 جهاز. • NRT_100_1000 – من 101 إلى 1000 جهاز. • NRT_GREATER_1000 – أكثر من 1000 جهاز. تؤكد هذه المعلمة بأنك قد قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها. 	حجم الشبكة	NETRANGETYPE
<ul style="list-style-type: none"> • SrvAccountDefault – سيتم إنشاء حساب المستخدم تلقائيًا. • SrvAccountUser – يتم تحديد حساب المستخدم يدويًا. 	طريقة تحديد المستخدم لتشغيل خدمة خادم الإدارة	SRV_ACCOUNT_TYPE
قيمة السلسلة.	اسم المستخدم للخدمة	SERVERACCOUNTNAME
قيمة السلسلة.	كلمة مرور المستخدم للخدمة	SERVERACCOUNTPWD
<ul style="list-style-type: none"> • MySQL – سيتم استخدام قاعدة بيانات MySQL أو MariaDB • MSSQL – سيتم استخدام قاعدة بيانات Microsoft SQL Server (SQL Express). 	نوع قاعدة البيانات	DBTYPE
قيمة السلسلة.	الاسم الكامل لخادم MySQL أو MariaDB	MYSQLSERVERNAME
قيمة رقمية.	رقم منفذ الاتصال بخادم MySQL أو MariaDB	MYSQLSERVERPORT
قيمة السلسلة.	اسم قاعدة بيانات خادم MySQL أو MariaDB	MYSQLDBNAME
قيمة السلسلة.	اسم المستخدم للاتصال بقاعدة بيانات خادم MySQL أو MariaDB	MYSQLACCOUNTNAME
قيمة السلسلة.	كلمة مرور المستخدم للاتصال بقاعدة بيانات خادم MySQL أو MariaDB	MYSQLACCOUNTPWD
<ul style="list-style-type: none"> • InstallMSSEE – التثبيت من حزمة. 	نوع استخدام قاعدة بيانات	MSSQLCONNECTIONTYPE

• ChooseExisting – استخدام الخادم المثبت.	MSSQL	
قيمة السلسلة.	الاسم الكامل لمثيل خادم SQL Server	MSSQLSERVERNAME
قيمة السلسلة.	اسم قاعدة بيانات خادم SQL Server	MSSQLDBNAME
• Windows. • SQLServer.	طريقة مصادقة الاتصال بخادم SQL Server	MSSQLAUTHTYPE
قيمة السلسلة.	اسم المستخدم للاتصال بخادم SQL Server في وضع SQLServer	MSSQLACCOUNTNAME
قيمة السلسلة.	كلمة مرور المستخدم للاتصال بخادم SQL Server في وضع SQLServer	MSSQLACCOUNTPWD
• 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	طريقة تحديد مجلد مشترك	CREATE_SHARE_TYPE
قيمة السلسلة.	المسار الكامل لمجلد مشترك موجود	EXISTSHAREFOLDERNAME
قيمة رقمية.	رقم المنفذ الخاص بالاتصال بخادم الإدارة	SERVERPORT
قيمة رقمية.	رقم منفذ إنشاء اتصال SSL بخادم الإدارة	SERVERSSLPORT
قيمة السلسلة.	عنوان خادم الإدارة	SERVERADDRESS
• 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 1024 بت.	حجم المفتاح لشهادة خادم الإدارة (بوحدة البت)	SERVERCERT2048BITS
قيمة السلسلة.	عنوان خادم الإدارة للاتصال بالأجهزة المحمولة، يتم تجاهله إن لم يتم تحديد مكوّن MobileSupport	MOBILESERVERADDRESS

يوضح الجدول الموجود أدناه خصائص MSI التي يمكنك تكوينها عند تثبيت عميل الشبكة. وجميع المعلومات اختيارية باستثناء اتفاقية ترخيص المستخدم النهائي (EULA) وSERVERADDRESS.

معلومات تثبيت عميل الشبكة في الوضع غير التفاعلي

القيم المتوفرة	الوصف	خاصية MSI
<ul style="list-style-type: none"> 1- لقد قرأت شروط اتفاقية ترخيص المستخدم النهائي بشكل كامل واستوعبتها وقبلتها. 0- لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت). بلا قيمة- لا أقبل شروط اتفاقية الترخيص (لا يتم إجراء التثبيت). 	الموافقة على شروط اتفاقية الترخيص	EULA
<ul style="list-style-type: none"> 1- عدم الاستخدام. قيمة أخرى أو دون قيمة - عدم القراءة. 	إعدادات تثبيت القراءة لملف الاستجابة	DONT_USE_ANSWER_FILE
قيمة السلسلة.	مسار لمجلد تثبيت عميل الشبكة	INSTALLDIR
قيمة السلسلة.	عنوان خادم الإدارة (مطلوب)	SERVERADDRESS
قيمة رقمية.	رقم منفذ الاتصال بخادم الإدارة	SERVERPORT
قيمة رقمية.	عدد المنافذ لاتصال مشفر لخادم الإدارة باستخدام بروتوكول SSL	SERVERSSLPORT
<ul style="list-style-type: none"> 1 - الاستخدام قيمة أخرى أو دون قيمة - عدم الاستخدام. 	سواء يتم استخدام اتصال SSL أم لا	USESSL
<ul style="list-style-type: none"> 1 - فتح. قيمة أخرى أو دون قيمة - عدم الفتح. 	سواء يتم فتح منفذ UDP أم لا	OPENUDPPOINT
قيمة رقمية.	رقم منفذ UDP	UDPPOINT
<ul style="list-style-type: none"> 1 - الاستخدام قيمة أخرى أو دون قيمة - عدم الاستخدام. 	سواء يتم استخدام خادم وكيل أم لا	USEPROXY
قيمة السلسلة.	عنوان الوكيل ورقم المنفذ للاتصال بالخادم الوكيل	موقع الوكيل (عنوان الوكيل:منفذ الوكيل)
قيمة السلسلة.	حساب للاتصال بخادم وكيل	PROXYLOGIN
قيمة السلسلة.	كلمة مرور الحساب للاتصال بالخادم الوكيل (لا تحدد أي تفاصيل عن الحسابات المميزة في معلومات حزم التثبيت).	PROXYPASSWORD
<ul style="list-style-type: none"> 0 - عدم استخدام بوابة الاتصال. 1 - استخدم عميل الشبكة هذا كبوابة اتصال 	وضع استخدام عبارة الاتصال	GATEWAYMODE

