kaspersky

Kaspersky Security Center 14 Linux

جدول المحتويات

التطبيق غير متوافق

الحماية ضد فيروسات الشبكة

الشهادة المشتركة

المهمة

بوابة الاتصال

تحديث

حالة الحماية

حالة حماية الشبكة

حزمة التثبيت

حقوق المسؤول

خادم الإدارة

خادم الإدارة الافتراضي

خادم الإدارة الرئيسي

خطورة الحدث

خوادم تحديث Kaspersky

سياسة

شهادة خادم الإدارة

عميل الشبكة

عميل خادم الإدارة (الجهاز العميل)

فترة الترخيص

قواعد بيانات مكافحة الفيروسات

مالك الجهاز

متجر التطبيقات

مجال البث

مجلد النسخ الاحتياطي

مجموعة الإدارة

مجموعة التطبيقات المرخصة

مجموعة الدور

محطة عمل المسؤول

مسؤول العميل

مسؤول موفر الخدمة

مستخدمين داخليين

مستودع الأحداث

مفتاح اشتراك إضافي

مفتاح مفعل

ملف التعريف

ملف المفتاح

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

	**ما الجديد** اكتشف كل ما هو جديد في أحدث إصدار للتطبيق.		**تطبيقات Kaspersky. الترخيص والتفعيل** تفعيل تطبيقات Kaspersky في بضع خطوات.
	**متطلبات الأجهزة والبرامج** تحقق أيًا من أنظمة التشغيل وإصدارات التطبيق مدعومة.		**تكوين حماية الشبكة** إدارة أمان المؤسسة
	**التثبيت:** تثبيت خادم الإدارة و Kaspersky Security Center 14 Web Console		**تطبيقات Kaspersky. تحديث قواعد البيانات والوحدات النمطية للبرامج** الحفاظ على موثوقية نظام الحماية.
	**اكتشاف الأجهزة المتصلة بالشبكة** اكتشف الأجهزة الجديدة والموجودة على شبكة مؤسستك.		**المراقبة وإعداد التقارير** عرض البنية الأساسية الخاصة بك، وحالات الحماية والإحصائيات.
	**تطبيقات Kaspersky. النشر المركزي** نشر تطبيقات Kaspersky.		**تعديل نقاط التوزيع و/أو بوابات الاتصال** تكوين نقاط التوزيع.

ما الجديد

Kaspersky Security Center 14 Linux

لدى Kaspersky Security Center 14 العديد من الميزات والتحسينات الجديدة:

- إلى جانب تنزيل التحديثات إلى مستودع خادم الإدارة، يمكن الآن تنزيل قواعد بيانات مكافحة الفيروسات لتطبيقات أمان Kaspersky من خلال مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع.

- يمكن نشر وتحديث قواعد بيانات مكافحة الفيروسات ووحدات التطبيق على الأجهزة المدارة من خلال خادم الإدارة أو نقاط التوزيع. يمكنك اختيار نظام التحديث الأمثل لمؤسستك، لتقليل الحمل على خادم الإدارة وتحسين حركة مرور البيانات على شبكة الشركة.

- يقوم Kaspersky Security Center بتنزيل التحديثات من خوادم تحديث Kaspersky فقط تلك التحديثات التي تطلبها تطبيقات أمان Kaspersky. هذا يقلل من حجم البيانات التي تم تنزيلها.

- يمكنك الآن استخدام ميزة ملفات الاختلافات لتنزيل قواعد بيانات مكافحة الفيروسات ووحدات البرامج. 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.

- تمت إضافة مهمة التحقق من صحة التحديث. باستخدام هذه المهمة، يمكنك التحقق تلقائيًا من التحديثات التي تم تنزيلها للتحقق من قابلية التشغيل والأخطاء قبل تثبيت التحديثات على الأجهزة المدارة.

حول Kaspersky Security Center Linux

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

تم تصميم Kaspersky Security Center Linux (يُشار إليه أيضًا باسم Kaspersky Security Center) لنشر وإدارة حماية أجهزة Linux® باستخدام خادم الإدارة المستند إلى Linux لتلبية متطلبات بيئات Linux الخالصة.

يمكّنك Kaspersky Security Center Linux من تثبيت تطبيقات أمان Kaspersky على الأجهزة الموجودة على شبكة الشركة، وتشغيل مهام الفحص والتحديث عن بُعد، وإدارة سياسات الأمان للتطبيقات المدارة. بصفتك مسؤولاً، يمكنك استخدام لوحة معلومات مفصلة توفر لقطة لحالات جهاز الشركة، وتقارير مفصلة، وإعدادات دقيقة في سياسات الحماية.

بالمقارنة مع Kaspersky Security Center الذي يحتوي على خادم إدارة يستند إلى Windows®، فإن Kaspersky Security Center Linux لديه مجموعة ميزات مختلفة.

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

باستخدام Kaspersky Security Center يمكنك القيام بما يلي:

- بإنشاء ترتيب هرمي لخوادم الإدارة لإدارة شبكة المؤسسة، بالإضافة إلى الشبكات الموجودة في المكاتب البعيدة أو مؤسسات العميل.
  المؤسسة العميلة عبارة عن مؤسسة يقوم مزود الخدمة بضمان حمايتها ضد الفيروسات.
- قم بإنشاء ترتيب هرمي لمجموعات الإدارة لإدارة مجموعة محددة من الأجهزة العميلة ككل.
- إدارة نظام الحماية ضد الفيروسات الذي تم إنشاؤه استنادًا إلى تطبيقات Kaspersky.
- أجر التثبيت عن بُعد للتطبيقات عبر Kaspersky وموردي البرامج الآخرين.
- تنفيذ نشر مركزي لمفاتيح الترخيص لتطبيقات Kaspersky على الأجهزة العميلة ومراقبة استخدامها وإعادة تجديد التراخيص.
- تلقي إحصاءات وتقارير عن تشغيل التطبيقات والأجهزة.
- تلقي إخطارات حول الأحداث الحرجة أثناء تشغيل تطبيقات Kaspersky.
- 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، على https://www.kaspersky.com) أو عبر الشركات الشريكة.

إذا اشتريت Kaspersky Security Center Linux من متجر عبر الإنترنت، يمكنك نسخ التطبيق من موقع الويب للمتجر. يتم إرسال المعلومات المطلوبة لتنشيط التطبيق عبر البريد الإلكتروني بعد الدفع.

متطلبات الأجهزة والبرامج

خادم الإدارة

الحد الأدنى لمتطلبات الجهاز:

- وحدة المعالجة المركزية 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.