• 2 – الاتصال بخادم الإدارة باستخدام بوابة الاتصال.			
قيمة السلسلة.	عنوان بوابة الاتصال	GATEWAYADDRESS	
• GetOnFirstConnection – تلقي شهادة من خادم الإدارة. • GetExistent – تحديد شهادة موجودة إذا كان هذا الخيار محددًا، فيجب تحديد الخاصية .CERTFILE.	طريقة تلقي شهادة	CERTSELECTION	
قيمة السلسلة.	مسار إلى ملف الشهادة	CERTFILE	
• 1 – التمكين. • 0 – عدم التمكين. • بلا قيمة – لا تمكّن.	تمكين الوضع الديناميكي للبنية الأساسية لسطح المكتب الافتراضي (VDI).	VMVDI	
• 1 – البدء. • قيمة أخرى أو دون قيمة – عدم البدء.	سواء بدء خدمة عميل الشبكة بعد اكتمال التثبيت أم لا	LAUNCHPROGRAM	
قيمة السلسلة.	علامة عميل الشبكة (لها الأولوية على العلامة الواردة في ملف الاستجابة)	NAGENTTAGS	

البنية التحتية الافتراضية

بدعم 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 تجري 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 (Windows فقط). 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 مثبت 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)**

- بالنسبة 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 لمدة تخزين الأحداث (بالأيام).

دعم نسخ الأجهزة الظاهرية

عملية نسخ جهاز ظاهري باستخدام عميل شبكة مثبت أو إنشاء واحد من قالب باستخدام عميل شبكة مثبت هي عملية مشابهة لنشر عملاء الشبكة عن طريق النطاق 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 النطاق 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®: يكتشف عميل الشبكة عملية نسخ للجهاز الظاهري عن طريق معرفات 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 المثبت عليها عميل الشبكة إلى حالته السابقة

يُعتبر Kaspersky Security Center تطبيقًا موزعًا. ستؤدي عودة نظام الملفات إلى الحالة السابقة على جهاز مثبت 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 المثبت عليها عميل شبكة على المجلد %Application%\ALLUSERSPROFILE\ 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 المثبت 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 14.

على قدر الإمكان، تجنب إعادة مجلد %Application Data\KasperskyLab\adminkit%\ALLUSERSPROFILE إلى حالته السابقة على جهاز مثبت 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 مثبت 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

يتم تطبيق الإجراء التالي فقط على Kaspersky Security Center 10 Service Pack 1 والأحدث.

الأجهزة المثبت عليها عميل الشبكة يمكنها الاتصال بخادم الإدارة إما من إنترنت 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 DMZ](#))، فيجب عليك تحديد عنوان بوابة الاتصال في الحقل المقابل لملف تعريف الاتصال.

التبديل بين خوادم الإدارة بناءً على الشبكة الحالية

يتم تطبيق الإجراء التالي فقط على Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 وعلى أي إصدارات أحدث.

إذا كان للمؤسسة مكاتب متعددة بها خوادم إدارة مختلفة وتنتقل بعض الأجهزة المثبت 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 ببيئة 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 نظام نشر لـ Kaspersky Device Management for iOS لأجهزة KES:

- نظام نشر باستخدام الاتصال المباشر للأجهزة بخادم الإدارة
- نظام النشر الذي يتضمن (Forefront® Threat Management Gateway (TMG

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 ثنائية الاتجاه، مصادقة تبادلية).

نظام توصيل أجهزة KES بالخادم الذي يتضمن تفويض Kerberos المقيد (KCD)

يعمل نظام توصيل أجهزة KES بخادم الإدارة الذي يتضمن تفويض Kerberos المقيد (KCD) على ما يلي:

• التكامل مع Microsoft Forefront TMG.

• استخدام تفويض Kerberos المقيد (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:

• نوع اتصال أجهزة KES بـ TMG يجب أن يكون "مصادقة SSL ثنائية الاتجاه"، أي أن الجهاز يجب أن يتصل بـ TMG 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 خصيصاً 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 سيتم فتحها، حدد الشهادة ذاتها التي تم تعيينها على بوابة TMG عندما تم 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 بوابة TMG.

يمكنك التأكد أن شهادة المستخدم متوافقة مع المتطلب الموضح أعلاه عن طريق استخدام طريقة من الطرق التالية:

• حدد شهادة المستخدم الخاصة في معالج حزمة التثبيت الجديدة وفي معالج تثبيت الشهادة.

• دمج خادم الإدارة مع البنية الأساسية للمفتاح العام (PKI) وتحديد الأعداد 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 الذي يحتوي على TMG هو `tmg.mydom.local`.
- اسم الجهاز المثبت 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 `KSCMobileSvcUser`) الذي ستعمل خدمة خادم الإدارة بموجبه. يمكنك تحديد حساب لخادم الإدارة عند تثبيت خادم الإدارة أو عبر الأداة المساعدة `klsvswch`. توجد الأداة المساعدة `klsvswch` في مجلد التثبيت الخاص بخادم الإدارة.

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 `KSCMobileSvcUser`، قم بإضافة SPN لنشر خدمة بروتوكول الجهاز المحمول على المنفذ 13292 الخاص بالجهاز المثبت عليه خادم الإدارة. بالنسبة لجهاز `kes4mob.mydom.local` المثبت عليه خادم الإدارة، سيظهر الاسم كمل يلي:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSvcUser
```

تكوين خصائص المجال الخاصة بالجهاز الذي يحتوي على `tmg.mydom.local` (TMG)

لتفويض حركة المرور، يجب عليك اعتماد الجهاز الذي يحتوي على `tmg.mydom.local` (TMG) إلى الخدمة المحددة بواسطة SPN (`http/kes4mob.mydom.local:13292`).

لا اعتماد الخدمة التي تحتوي على TMG إلى الخدمة المحددة بواسطة SPN (`http/kes4mob.mydom.local:13292`)، يجب أن يقوم المسؤول بالإجراءات التالية:

1. في أداة الإضافة الخاصة بـ Microsoft Management Console التي تحمل الاسم "مستخدمو وأجهزة كمبيوتر Active Directory"، حدد الجهاز المثبت عليه `tmg.mydom.local` (TMG).
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 `http/kes4mob.mydom.local:13292` SPN.

شهادة خاصة (مخصصة) لعملية النشر (`kes4mob.mydom.global`)

لنشر بروتوكول الجهاز المحمول الخاص بخادم الإدارة، يجب عليك إصدار شهادة خاصة (مخصصة) لـ `kes4mob.mydom.global` FQDN 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).

على بوابة TMG، بالنسبة لحركة المرور التي تنتقل من جهة الجهاز المحمول إلى المنفذ 13292 الخاص بـ kes4mob.mydom.global، يجب عليك تكوين KCD على (http/kes4mob.mydom.local:13292) SPN، 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 مر اسلة Google Firebase Cloud

لضمان الاستجابة الفورية لأجهزة KES على Android لأوامر المسؤول، فيجب عليك تمكين استخدام مر اسلة Google™ Firebase Cloud (يُشار إليها فيما بعد باسم FCM) في خصائص خادم الإدارة.

لتمكين استخدام مر اسلة 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 Google Firebase Cloud Messaging.

4. في الحقلين مُعرّف المرسل ومفتاح الخادم، حدد إعدادات FCM: SENDER_ID ومفتاح API.

تعمل خدمة FCM في نطاق العناوين التالي:

- من جهة جهاز KES، مطلوب الوصول إلى المنافذ: (HTTPS) 443 و (HTTPS) 5228 و (HTTPS) 5229 و (HTTPS) 5230 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 (HTTPS) 443 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 خدمة FCM: استرداد SENDER_ID ومفتاح API

لتكوين خدمة FCM، يجب على المسؤول القيام بالإجراءات التالية:

1. التسجيل على [بوابة Google](#).

2. انتقل إلى [بوابة المطورين](#).

3. قم بإنشاء مشروع جديد عن طريق النقر على زر إنشاء مشروع، وحدد اسم المشروع، وحدد المعرف.

4. انتظر حتى يتم إنشاء المشروع.

في الصفحة الأولى من المشروع، في الجزء العلوي من الصفحة، يعرض حقل رقم المشروع معرّف SENDER_ID ذي الصلة.

5. انتقل إلى القسم مفاتيح API & المصادقة / مفاتيح API وقم بتمكين خدمة **Android - Google Firebase Cloud Messaging**.

6. انتقل إلى القسم مفاتيح API & المصادقة / بيانات الاعتماد، وانقر على الزر إنشاء مفتاح جديد.

7. انقر على زر مفتاح الخادم.

8. قم بفرص القيود (إن وجدت)، انقر على زر إنشاء.

9. قم باسترداد مفتاح API من خصائص المفتاح الذي تم إنشاؤه حديثاً (الحقل مفتاح الخادم).

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:

- تعيين للمستخدم شهادة خاصة (مخصصة) من ملف في معالج اتصال الجهاز الجديد أو 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 سيستخدم 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 قالب 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 المثبت عليه خادم الإدارة الذي يتم بدء التكامل مع PKI منه.
- أن يملك حق تسجيل الدخول كخدمة.
- يجب أن يعمل الجهاز المثبت 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 مكون 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، ففتيح لك خصائصه تغيير المنافذ لـ HTTP (8060) و HTTPS (8061). بالإضافة إلى تغيير المنافذ، يمكنك استبدال شهادة الخادم لـ HTTPS وتغيير FQDN الخاص بخادم الويب الخاص بـ HTTP.

عمل روتيني آخر

يوفر هذا القسم توصيات حول العمل الروتيني باستخدام Kaspersky Security Center.

إشارات حركة المرور 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 أجزاء معلومات تحتوي على إشارات حركة مرور. 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	وظيفة تطبيق الأمان: حالة الحماية والفحص للكشف عن الفيروسات
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.

الوصول عن بُعد للأجهزة المدارة

هذا القسم يوفر معلومات حول الوصول للأجهزة المُدارة عن بُعد.

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 وكيل 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 لوكيل الشبكة بخادم الإدارة خلال فترة المزامنة.

لا يمكن إجراء بعض العمليات بدون اتصال مبكر بين وكيل الشبكة وخادم الإدارة مثل تشغيل المهام المحلية وإيقافها، أو تلقي إحصائيات تطبيق مُدار، أو إنشاء نق. 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. قم بأحد الإجراءات التالية:

- إذا كان الجهاز المُدار يصل إلى خادم الإدارة مباشرةً (أي ليس عبر نقطة توزيع):

a. في شجرة وحدة التحكم، حدد المجلد **الأجهزة المُدارة**.

b. في مساحة العمل الخاصة بالمجلد، حدد الجهاز المُدار الذي تريد توفير اتصال مستمر به.

c. في قائمة السياق الخاصة بالجهاز، حدد **خصائص**.

يتم فتح نافذة خصائص الجهاز المحدد.

- إذا كان الجهاز المُدار يصل إلى خادم الإدارة من خلال نقطة توزيع تعمل في وضع البوابة، وليس بشكل مباشر:

a. في شجرة وحدة التحكم، حدد عقدة **خادم الإدارة**.

b. في قائمة السياق الخاصة بالعقدة، حدد **خصائص**.

c. في نافذة خصائص خادم الإدارة التي يتم فتحها، حدد قسم **نقاط التوزيع**.

d. في القائمة، حدد نقطة التوزيع اللازمة، وانقر فوق **خصائص**.

يتم فتح نافذة خصائص نقطة التوزيع.

2. في القسم عام في النافذة المعروضة، حدد الخيار **عدم قطع الاتصال عن خادم الإدارة**.

يتم إنشاء اتصال مستمر بين الجهاز المُدار وخادم الإدارة.

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 متتالية 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 المدارة في وحدة تحكم الإدارة، يحتوي عنصر القائمة **جميع & المهام على الأمر فرض المزامنة**. عندما ينفذ Kaspersky Security Center 14 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 مثبت 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 و عميل VNC والأدوات الأخرى بهذه الطريقة.

يقدم هذا القسم معلومات حول تغيير حجم Kaspersky Security Center.

حول هذا الدليل

يُعد دليل قياس Kaspersky Security Center 14 (المشار إليه كذلك باسم "Kaspersky Security Center") خاص بالمحترفين الذين يقومون بتنصيب 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 المثبت 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
 - 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 تنصيب 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.

Kaspersky Security Center قيود

القيمة	نوع القيد
100,000	العدد الأقصى للأجهزة المدارة لكل خادم إدارة
300	الحد الأقصى لعدد الأجهزة التي تم تحديد خيار عدم قطع الاتصال عن خادم الإدارة عليها
10,000	الحد الأقصى لعدد مجموعات الإدارة
45,000,000	الحد الأقصى لعدد الأحداث التي سيتم تخزينها
2000	الحد الأقصى لعدد السياسات
2000	الحد الأقصى لعدد المهام
1,000,000	الحد الأقصى للعدد الإجمالي لعناصر الوحدات التنظيمية Active Directory، وحسابات المستخدمين، والأجهزة، ومجموعات الأمان
100	الحد الأقصى لعدد ملفات التعريف في سياسة ما
500	الحد الأقصى لعدد خوادم الإدارة الثانوية على خادم إدارة أساسي واحد
500	الحد الأقصى لعدد خوادم الإدارة الافتراضية
10,000	الحد الأقصى لعدد الأجهزة التي يمكن أن تغطيها نقطة توزيع واحدة (تستطيع نقاط التوزيع تغطية الأجهزة غير المحمولة فقط)
10000، بما في ذلك الأجهزة المحمولة	الحد الأقصى لعدد الأجهزة التي قد تستخدم بوابة اتصال واحدة
100000 ناقص عدد الأجهزة المدارة الثابتة	العدد الأقصى للأجهزة المحمولة لكل خادم إدارة

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 الموصى به من متطلبات الأجهزة إلى نظام إدارة قواعد البيانات و خادم 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 و خادم SQL على أجهزة مختلفة، وتحتوي الشبكة على 50,000 جهاز

تكوين الجهاز المثبت عليه خادم الإدارة

الأجهزة	القيمة
وحدة المعالجة المركزية	4 مراكز معالجة، 2500 ميغا هرتز
الذاكرة العشوائية	8 جيجابايت
محرك القرص الثابت	300 جيجابايت، RAID مستحسن
محول الشبكة	1 جيجابايت

تكوين الجهاز المثبت عليه خادم SQL

الأجهزة	القيمة
وحدة المعالجة المركزية	4 مراكز معالجة، 2500 ميغا هرتز
الذاكرة العشوائية	16 جيجابايت
محرك القرص الثابت	200 جيجابايت، SATA RAID
محول الشبكة	1 جيجابايت

خادم الإدارة و خادم SQL على الجهاز نفسه، وتحتوي الشبكة على 50,000 جهاز

تكوين الجهاز المثبت عليه خادم الإدارة و خادم SQL

الأجهزة	القيمة
وحدة المعالجة المركزية	8 مراكز معالجة، 2500 ميغا هرتز
الذاكرة العشوائية	16 جيجابايت
محرك القرص الثابت	500 جيجابايت، SATA RAID
محول الشبكة	1 جيجابايت

خادم الإدارة و خادم SQL على أجهزة مختلفة، وتحتوي الشبكة على 100,000 جهاز

تكوين الجهاز المثبت عليه خادم الإدارة

الأجهزة	القيمة
وحدة المعالجة المركزية	8 مراكز معالجة، 2.13 جيجا هرتز
الذاكرة العشوائية	8 جيجابايت
محرك القرص الثابت	1 تيرابايت، مع RAID
محول الشبكة	1 جيجابايت

تكوين الجهاز المثبت عليه خادم SQL

الأجهزة	القيمة
وحدة المعالجة المركزية	8 مراكز معالجة، 2.53 جيجا هرتز
الذاكرة العشوائية	26 جيجابايت

محرك القرص الثابت	500 جيجابايت، SATA RAID
محول الشبكة	1 جيجابايت

كانت الاختبارات تعمل بموجب الإعدادات التالية:

- التعيين التلقائي لنقاط التوزيع ممكن 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

عدد الأجهزة المدارة	الفاصل الزمني للمزامنة (بالدقائق)
10,000	15
20,000	30
30,000	45
40,000	60
50,000	75
100,000	150

حساب مساحة قاعدة البيانات

يمكن حساب مقدار المساحة التقريبية التي يجب أن يتم حجزها في قاعدة البيانات باستخدام الصيغة التالية:

$$600 * N * F * 1.2 + 2.5 * A + 2.3 * E + C, \text{ كيلو بايت}$$

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 (0.03 * C) 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) ضعف 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، فعليك مراعاة أن القيمة 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 %Application Data\KasperskyLab\adminkit% ALLUSERSPROFILE% بشكل تقريبي باستخدام المعادلة:

$$(724 * A + 0.17 * E + 0.15 * C) \text{ كيلو بايت}$$

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 %Application Data\KasperskyLab\adminkit% ALLUSERSPROFILE%) 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. بشكل افتراضي، يتم تخزين التصحيحات في مجلد ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\working\wusfiles% (يمكنك استخدام الأداة المساعدة klsrvswch لتحديد مجلد مختلف لتخزين التصحيحات). 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](#).