أنظمة التشغيل التالية مدعومة:

- 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) 32 بت/64 بت
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32 بت/64 بت
- CentOS 7.x 64 بت
- Red Hat Enterprise Linux Server 8.x 64 بت
- Red Hat Enterprise Linux Server 7.x 64 بت
- SUSE Linux Enterprise Server 12 (جميع حزم الخدمة) 64 بت
- SUSE Linux Enterprise Server 15 (جميع حزم الخدمة) 64 بت
- Astra Linux Special إصدار 1.7 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي) 64 بت
- Astra Linux Special إصدار 1.6 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي) 64 بت
- Astra Linux Common إصدار 2.12 64 بت
- Alt Server 10 64 بت
- Alt Server 9.2 64 بت
- Alt 8 SP Server (LKNV.11100-01) 64 بت
- Alt 8 SP Server (LKNV.11100-02) 64 بت
- Alt 8 SP Server (LKNV.11100-03) إصدار 64 بت
- Oracle Linux 7 64 بت
- Oracle Linux 8 64 بت
- RED OS 7.3 Server 64 بت
- RED OS 7.3 إصدار معتمد 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
- 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 البرنامج المغلق 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

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

- مجتمع MySQL 5.7 32 بت/64 بت
- مجتمع MySQL 8.0 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 10.1.30 وأحدث 32 بت / 64 بت

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.

أحد أنظمة التشغيل التالية (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 64 بت
- Astra Linux Special إصدار 1.6 (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 بت
- Alt Server 10 64 بت
- Astra Linux Special إصدار 1.7 (بما في ذلك وضع بيئة البرنامج المغلق 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

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
- Safari 15 على macOS

عميل الشبكة

الحد الأدنى لمتطلبات الجهاز:

- وحدة المعالجة المركزية 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 للأجهزة التي تعمل بنظام Linux: يجب تثبيت مترجم لغة Perl الإصدار 5.10 أو أعلى.

أنظمة التشغيل التالية مدعومة:

- 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) 32 بت/64 بت
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 بت
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32 بت/64 بت
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 بت/64 بت
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 بت/64 بت
- CentOS 8.x 64 بت
- CentOS 7.x 64 بت
- CentOS 7.x ARM 64 بت
- Red Hat Enterprise Linux Server 8.x 64 بت
- Red Hat Enterprise Linux Server 7.x 64 بت
- Red Hat Enterprise Linux Server 6.x 32 بت/64بت
- SUSE Linux Enterprise Server 12 (جميع حزم الخدمة) 64 بت
- SUSE Linux Enterprise Server 15 (جميع حزم الخدمة) 64 بت
- SUSE Linux Enterprise Desktop 15 (جميع حزم الخدمة) 64 بت
- SUSE Linux Enterprise Desktop 15 (حزمة الخدمة 3) ARM 64 بت
- openSUSE 15 64 بت
- نظام EulerOS 2.0 SP8 ARM
- نظام التشغيل Pardus OS 19.1 64 بت
- Astra Linux Special إصدار 1.7 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي) 64 بت
- Astra Linux Special إصدار 1.6 (بما في ذلك وضع بيئة البرنامج المغلق والوضع الإلزامي) 64 بت
- Astra Linux Common إصدار 2.12 64 بت
- Astra Linux Special الإصدار 4.7 ARM
- Alt Server 10 64 بت
- Alt Server 9.2 64 بت
- Alt Workstation 10 32 بت / 64 بت
- محطة العمل البديلة 9.2 32 بت / 64 بت
- Alt 8 SP Server (LKNV.11100-01) 64 بت

- Alt 8 SP Server (LKNV.11100-02) 64 بت
- Alt 8 SP Server (LKNV.11100-03) إصدار 64 بت
- Alt 8 SP Workstation (LKNV.11100-01) 32 بت / 64 بت
- Alt 8 SP Workstation (LKNV.11100-02) 32 بت / 64 بت
- Alt 8 SP Workstation (LKNV.11100-03) 32 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 بت DE: MATE)

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 البرنامج المغلق 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

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

حول Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console هو تطبيق ويب مصمم لإدارة حالة نظام أمان شبكات المؤسسة التي تتم حمايتها باستخدام تطبيقات Kaspersky.

يمكنك إجراء ما يلي باستخدام التطبيق:

- إدارة حالة نظام أمان المؤسسة.
- تثبيت تطبيقات Kaspersky على الأجهزة على شبكتك وإدارة التطبيقات المثبتة.
- إدارة السياسات المنشأة للأجهزة الموجودة على شبكتك.
- إدارة حسابات المستخدمين.
- إدارة المهام للتطبيقات المثبتة على أجهزة شبكتك.
- عرض التقارير على حالة نظام الأمان.
- إدارة تسليم التقارير إلى مديري النظام وخبراء تكنولوجيا المعلومات الآخرين.

Kaspersky Security Center 14 Web Console يوفر واجهة ويب تضمن تفاعل بين جهازك وخادم الإدارة على مستعرض. خادم الإدارة هو تطبيق مصمم لإدارة تطبيقات Kaspersky مثبتة على أجهزة شبكتك. يتصل خادم الإدارة بالأجهزة على شبكتك عبر قنوات تحميها طبقة مآخذ التوصيل الآمنة (SSL). 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 التوصيل 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.

قائمة من تطبيقات Kaspersky المدعومة

يدعم Kaspersky Security Center Linux النشر المركزي وإدارة Kaspersky Endpoint Security لنظام التشغيل Linux. يسمح هذا التطبيق بحماية محطات العمل وخوادم الملفات. راجع صفحة ويب دورة حياة دعم المنتج لإصدارات التطبيقات.

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

يوفر Kaspersky Kaspersky Security Center كحل محلي لمنصتين أساسيتين – Windows وLinux. في الحل المستند إلى Windows، تقوم بتثبيت خادم الإدارة على جهاز يعمل بنظام التشغيل Windows، ويحتوي الحل المستند إلى Linux على إصدار خادم الإدارة المصمم ليتم تثبيته على جهاز Linux.