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 و 4 مراكز نواة.

• ذاكرة الوصول العشوائي: 8 جيجابايت

• القرص: SSD 120 جيجا بايت.

بالإضافة إلى ذلك، يجب أن تتمتع نقطة التوزيع بإمكانية الوصول إلى الإنترنت ويجب أن تظل متصلة دائمًا.

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 مثل 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.

حساب عدد نقاط التوزيع وتكوينهم

كلما زاد عدد الأجهزة العملية 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 العملية 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 نقاط التوزيع	عدد الأجهزة العملية في مقطع الشبكة
0 (لا تتم بتعيين نقاط توزيع)	أقل من 300
مقبول: $(N/10,000 + 1)$ ، موصى به: $(N/5000 + 2)$ ، حيث N هو عدد الأجهزة المتصلة بالشبكة	أكثر من 300

عدد نقاط التوزيع التي تم تعيينها حصريًا في شبكة تحتوي على مقاطع شبكات متعددة بناءً على عدد الأجهزة المتصلة بالشبكة

عدد نقاط التوزيع	عدد الأجهزة العملية لكل مقطع شبكة
0 (لا تتم بتعيين نقاط توزيع)	أقل من 10
1	10-100
مقبول: $(N/10,000 + 1)$ ، موصى به: $(N/5000 + 2)$ ، حيث N هو عدد الأجهزة المتصلة بالشبكة	أكثر من 100

استخدام الأجهزة العملية القياسية (محطات العمل) كنقاط توزيع

إذا كنت تخطط لاستخدام أجهزة عملية 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 نقاط التوزيع	عدد الأجهزة العملية في مقطع الشبكة
0 (لا تتم بتعيين نقاط توزيع)	أقل من 300
$(N/300 + 1)$ ، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل	أكثر من 300

عدد محطات العمل التي تعمل كنقاط توزيع في شبكة تحتوي على مقاطع شبكات متعددة بناءً على عدد الأجهزة المتصلة بالشبكة

عدد نقاط التوزيع	عدد الأجهزة العملية لكل مقطع شبكة
0 (لا تتم بتعيين نقاط توزيع)	أقل من 10
1	10-30
2	30-300
$(N/300 + 1)$ ، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل	أكثر من 300

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 10000 جهاز من الأجهزة المُدارة، بما في ذلك الأجهزة المحمولة.

تسجيل المعلومات حول أحداث المهام والسياسات

يقدم هذا القسم الحسابات المتعلقة بخزيرين 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 بشكل متكرر (على سبيل المثال، أكثر من مرة أسبوعيًا) وعلى رقم كبير إلى حد 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:

- **حفظ الأحداث المتعلقة بتقدم تنفيذ المهمة.** في هذه الحالة، تتلقى قاعدة البيانات فقط المعلومات حول بدء المهمة وتقدم المهمة وإكمالها (ناجحة، مع إرجاع تحذير أو خطأ) من كل جهاز يتم تشغيل المهمة عليه.
- **حفظ النتائج تنفيذ المهمة فقط.** 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 حد 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 القيام بذلك، ستقلل من عدد الأحداث الموجودة في قاعدة البيانات، وتزيد من سرعة تنفيذ السيناريوهات المقترنة بتحليل جدول الأحداث في قاعدة البيانات وخفض خطر الكتابة فوق الأحداث الحرجة بواسطة عدد كبير من الأحداث التي تتضمن تغييرات في حالة المهام الجماعية.

كما يمكنك تقليل مدة التخزين للأحداث المقترنة بمهمة أو سياسة. الفترة الافتراضية هي سبعة 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:

- الأحداث التي تتضمن تغييرات في الحالة الوسيطة للمهام الجماعية وحساب أحداث تطبيق السياسة الخاصة بقاعدة بيانات Kaspersky Security Center
 - يبدأ سجل أحداث Kaspersky في عرض إدخال 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 قليلًا، إذا لزم الأمر، ولكن إذا كان عدد الأجهزة الموجود في شبكتك صغير نسبيًا (أقل من 10000).

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 قاعدة البيانات ومهام جماعية لتحديث Kaspersky Endpoint Security جزءًا من الوظائف الأساسية لـ Kaspersky Security Center.

تُعتبر مهمة المخزون جزءًا من ميزة إدارة الثغرات الأمنية والتصحيحات ولا تتوفر في حالة عدم تفعيل هذه الميزة.

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
10000 أو أكثر	مرة في اليوم أو أقل

مهمة النسخ الاحتياطي لبيانات خادم الإدارة ومهمة صيانة قاعدة البيانات

يتوقف خادم الإدارة عن العمل عند تشغيل المهام التالية:

- النسخ الاحتياطي لبيانات خادم الإدارة
- صيانة قاعدة البيانات

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 مخزون البرنامج

يجب ألا يتجاوز عدد الملفات التنفيذية التي يستلمها خادم الإدارة من جهاز مفرد 150000 جهاز. عند وصول Kaspersky Security Center إلى هذا الحد، لا يمكنه تلقي أي ملفات جديدة.

في المعتاد، لا يتخطى عدد ملفات جهاز عميل مشترك 60000. عدد الملفات التنفيذية على خادم ملف يمكن أن يكون أكبر من أو يتخطى عقدة 150000.

أوضحت قياسات الاختبار أن نتيجة مهمة المخزون كانت كما يلي على جهاز يعمل بنظام تشغيل Windows 7 مثبت عليه Kaspersky Endpoint Security 11 وغير مثبت عليه تطبيقات جهة خارجية:

- عند إلغاء تحديد خانة الاختيار مخزون الوحدات النمطية لـ DLL ومخزون الملفات النصية: حوالي 3000 ملف.
- عند تحديد خانة الاختيار مخزون الوحدات النمطية لـ DLL ومخزون 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
تنصيب Kaspersky Endpoint Security 11.7 for Windows مع قواعد بيانات محدثة	390 ميغابايت	3.3 ميغابايت
تنصيب عميل الشبكة	75 ميغابايت	397 كيلوبايت
التنصيب المتزامن لعميل الشبكة و Kaspersky Endpoint Security 11.7 for Windows	459 ميغابايت	3.6 ميغابايت
التحديث المبدئي لقواعد بيانات مكافحة الفيروسات دون تحديث قواعد البيانات الموجودة في الحزمة (في حالة تعطيل مشاركة Kaspersky Security Network)	113 ميغابايت	1.8 ميغابايت
تحديث يومي لقواعد بيانات مكافحة الفيروسات؛ (في حال تمكين مشاركة Kaspersky Security Network)	22 ميغابايت	373 ميغابايت
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 ميغابايت

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 وفقاً 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.

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، قم بالاتصال بخدمة الدعم الفني. سيجيب أخصائيو خدمة الدعم الفني على كافة تساؤلاتك المتعلقة بتنصيب Kaspersky Security Center واستخدامه.

Kaspersky توفر الدعم لتطبيق Kaspersky Security Center أثناء دورة حياته (انظر [صفحة دورة حياة دعم المنتج](#)). قبل الاتصال بالدعم الفني، الرجاء 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

[Kaspersky CompanyAccount](#) 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 Kaspersky CompanyAccount، قم بزيارة [موقع ويب الدعم الفني](#).

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 تشمل 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](#).

(AWS Application Program Interface (AWS API)

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 و خادم 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.

Kaspersky Private Security Network (شبكة KSN الخاصة)

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:

- أجهزة المستخدم غير متصلة بالإنترنت.
- كان إرسال أي بيانات خارج الدولة أو شبكة اتصال محلية (LAN) لشركة محظور بموجب القانون أو سياسات أمان الشركة.

مسؤول Kaspersky Security Center

الشخص المسؤول عن إدارة عمليات التطبيق من خلال نظام Kaspersky Security Center للإدارة المركزية عن بُعد.

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 مع خادم الإدارة. تم تصميم خادم الويب لنقل حزم التنصيب المستقلة وملفات تعريف iOS MDM وملفات من المجلد المشترك، عبر أحد الشبكات.

(Kaspersky Security Network (KSN

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 قبل تطبيقات Kaspersky، ويحسن من أداء بعض مكونات الحماية، ويقلل أيضًا من احتمالية ظهور حالات إيجابية زائفة.

SSL

بروتوكول تشفير البيانات المستخدمة في الإنترنت والشبكات المحلية. يتم استخدام طبقة مأخذ توصيل أمانة (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 و Microsoft NAP.

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 حول بنية مجموعات الإدارة وأجهزة الكمبيوتر العميلة
- مستودع ملفات التنصيب للتعليد للتثبيت البعيد للتطبيقات (محتوى المجلدات: الحزم وإزالة تنصيب التحديثات).
- شهادة خادم الإدارة

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 مسبقاً 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 الاحتمالي 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.

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 بنفقها 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.

جهاز EAS

الجهاز المحمول المتصل بخادم الإدارة عبر بروتوكول Exchange ActiveSync. يمكن توصيل وإدارة الأجهزة التي تعمل بأنظمة تشغيل iOS وAndroid وWindows® Phone عبر استخدام البروتوكول Exchange ActiveSync.

جهاز iOS MDM

جهاز محمول متصل بخادم الأجهزة المحمولة التي تعمل بنظام iOS MDM باستخدام البروتوكول iOS MDM. يمكن توصيل الأجهزة التي تعمل بنظام تشغيل iOS وإدارتها بواسطة البروتوكول iOS MDM.

جهاز KES

جهاز محمول متصل بخادم الإدارة ومُدار عبر Kaspersky Endpoint Security for Android.

جهاز حماية UEFI

تكامل الجهاز المثبت عليه Kaspersky Anti-Virus for UEFI 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.

تحديث

تمت استعادة إجراء استبدال أو إضافة ملفات جديدة (قواعد بيانات أو وحدات نمطية للتطبيق) من خوادم تحديث Kaspersky.

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 المثبتة واستخدام مفاتيح الترخيص وعدد التهديدات المكتشفة 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 فوراً 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 Exchange

هو أحد مكونات Kaspersky Security Center، والذي يتيح لك توصيل الأجهزة المحمولة Exchange ActiveSync بخادم الإدارة.

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 اعتماداً على الموقف الذي وقع فيه الحدث.

خوادم تحديث Kaspersky

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

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 للمصادقة في وحدات التحكم الإدارية ولتبادل البيانات مع الأجهزة العملية. يتم إنشاء الشهادة تلقائياً عند تثبيت خادم الإدارة، ومن ثم يتم تخزينها على خادم الإدارة.

صورة جهاز (AMI Amazon)

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 مشتركاً بين جميع تطبيقات الشركة لـ Microsoft® Windows®. تتوفر إصدارات منفصلة من عميل الشبكة لتطبيقات Kaspersky التي تم تطويرها لأنظمة Unix-like OS و macOS.

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 نسخ 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.

مجموعة الدور

مجموعة من مستخدمي الأجهزة المحمولة Exchange ActiveSync الذين تم منحهم حقوق مطابقة [لحقوق المسؤول](#).

محطة عمل المسؤول

تم تثبيت جهاز يحتوي على وحدة تحكم الإدارة. 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 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 تفضيلاً بين الثغرات الأمنية التي ينبغي للتصحيحات إصلاحها.