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

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

الميزة أو الملكية	Kaspersky Security Center	
	حل قائم على Windows	حل قائم على Linux
موقع خادم الإدارة	في أماكن العمل	في أماكن العمل
موقع نظام إدارة قواعد البيانات (DBMS)	في أماكن العمل	في أماكن العمل
نظام تشغيل لتثبيت خادم الإدارة عليه	Windows	Linux
نوع وحدة التحكم الإدارية	في أماكن العمل وعلى شبكة الإنترنت	على شبكة الإنترنت
نظام تشغيل لتثبيت وحدة الإدارة المستندة إلى الويب عليه	نظام التشغيل Windows أو Linux	نظام التشغيل Windows أو Linux
التسلسل الهرمي لخوادم الإدارة	✓	✓
التسلسل الهرمي لمجموعة الإدارة	✓	✓
استقصاء الشبكة	✓	✓ (حسب نطاقات IP فقط)

أقصى عدد من الأجهزة المدارة	100،000	20,000
حماية الأجهزة المدارة التي تعمل بأنظمة Windows وmacOS وLinux	✓	– (حماية أجهزة Linux فقط)
حماية الأجهزة المحمولة	✓	–
حماية الأجهزة الافتراضية	✓	–
حماية البنية التحتية السحابية العامة	✓	–
إدارة أمان تتمحور حول الجهاز	✓	✓
إدارة الأمان تتمحور حول المستخدم	✓	✓
سياسات التطبيق	✓	✓
مهام تطبيقات Kaspersky	✓	✓
Kaspersky Security Network	✓	–
وكيل KSN	✓	–
Kaspersky Private Security Network	✓	–
النشر المركزي لمفاتيح الترخيص لتطبيقات Kaspersky	✓	✓
دعم خوادم الإدارة الافتراضية	✓	✓
تثبيت تحديثات برامج الطرف الثالث وإصلاح الثغرات الأمنية لبرامج الطرف الثالث	✓	– (باستخدام مهمة التثبيت عن بعد فقط)
إشعارات حول الأحداث التي وقعت على الأجهزة المدارة	✓	✓
إنشاء وإدارة حسابات المستخدمين	✓	✓
مراقبة السياسات وحالة المهام	✓	✓
نشر مجموعة تجاوز الفشل من Kaspersky	✓	✓

المفاهيم الأساسية

يوضح هذا القسم المفاهيم الأساسية ذات الصلة بتطبيق Kaspersky Security Center Linux.

خادم الإدارة

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

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

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

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

ويقوم خادم الإدارة بالوظائف التالية:

- تخزين بنية مجموعات الإدارة
- تخزين معلومات حول تكوين الأجهزة العميلة.
- ترتيب المستودعات لحزم توزيع التطبيقات.
- تثبيت التطبيقات عن بُعد على الأجهزة العميلة وإزالة التطبيقات.
- تحديث قواعد بيانات التطبيقات والوحدات النمطية لبرامج تطبيقات Kaspersky
- إدارة السياسات والمهام على الأجهزة العميلة.
- تخزين معلومات حول الأحداث التي وقعت على الأجهزة العميلة.
- إنشاء تقارير حول تشغيل تطبيقات Kaspersky.
- نشر مفاتيح الترخيص على أجهزة العملاء، وتخزين معلومات حول مفاتيح الترخيص.
- إعادة توجيه الإخطارات حول تقدم المهام (مثل اكتشاف فيروس على جهاز عميل).

تسمية خوادم الإدارة في واجهة التطبيق

في واجهة 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 وحدةKaspersky 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 مُقيَّد. ثم ستتضمن مجموعات الإدارة الخاصة بخادم الإدارة الرئيسي الأجهزة العميلة الخاصة بجميع خوادم الإدارة الثانوية. وهكذا، يمكن إدارة الأقسام المنعزلة والمستقلة من الشبكات بواسطة خوادم إدارة مختلفة تتم إدارتها في المقابل بواسطة الخادم الرئيسي.

خوادم الإدارة الافتراضية حالة خاصة من خوادم الإدارة الثانوية.

في التسلسل الهرمي، لا يمكن أن يعمل خادم إدارة Kaspersky Security Center Linux إلا كخادم ثانوي يُدار بواسطة خادم إدارة أساسي لـ Kaspersky Security Center المستند إلى Windows أو Kaspersky Security Center Cloud Console.

يمكن استخدام التسلسل الهرمي لخوادم الإدارة للقيام بما يلي:

- تخفيف الحمل على خادم الإدارة (مقارنةً بخادم إدارة منفرد مثبت على الشبكة بالكامل).
- تخفيف حركة مرور الإنترانت وتبسيط التعامل مع المكاتب البعيدة. وليس من الضروري إنشاء اتصالات بين خادم الإدارة الرئيسي وجميع الأجهزة المتصلة بالشبكة، والتي قد توجد في مناطق أخرى على سبيل المثال. ويكفي تثبيت خادم إدارة تابع في كل قطاع شبكة، وتوزيع الأجهزة فيما بين مجموعات إدارة الخوادم التابعة، وإنشاء اتصالات بين الخوادم التابعة والخوادم الرئيسية عبر قنوات اتصال سريعة.
- توزيع المسؤوليات بين مسؤولي أمان مكافحة الفيروسات. جميع إمكانيات الإدارة المركزية ومراقبة حالة أمان مكافحة الفيروسات في شبكات الشركة تظل متوفرة.
- كيف يستخدم موفرو 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 Linux ومصمم لإدارة الحماية ضد الفيروسات لشبكة مؤسسة 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 Linux على إعادة تشغيل خادم الإدارة الرئيسي وجميع خوادم الإدارة الافتراضية.

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

خادم الويب

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

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

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

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

تكون بنية جملة رابط نقل المعلومات كما يلي:

```
<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 المستخدم وصولاً إليه.

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

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

عميل الشبكة

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

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

- تتميز بالاسم "عميل شبكة Kaspersky Security Center 14 Linux"
- تعيين للبدء تلقائيًا عند بدء تشغيل نظام التشغيل
- باستخدام حساب النظام المحلي

ويُطلق على الجهاز الذي لديه عميل شبكة مثبت به جهاز مُدار أو جهاز. يمكنك تثبيت عميل الشبكة من أحد المصادر التالية:

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

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

أسماء العملية التي يبدأها عميل الشبكة هي كما يلي:

- klnagent64.service (لنظام تشغيل 64 بت)
- klnagent.service (لنظام تشغيل 32 بت)

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

مجموعات الإدارة

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

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

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

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

يمكنك إنشاء تسلسلات هرمية تتمتع بأية درجة من التداخل لخوادم الإدارة والمجموعات. يمكن أن يتضمن مستوى التسلسل الهرمي الفردي خوادم إدارة ثانوية وافتراضية ومجموعات وأجهزة مُدارة. يمكنك تحريك الأجهزة من مجموعة إلى أخرى من دون تحريكها فعليًا. على سبيل المثال، إذا تغير منصب الموظف في المؤسسة من منصب المحاسب إلى المُطوّر، فبإمكانك تحريك 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 Linux ومثبت عليه عميل الشبكة. يمكنك إدارة مثل هذه الأجهزة عن طريق إنشاء مهام وسياسات للتطبيقات المثبتة على هذه الأجهزة. يمكنك كذلك تلقي التقارير من الأجهزة المُدارة.

يمكنك جعل جهاز مُدار يعمل كنقطة توزيع وكبوابة اتصال.

يمكن إدارة الجهاز بواسطة خادم إدارة واحد فقط. يمكن لخادم إدارة واحد إدارة ما يصل إلى 20,000 جهاز.

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

يشار إلى الأجهزة التي تم تثبيت خادم Kaspersky Security Center 14 Web Console Server عليها على أنها محطات عمل المسؤول. يمكن للمسؤولين استخدام هذه الأجهزة في الإدارة المركزية عن بُعد لتطبيقات Kaspersky المُثبتة على أجهزة العملاء.

ولا توجد قيود على عدد محطات عمل المسؤول. من أي 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 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 المهمات والسياسات المخصصة للتطبيق.

يمكنك تنزيل المكونات الإضافية للإدارة من صفحة ويب خدمة العملاء لـ Kaspersky.

يوفر مكون الإدارة الإضافي ما يلي:

- واجهة لإنشاء وتحرير مهمات التطبيقات وإعداداتها
- واجهة لإنشاء وتحرير السياسات وملفات تعريف السياسة للتحكم عن بُعد والتكوين المركزي لتطبيقات Kaspersky والأجهزة.
- يتم إنشاء نقل الأحداث عن طريق التطبيقات
- وظائف Kaspersky Security Center 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. يكون للسياسة إحدى الحالات التالية:

حالة السياسة	

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

تعمل السياسات وفق القواعد التالية:

- يمكن تكوين عدة سياسات بقيم مختلفة لتطبيق واحد.
- يمكن تفعيل سياسة واحدة فقط للتطبيق الحالي.
- يمكن أن يكون للسياسة سياسات فرعية.

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

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

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

تعمل ملفات التعريفية للسياسة وفقًا للقواعد التالية:

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

ملفات تعريف السياسة

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

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

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

المهام

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

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

يمكن إجراء المهام على خادم الإدارة وعلى الأجهزة.

يتم إجراء المهام التالية على خادم الإدارة:

- التوزيع التلقائي للتقارير
- تنزيل التحديثات إلى مستودع خادم الإدارة
- النسخ الاحتياطي لبيانات خادم الإدارة
- صيانة قاعدة البيانات
- 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 وحدة تحكم Kaspersky Security Center 14 Web أو بواسطة مستخدم جهاز بعيد (على سبيل المثال، عبر واجهة تطبيق الأمان). في حالة تعديل مهمة محلية بواسطة المسؤول ومستخدم الجهاز المُدار في الوقت نفسه، فستسري التغييرات التي يقوم بها المسؤول حيث أنه يملك أولوية أعلى.

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

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

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

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

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

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