مفتاح اشتراك إضافي

مفتاح يُصادق على حق استخدام التطبيق لكن لا يتم استخدامه حالياً.

مفتاح مفعّل

مفتاح الترخيص الذي يستخدمه التطبيق حاليًا.

مفتاح وصول AWS IAM

تركيبة تتكون من معرف مفتاح (يبدو وكأنه "AKIAIOSFODNN7EXAMPLE") ومفتاح سري (يبدو وكأنه "wJalrXUtnFEMI/K7MDENG/bPxrFcYEXAMPLEKEY"). ينتمي هذا الاقتران إلى مستخدم IAM ويستخدم للحصول وصول إلى خدمات AWS.

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](https://aws.amazon.com/console).

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 التعريف

مجموعة من الإعدادات الخاصة بالأجهزة المحمولة في Exchange [Exchange](#) التي تحدد سلوكها عند الاتصال بخادم Exchange server.

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 بتنصيب 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 الموصولة 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 الموصولة 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 للبعيد 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.

وحدة تحكم الإدارة

أحد مكونات Kaspersky Security Center الذي يوفر واجهة مستخدم لخدمات الإدارة لخادم الإدارة و عميل 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

تُعد العلامات التجارية المسجلة وعلامات الخدمة ملكية خاصة لأصحابها.

تُعد Microsoft و Active Directory و ActiveSync و BitLocker و Excel و Forefront و Internet Explorer و InfoPath و Hyper-V و OneNote و SQL Server و SharePoint و PowerPoint و PowerShell و Office 365 و MS-DOS و MultiPoint و Microsoft و Edge و Windows Mobile و Windows Media و Windows PowerShell و Windows و Win32 و Visio و Tahoma و Skyp و Outlook و Windows Server و Windows Phone و Windows Vista و Windows Azure و علامات تجارية مسجلة لمجموعة شركات Microsoft.

Adobe و Acrobat و Flash و Shockwav و PostScript هم علامات تجارية مسجلة أو علامات تجارية لشركة Adobe في الولايات المتحدة و/أو بلدان أخرى.

إن AirPlay و AirDrop و AirPrint و App Store و Apple و Apple Configurator و AppleScript و FaceTime و FileVault و iBook و Tiger و Snow Leopard و Safari و OS X و Mac OS و Mac و macOS و Leopard و iTunes و iPhone و iPad و iCloud و iBooks و QuickTime و Touch ID هي علامات تجارية تابعة لشركة Apple Inc. ومسجلة في الولايات المتحدة الأمريكية وبلدان ومناطق أخرى.

إن AMD و AMD64 هي علامات تجارية أو علامات تجارية مسجلة لشركة Advanced Micro Devices, Inc.

تُعد Amazon و Amazon Web Services و AWS و Amazon EC2 و AWS Marketplace و علامات مسجلة تملكها شركة Amazon.com, Inc. أو شركاتها التابعة في الولايات المتحدة الأمريكية و/أو في البلدان الأخرى.

Android و Chrome و Chromium و Dalvik و Firebase و Google و Google Chrome و Google Earth و Google Play و Google و Hangouts و Maps و YouTube هي علامات تجارية لشركة Google LLC.

Apache و شعار Apache هما علامتان تجاريتان لشركة Apache Software Foundation.

إن BlackBerry مملوكة لشركة Research In Motion Limited ومسجلة في الولايات المتحدة ويمكن أن تكون معلقة أو مسجلة في بلدان أخرى.

كلمة Bluetooth و علامتها وشعاراتها تعتبر مملوكة لشركة Bluetooth SIG, Inc.

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.

تعد Cisco، و Cisco Systems، و Cisco Jabber، و iOS علامات تجارية مسجلة لشركة Cisco Systems, Inc. و/أو الشركات التابعة لها في الولايات المتحدة وبلدان معينة أخرى.

تعد CVE علامة تجارية مسجلة لشركة MITER Corporation.

تُعد Citrix و XenServer علامات تجارية لشركة Citrix Systems, Inc. و/أو واحدة أو أكثر من الشركات التابعة والمسجلة في مكتب براءات الاختراع بالولايات المتحدة الأمريكية وفي البلدان الأخرى.

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.

Debian هي علامة تجارية مسجلة لشركة Software in the Public Interest, Inc.

Dropbox هي علامة تجارية مملوكة لشركة Dropbox, Inc.

FusionCompute و FusionSphere علامتان تجاريتان لشركة Huawei Technologies Co., Ltd المسجلة في الصين وبلدان أخرى.

Firebird هي علامة تجارية مسجلة لمؤسسة Firebird Foundation.

Foxit هي علامة تجارية مسجلة لشركة Foxit Corporation.

Firefox و Mozilla و Thunderbird هي علامات تجارية مملوكة لمؤسسة Mozilla Foundation.

إن FreeBSD علامة تجارية مسجلة لمؤسسة FreeBSD foundation.

إن Oracle و Java و JavaScript و TouchDown علامات تجارية مسجلة لشركة Oracle و/أو شركاتها التابعة.

إن OpenAPI علامة تجارية لمؤسسة Linux Foundation.

إن QRadar و IBM علامات تجارية تابعة لشركة International Business Machines Corporation، مسجلة في العديد من البلدان حول العالم.

تُعد Intel و Core و Xeon علامات تجارية لشركة Intel Corporation في الولايات المتحدة و/أو بلدان أخرى.

تعد CentOS علامة تجارية لشركة Red Hat, Inc.

إن Ansible و Fedora و Red Hat و Red Hat Enterprise Linux علامات تجارية أو علامات تجارية مسجلة لشركة Red Hat, Inc. أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

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.

Micro Focus هو علامة تجارية أو علامة تجارية مسجلة لشركة Micro Focus (IP) Limited أو فروعها في المملكة المتحدة والولايات المتحدة الأمريكية وبلدان أخرى.

وعلامة Node.js هي علامة تجارية تابعة لشركة Joyent, Inc.