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

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

نطاق المهمة

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

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

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

- تحديد أجهزة معينة يدويًا.

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

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

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

- تعيين تحديد جهاز.

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

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

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

كيفية ارتباط إعدادات التطبيق المحلية بالسياسات

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

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

يتم تحديد قيمة الإعدادا 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 إعداد، فإن التطبيق يستخدم قيمة الإعداد المحلية على كل جهاز عميل بدلاً من القيمة المحددة في السياسة. ويمكن بعدها تغيير الإعداد في إعدادات التطبيق المحلية.

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 مؤمَّن ضد التغييرات في السياسة.
- بواسطة سياسة المجموعة إذا كان الإعداد مؤمَّنًا ضد التغييرات

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

نقطة توزيع

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

- توزيع التحديثات وحزم التثبيت الواردة من خادم الإدارة على الأجهزة العميلة في المجموعة (بما في ذلك التوزيع من خلال الإرسال المتعدد باستخدام UDP). يمكن تلقي التحديثات سواء من خادم الإدارة أو من خوادم تحديث Kaspersky. في الحالة الأخيرة، يجب إنشاء مهمة تحديث لنقطة التوزيع.

  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 تتوافر بوابة الاتصال، ولكن هناك إمكانية تقنية للاتصال المباشر مع خادم الإدارة، فسيتم توصيل الأجهزة المدارة بخادم الإدارة مباشرة.

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

- قم بإجراء التثبيت عن بُعد للتطبيقات بواسطة Kaspersky وبائعي البرامج الآخرين، بما في ذلك التثبيت على أجهزة العميل بدون عميل الشبكة.

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

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

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

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

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

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

لا يشارك عملاء الشبكة الذين لديهم ملف تعريف اتصال نشط في اكتشاف مجال البث.

يعين Kaspersky Security Center Linux لكل عميل شبكة عنوان IP للإرسال المتعدد وفريد من نوعه يختلف عن كل عنوان آخر. يتيح لك ذلك تجنب الحمل الزائد على الشبكة الذي يمكن أن يحدث نظرًا إلى تراكب IP. لن يتم تغيير عناوين IP للإرسال المتعدد التي تم تعيينها في الإصدارات السابقة للتطبيق.

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

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

تتطلب نقطة التوزيع توفر 4 جيجابايت على الأقل كمساحة خالية على القرص. إذا كانت مساحة القرص الخالية لنقطة التوزيع أقل من 2 جيجابايت، يقوم Kaspersky Security Center Linux بإنشاء حادث في نفس مستوى خطورة التحذير. سيتم نشر الحادث في خصائص الجهاز، في قسم **الحوادث**.

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

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

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

بوابة الاتصال

بوابة الاتصال هي عميل شبكة يعمل في وضع خاص. تقبل بوابة الاتصال الاتصالات من عملاء الشبكة الآخرين وتقوم 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.

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.

الترخيص

يقدم هذا القسم معلومات حول المفاهيم العامة المتعلقة بترخيص Kaspersky Security Center 14 Linux.

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.

اقرأ "اتفاقية الترخيص" بعناية قبل بدء استخدام التطبيق.

يحتوي Kaspersky Security Center Linux 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 Linux 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 بـ Linux باستخدام الطرق التالية:

- أثناء تنزيل حزمة توزيع عميل الشبكة من خوادم الويب الخاصة بـ Kaspersky.
- أثناء تثبيت عميل الشبكة لنظام Linux.

يُرجى ملاحظة أنه عند تثبيت Network Agent لـ Linux ، يتم عرض اتفاقية ترخيص المستخدم النهائي لعميل الشبكة باللغة الإنجليزية. يمكنك التحقق من اتفاقية ترخيص المستخدم النهائي لعميل الشبكة بلغات أخرى في مجلد /opt/kaspersky/klnagent64/share/license/ قبل قبول شروط اتفاقية ترخيص المستخدم النهائي أثناء التثبيت.

- من خلال قراءة مستند license.txt المضمن في حزمة توزيع عميل الشبكة الخاص بنظام Linux.
- من خلال قراءة مستند license.txt في مجلد تثبيت عميل الشبكة الخاص بنظام 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 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 وفقًا 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 Linux 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 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 وفقًا لشروط اتفاقية ترخيص المستخدم النهائي. يتم إنشاء مفاتيح الترخيص بواسطة أخصائيين في Kaspersky.

يمكنك إضافة مفتاح ترخيص إلى التطبيق باستخدام إحدى الطرق التالية: عن طريق تطبيق ملف المفتاح أو عن طريق إدخال رمز التنشيط. يتم عرض مفتاح الترخيص في واجهة التطبيق بمثابة تسلسل أبجدي رقمي فريد من نوعه بعد قيامك بإضافته إلى التطبيق.

يمكن منع مفتاح الترخيص بواسطة Kaspersky في حالة انتهاك شروط اتفاقية الترخيص. إذا تم منع مفتاح الترخيص، فيجب إضافة مفتاح آخر إذا كنت ترغب في استخدام التطبيق.

يمكن أن يكون مفتاح الترخيص نشطًا أو إضافيًا (أو احتياطيًا).

مفتاح الترخيص المفعّل هو مفتاح الترخيص الذي يستخدم حاليًا من قبل التطبيق. يمكن إضافة مفتاح ترخيص مفعل لترخيص تجريبي أو تجاري. لا يمكن أن يستخدم التطبيق أكثر من مفتاح ترخيص واحد مفعل.

مفتاح الترخيص الإضافي (أو الاحتياطي) هو مفتاح ترخيص يُعطي المستخدم الحق في استخدام التطبيق ولكن لا يتم استخدامه حاليًا. يُصبح مفتاح الترخيص الإضافي مفعلًا تلقائيًا عند انتهاء صلاحية الترخيص المرتبط بمفتاح الترخيص المفعل الحالي. لا يمكن إضافة مفتاح ترخيص إضافي إلا اذا كان قد تم بالفعل إضافة مفتاح ترخيص مفعل.

يمكن إضافة مفتاح الترخيص للترخيص التجريبي كمفتاح الترخيص المفعل. لا يمكن إضافة مفتاح الترخيص للترخيص التجريبي كمفتاح الترخيص الإضافي.

عرض سياسة الخصوصية

سياسة الخصوصية متاحة عبر الإنترنت على https://www.kaspersky.com/Products-and-Services-Privacy-Policy.

سياسة الخصوصية متاحة أيضًا في وضع عدم الاتصال:

- يمكنك قراءة سياسة الخصوصية قبل تثبيت Kaspersky Security Center.
- يتم تضمين نص سياسة الخصوصية في ملف license.txt، في مجلد تثبيت Kaspersky Security Center.
- يتوفر ملف privacy_policy.txt على جهاز مُدار في مجلد تثبيت عميل الشبكة.
- يمكنك فك ضغط ملف privacy_policy.txt من حزمة توزيع عميل الشبكة.

خيارات ترخيص Kaspersky Security Center

يتم تقديم Kaspersky Security Center كجزء من تطبيقات Kaspersky لحماية شبكات الشركة. كما يمكنك تنزيله من موقع الويب الخاص بـ Kaspersky.

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 العميلة.
- عرض وترخيص مجموعات التطبيقات المرخصة الموجودة.
- إحصاءات وتقارير حول تشغيل التطبيق، بالإضافة إلى إخطارات حول الأحداث الحرجة
- 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.

حول ملف المفتاح

ملف المفتاح هو ملف بامتداد .key مقدم لك من قبل Kaspersky. تم تصميم ملفات المفتاح لتفعيل التطبيق من خلال إضافة مفتاح ترخيص.

تتلقى ملف المفتاح الخاص بك عبر عنوان البريد الإلكتروني الذي حددته عند شراء Kaspersky Security Center أو عند طلب الإصدار التجريبي من Kaspersky Security Center.

لتنشيط التطبيق باستخدام ملف المفتاح، فأنت لست بحاجة إلى الاتصال بخوادم تنشيط Kaspersky.

إذا تم حذف ملف المفتاح عن طريق الخطأ، فيمكنك استعادته. قد تحتاج إلى ملف المفتاح لتسجيل حساب Kaspersky CompanyAccount، على سبيل المثال.

لاستعادة ملف المفتاح الخاص بك، قم بتنفيذ أحد الإجراءات التالية:

- اتصل ببائع الترخيص.
- استلم ملف مفتاح عبر موقع الويب الخاص بـ Kaspersky باستخدام رمز التنشيط المتوفر لديك.

بخصوص تزويد البيانات

نقل البيانات إلى مالك الحق

متوفر في اتفاقية ترخيص المستخدم النهائي لـ Kaspersky Security Center 14 Linux.

البيانات التي تتم معالجتها محليًا

تم تصميم Kaspersky Security Center Linux للتنفيذ المركزي لمهام الإدارة والصيانة الأساسية في شبكة المؤسسة. يُمكّن برنامج Kaspersky Security Center Linux المسؤول من الوصول إلى المعلومات المفصلة حول مستوى أمان شبكة المؤسسة؛ ويسمح Kaspersky Security Center Linux للمسؤول بتكوين جميع مكونات الحماية بناءً على تطبيقات Kaspersky. يؤدي Kaspersky Security Center Linux الوظائف الأساسية التالية:

- اكتشاف الأجهزة ومستخدميها في شبكة المؤسسة
- إنشاء تسلسل هرمي لمجموعات الإدارة لإدارة الجهاز
- تثبيت تطبيقات Kaspersky على الأجهزة
- إدارة إعدادات التطبيقات المُثبتة ومهامها
- تنشيط تطبيقات Kaspersky على الأجهزة
- إدارة حسابات المستخدمين
- عرض معلومات حول تشغيل تطبيقات Kaspersky على الأجهزة

- عرض التقارير

يمكن لـ Kaspersky Security Center Linux تلقي المعلومات التالية، وتخزينها، ومعالجتها من أجل تأدية وظائفه الرئيسية:

- معلومات حول الأجهزة في شبكة المؤسسة التي تم استلامها بوصفها نتيجة اكتشاف الجهاز في شبكة من خلال فحص الفواصل الزمنية لـ IP. يجمع خادم الإدارة البيانات بنفسه أو يتلقى البيانات من وكيل 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 Kaspersky Security Center 14 Web Console:

  - المواصفات الفنية للجهاز المُدار ومكوناته المطلوبة لتعريف الجهاز: اسم عرض الجهاز ووصفه، 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: بنية نظام التشغيل، ومورد نظام التشغيل، ورقم بنية نظام التشغيل، ومعرف إصدار نظام التشغيل، ومجلد موقع نظام التشغيل، إذا كان الجهاز عبارة عن جهاز افتراضي – نوع الجهاز الافتراضي.

  - 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 Kaspersky Security Center 14 Web Console.

- تفاصيل تطبيقات Kaspersky المُثبتة على الجهاز. ينقل التطبيق المُدار البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة:

  - إعدادات تطبيقات Kaspersky المثبتة على الجهاز المُدار: اسم تطبيق Kaspersky وإصداره، وحالته، وحالة الحماية في الوقت الفعلي، وتاريخ ووقت آخر فحص للجهاز، وعدد التهديدات التي تم اكتشافها، وعدد العناصر التي لم يتم تطهيرها، وتوافرمكونات التطبيق وحالتها، وتفاصيل إعدادات تطبيق Kaspersky ومهامه، ومعلومات حول مفاتيح الترخيص النشطة والاحتياطية، وتاريخ تثبيت التطبيق، والمعرّف.