تعتبر Novell و NetWare علامتان تجاريتان مسجلتان لشركة Novell Inc. في الولايات المتحدة الأمريكية وبلدان أخرى.

يُعتبر Parallels وشعار Parallels هما علامتان تجاريتان أو علامتان تجاريتان مسجلتان لشركة Parallels International GmbH في كندا والولايات المتحدة أو في أي مكان آخر.

تُعد Puppet علامة تجارية أو علامة تجارية مسجلة لشركة Puppet, Inc.

تُعد Python علامة تجارية أو ماركة مسجلة لشركة Python Software Foundation.

Radmin هي علامة تجارية مسجلة لشركة Famatech.

تُعد Samsung علامة تجارية لشركة SAMSUNG في الولايات المتحدة أو البلدان الأخرى.

SPL و Splunk هي علامات تجارية مسجلة لشركة Splunk, Inc. في الولايات المتحدة الأمريكية وبلدان أخرى.

Symbian هي علامة تجارية مملوكة لشركة Symbian Foundation Ltd.

SUSE هي علامة تجارية مسجلة لشركة SUSE LLC في الولايات المتحدة الأمريكية وبلدان أخرى.

تُعد Ubuntu علامة تجارية مسجلة لشركة Canonical Ltd.

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.

إن VMware و VMware vSphere و VMware Workstation علامات تجارية مسجلة أو علامات تجارية لشركة VMware, Inc. في الولايات المتحدة و/أو نطاقات قضائية أخرى.

Kaspersky Security Center 14 Web Console يحتوي على عدد من القيود التي ليست حرجة لتشغيل التطبيق:

- أثناء تسجيل الدخول إلى Kaspersky Security Center 14 Web Console، إذا كنت تستخدم مصادقة المجال، وتحدد خادم إدارة افتراضي للاتصال به، ثم تقوم بتسجيل الخروج، ومحاولة تسجيل الدخول إلى مخدّم الإدارة الأساسي، فسيصل Kaspersky Security Center 14 Web Console بخادم الإدارة الافتراضي. للاتصال بمخدّم الإدارة الأساسي، أعد فتح المتصفح.
- إذا قمت بتحديد إعدادات الخادم الوكيل في خصائص خادم الإدارة، ثم قمت بتمكين الخيار **عدم استخدام الخادم الوكيل** في مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، فسيتم تجاهل هذا الخيار ويتم إنشاء الاتصال من خلال الخادم الوكيل.
- إذا فتحت Kaspersky Security Center 14 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.
- يحدث خطأ عند محاولة استعادة كائن من مستودع النسخ الاحتياطي (العمليات ← المستودعات ← النسخ الاحتياطي) أو إرسال الكائن إلى Kaspersky.
- يرسل الجهاز المُدار الذي يحتوي على أكثر من محول شبكة واحد معلومات خادم الإدارة حول عنوان MAC لمحول الشبكة غير المستخدم للاتصال بخادم الإدارة.
- الإعدادات المقفلة في السياسة الرئيسية لـ Kaspersky Endpoint Security for Linux موروثة، ولكنها غير مقفلة في السياسات الفرعية.
- بعد الترقية إلى Kaspersky Security Center 14، إذا قمت بالتبديل من خادم إدارة أساسي إلى خادم ثانوي، ثم عدت إلى الخادم الأساسي، ثم حاولت العودة إلى الخادم الثانوي، فلن يتمكن Kaspersky Security Center 14 Web Console من فتح الخادم الثانوي. تتكرر هذه المشكلة فقط إذا تم تثبيت المكون الإضافي للويب لـ Kaspersky Endpoint Security for Windows الإصدار 11.9.
- في وحدة التحكم الإدارية المعتمدة على MMC، عند إنشاء سياسة لـ Kaspersky Industrial CyberSecurity for Linux Nodes 1.0، يعرض Kaspersky Security Center رسالة خطأ حول إنشاء تفريغ تشخيصي. ومع ذلك، يتم إنشاء السياسة بنجاح.
- يمكن حذف فئة التطبيق التي أضفتها إلى ميزة التحكم في التطبيق في سياسة Kaspersky Endpoint Security for Linux.
- في أداة الرسم البياني الدائري على جزء المعلومات، لا يتغير لون النص إلى فاتح بعد تبديل سمة وحدة التحكم إلى اللون الداكن.
- قد يتم عرض حالة غير صحيحة لمهمة محلية في قائمة المهام في خصائص الجهاز.
- عند إضافة أكثر من 200 استثناء إلى قاعدة التحكم في العيوب التكميلية، يتم عرض رسالة خطأ بدلاً من رسالة تحذير.
- في قسم **فئات التطبيق**، إذا تم عرض العمود **المستخدمة في السياسات**، فلا يمكن إخفاؤه.
- في إعدادات مهمة تغيير خادم الإدارة، توجد بعض الخيارات في غير محلها.
- في سياسة عميل الشبكة، يحتوي قسم **جدول الاتصال** على عنوان غير صحيح.
- استقصاء شبكة Quick/Full Windows يُنتج نتيجة فارغة.
- إذا كنت تستخدم الأداة المساعدة sysprep.exe لالتقاط صورة لنظام التشغيل وإضافة الإعدادات الضرورية، فسيتم نشر صورة نظام التشغيل الملتقطة بدون هذه الإعدادات.
- في حالة تثبيت Kaspersky Security Center 14 Web Console باستخدام إدارة الهوية والوصول، فمن ثم عليك تغيير خادم إدارة Kaspersky Security Center 14 Web Console، ولن تحصل إدارة الهوية والوصول على معلومات بشأن خادم الإدارة الجديد.
- أزرار **استعادة** و **إرسال إلى Kaspersky** في قسم **العمليات** ← **المستودعات** ← **النسخ الاحتياطي** لا يعمل.
- في قسم **الشهادات** في نافذة خصائص خادم الإدارة، عند إضافة شهادة، على سبيل المثال شهادة خادم الويب، يحجب الزر **إغلاق ("X")** الحقل **نوع الشهادة**، ويعرض الزر **إظهار** غير الضروري.

- إعادة تحميل خدمة خادم الإدارة على خادم إدارة ثانوي تتسبب في قطع الاتصال بين Kaspersky Security Center 14 Web Console وخادم الإدارة الأساسي.
- يتم عرض رسائل الخطأ الخاصة بهجمات Zip Slip و Zip Bomb باللغة الإنجليزية فقط.
- لا يمكن فتح نافذة خصائص دور من قائمة الأدوار المعينة للمستخدم.
- لا يمكن فرز الإخطارات حسب التاريخ.
- في خصائص تحديثات Microsoft، في قسم الأجهزة، لا يتوفر البحث حسب "حالة التثبيت" و "عنوان IP".
- نشر Windows 10 الإصدار 2004 عبر PXE (Preboot Execution Environment) غير مدعوم.
- لا يتم استبدال المرشحات القديمة في تحديثات الحدث بفلاتر جديدة؛ لتجنب ذلك، يمكنك حذف عوامل التصفية القديمة يدويًا.