  - 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.

- البيانات المُتضمنة في الأحداث من مكونات Kaspersky Security Center Linux وتطبيقات Kaspersky المُدارة. يقوم عميل الشبكة بنقل البيانات من الجهاز إلى خادم الإدارة.

- إعدادات مكونات Kaspersky Security Center Linux وتطبيقات Kaspersky المُدارة والمقدمة في السياسات وملفات تعريف السياسات. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console.

- إعدادات مهمة مكونات Kaspersky Security Center Linux وتطبيقات Kaspersky المُدارة. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console.

- البيانات التي تمت معالجتها بواسطة ميزة إدارة الثغرات الأمنية والتصحيحات. يتم نقل عميل الشبكة من الجهاز إلى معلومات خادم الإدارة حول الأجهزة المكتشفة على الأجهزة المدارة (سجل الأجهزة).

- فئات مستخدمي التطبيقات. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console.

- قائمة الملفات التنفيذية التي تم اكتشافها في الأجهزة المُدارة بواسطة ميزة التحكم في التطبيقات. 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 النسخ الاحتياطي. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- تفاصيل الملفات الموضوعة في العزل. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- تفاصيل الملفات التي طلبها أخصائيون في Kaspersky لإجراء تحليل مفصل عليها. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- تفاصيل الأجهزة الخارجية (وحدات الذاكرة، وأدوات نقل المعلومات، وأدوات النسخ المطبوع للمعلومات، وحافلات التوصيل) المُثبتة أو المُتصلة بالجهاز المُدار والتي تم اكتشافها بواسطة ميزة التحكم في الجهاز. يقوم التطبيق المُدار بنقل البيانات من الجهاز إلى خادم الإدارة من خلال عميل الشبكة. يتم توفير قائمة كاملة من البيانات في ملفات التعليمات الخاصة بالتطبيق المقابل.

- 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.

- تفاصيل رموز التنشيط المُدخلة. يقوم المستخدم بإدخال البيانات في واجهة وحدة تحكم الإدارة أو واجهة Kaspersky Security Center 14 Web Console.

- حسابات المستخدمين: الاسم والوصف والاسم الكامل وعنوان البريد الإلكتروني ورقم الهاتف الرئيسي وكلمة المرور. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console.

- محفوظات مراجعة كائنات الإدارة. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console.

- سجل كائنات الإدارة المحذوفة. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console.

- حزم التثبيت التي تم إنشاؤها من الملف، وكذلك إعدادات التثبيت. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج 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 التحكم في الإدارة أو واجهة برنامج 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 حدث Kaspersky لمكونات Kaspersky Security Center Linux والتطبيق المُدار من Kaspersky. يتم تخزين سجل أحداث Kaspersky على كل جهاز ولا يتم نقلها مطلقًا إلى خادم الإدارة.

- شهادة التوصيل الآمن للأجهزة المُدارة ومكونات Kaspersky Security Center Linux. يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console.

- بيانات خادم الإدارة التي يُدخلها المستخدم في Kaspersky Security Center 14 Web Console.

- أي بيانات يقوم المستخدم بإدخالها فيKaspersky Security Center 14 Web Console.

يمكن أن تكون البيانات المُدرجة أعلاه موجودة في Kaspersky Security Center Linux في حالة تطبيق إحدى الطرق التالية:

- يقوم المستخدم بإدخال البيانات في واجهة وحدة التحكم في الإدارة أو واجهة برنامج Kaspersky Security Center 14 Web Console.

- 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 وعميل الشبكة بتعيين نقطة توزيع لجمع معلومات حول الأجهزة المتصلة بالشبكة.

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 Kaspersky إلا من خلال ملفات التفريغ أو ملفات التتبع أو ملفات السجل الخاصة بمكونات Kaspersky Security Center Linux، بما في ذلك ملفات السجل التي تم إنشاؤها بواسطة أدوات التثبيت والأدوات المساعدة.

تحمي شركة Kaspersky أي معلومات يتم استلامها وفقًا لقانون وقواعد Kaspersky المعمول بها. تم نقل البيانات عبر قناة آمنة.

باتباع الروابط في وحدة تحكم الإدارة أو Kaspersky Security Center 14 Web Console، يوافق المستخدم على النقل التلقائي للبيانات التالية:

- رمز Kaspersky Security Center Linux
- إصدار Kaspersky Security Center Linux
- تعريب Kaspersky Security Center Linux
- 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.

حول الاشتراك

إن الاشتراك في Kaspersky Security Center Linux هو أمر لاستخدام التطبيق بموجب الإعدادات المحددة (تاريخ انتهاء صلاحية الاشتراك، وعدد الأجهزة المحمية). يمكنك تسجيل اشتراكك في Kaspersky Security Center Linux 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 Linux بموجب اشتراك، يجب تطبيق رمز التنشيط الذي تلقيته من موفر الخدمة.

يمكنك تطبيق رمز تنشيط مختلف لـ Kaspersky Security Center Linux 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 Linux بشكل تلقائي الوصول إلى خادم التفعيل في فترات زمنية محددة حتى انتهاء صلاحية الاشتراك. يمكنك تجديد اشتراكك على موقع ويب موفر الخدمة.

تم تجاوز حد أحداث الترخيص

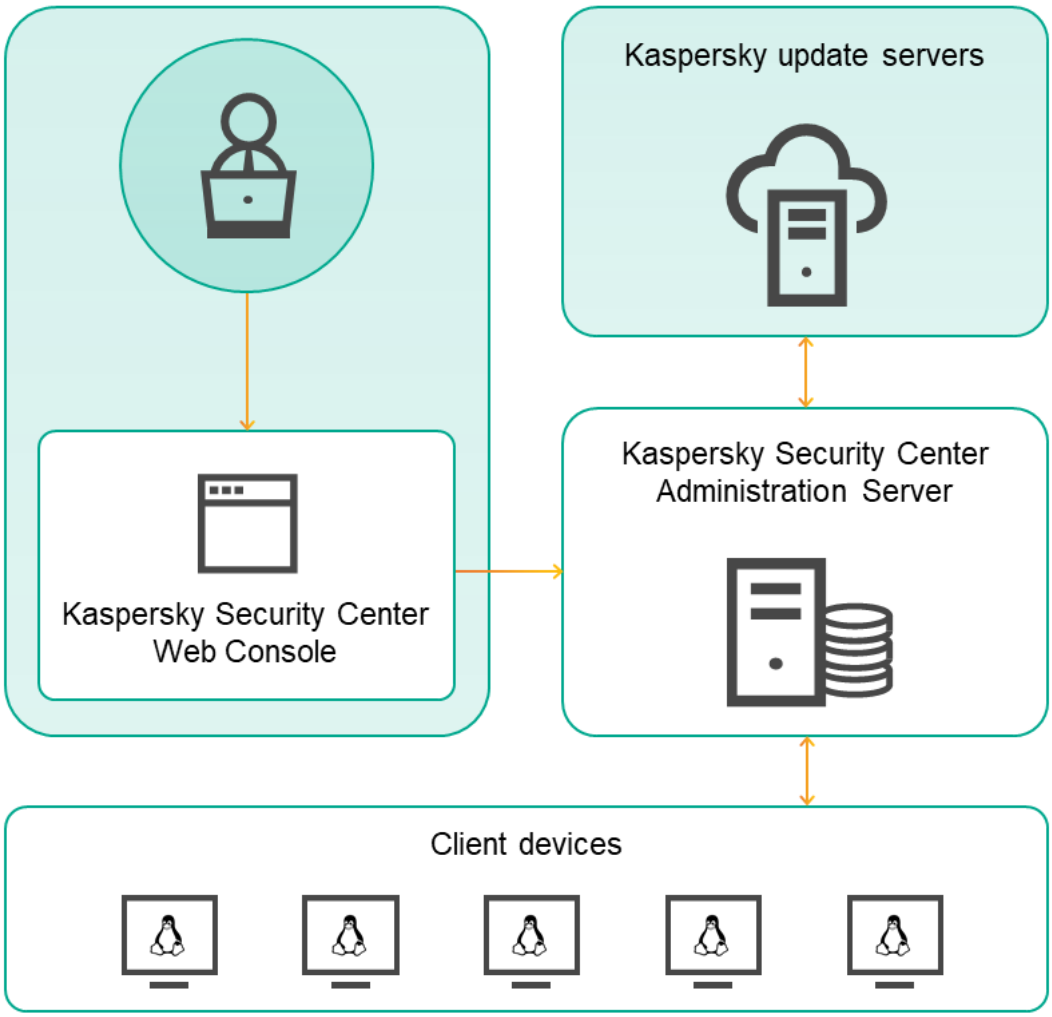
يسمح لك Kaspersky Security Center Linux بالحصول على معلومات عن الأحداث عند تجاوز بعض حدود الترخيص بواسطة تطبيقات Kaspersky المثبتة على أجهزة العملاء.

يتم تحديد مستوى أهمية هذه الأحداث عند تجاوز بعض قيود الترخيص وفقًا للقواعد التالية:

- إذا كان عدد الوحدات المستخدمة حاليًا والتي يشملها ترخيص مفرد تشكّل ما بين 90% و100% من إجمالي عدد الوحدات المشمولة بواسطة الترخيص نفسه، فسيتم نشر الحدث بمستوى الأهمية **معلومات**.
- إذا كان عدد الوحدات المستخدمة حاليًا والتي يشملها ترخيص مفرد تشكّل ما بين 100% و110% من إجمالي عدد الوحدات المشمولة بواسطة الترخيص نفسه، فسيتم نشر الحدث بمستوى الأهمية **تحذير**.
- إذا كان عدد الوحدات المستخدمة حاليًا والتي يشملها ترخيص مفرد يتجاوز 110% من إجمالي عدد الوحدات المشمولة بواسطة الترخيص نفسه، فيتم نشر الحدث بمستوى الأهمية **حدث حرج**.

البنية الهندسية

يقدم هذا القسم وصفًا لمكونات Kaspersky Security Center وتفاعلها.



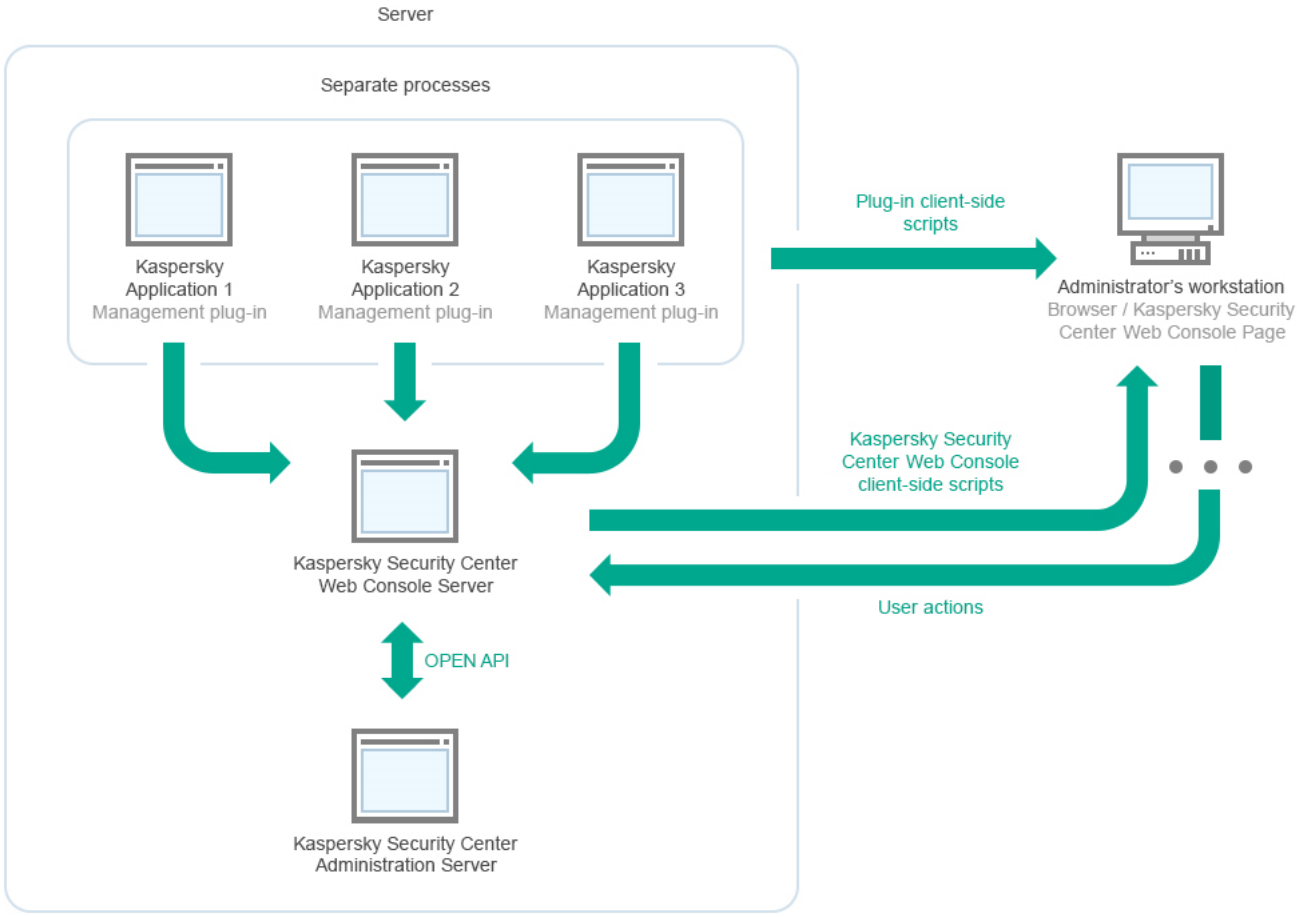
بنية Kaspersky Security Center 14 Linux

يتكون Kaspersky Security Center 14 Linux من المكونات الأساسية التالية:

- **Kaspersky Security Center Web Console**. تقدم واجهة الويب لإنشاء وصيانة نظام حماية شبكة تنظيم العميل التي تتم إدارتها بواسطة Kaspersky Security Center.
- **خادم إدارة Kaspersky Security Center** (ويُشار إليه كذلك باسم الخادم). يعمل على مركزة تخزين معلومات حول التطبيقات المثبتة على شبكة المؤسسة وحول كيفية إدارتها.
- **خوادم تحديث Kaspersky**. خوادم 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 قِبل تطبيقات Kaspersky، ويحسن من أداء بعض مكونات الحماية، ويقلل أيضًا من احتمالية ظهور حالات إيجابية زائفة.
- **أجهزة العميل**. أجهزة شركة العميل المحمية بواسطة Kaspersky Security Center 14 Linux. يجب أن يكون لكل جهاز يلزم حمايته أحد تطبيقات أمان Kaspersky المثبتة.

نشر مخطط خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console

يوضِّح الشكل أدناه مخطط النشر لكلٍ من خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console.



نشر مخطط 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 Server مع خادم إدارة Kaspersky Security Center عبر OpenAPI. يطلب Kaspersky Security Center 14 Web Console Server المعلومات المطلوبة من خادم إدارة Kaspersky Security Center ويعرض نتائج عملياتك في Kaspersky Security Center 14 Web Console.

المنافذ المستخدمة بواسطة Kaspersky Security Center Linux

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

المنفذ الذي يستخدمه خادم الإدارة الخاص بـ Kaspersky Security Center Linux

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 **خادم الويب** من نافذة خصائص خادم الإدارة.
8061	klcsweb	TCP ((TLS	نقل حزم التثبيت التي تم نشرها إلى أجهزة عميلة	نشر حزم التثبيت. يمكنك تغيير رقم المنفذ الافتراضي في قسم **خادم الويب** من نافذة خصائص خادم الإدارة.
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 تكوين منافذ الاتصال أثناء تثبيت Kaspersky Security Center Linux؛ يمكنك تغيير رقم المنفذ الافتراضي لتلقي الاتصالات من خوادم الإدارة الثانوية عند إنشاء تسلسل هرمي لخوادم الإدارة.
13000	klserver	UDP	تلقي معلومات حول الأجهزة التي تم إيقاف تشغيلها من عملاء الشبكة	إدارة الأجهزة العميلة. يمكنك تغيير رقم المنفذ الافتراضي في إعدادات نهج عميل الشبكة.
13299	klserver	TCP ((TLS	تلقي اتصالات من Kaspersky Security Center 14 Web Console إلى خادم الإدارة؛ تلقي اتصالات إلى خادم الإدارة عبر OpenAPI	Kaspersky Security Center 14 Web Console، OpenAPI. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة (في القسم الفرعي **منافذ الاتصال** في القسم **العام**)، أو عند إنشاء تسلسل هرمي لخوادم الإدارة.
14000	klserver	TCP	تلقي اتصالات من عملاء الشبكة	إدارة الأجهزة العميلة. يمكنك تغيير رقم المنفذ الافتراضي عند تكوين منافذ الاتصال أثناء تثبيت Kaspersky Security Center Linux أو عند توصيل جهاز عميل بخادم الإدارة يدويًا.
13111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)	ksnproxy	TCP	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة.
15111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)	ksnproxy	UDP	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة.
17000	klactprx	TCP	استلام الاتصالات لتفعيل التطبيق من	خادم وكيل التفعيل للأجهزة المدارة.

		TLS))	الأجهزة المدارة	يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص خادم الإدارة (في **المنافذ الإضافية** القسم الفرعي بالقسم **العام**).
19170	klserver	HTTPS (TLS))	نفق الاتصالات إلى الأجهزة المُدارة باستخدام الأداة المساعدة klsctunnel	الاتصال عن بُعد بالأجهزة المدارة باستخدام Kaspersky Security Center 14 Web Console. يمكنك تغيير رقم المنفذ الافتراضي باستخدام الأداة المساعدة klscflag.

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 MariaDB). يرجى الرجوع إلى وثائق نظام إدارة قواعد البيانات (DBMS) للحصول على المعلومات ذات الصلة.

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

المنفذ الذي يستخدمه خادم Kaspersky Security Center Linux 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 من مستعرض الويب إلى Kaspersky Security Center 14 Web Console	Kaspersky Security Center 14 Web Console. يمكنك تغيير رقم المنفذ الافتراضي عند تثبيت Kaspersky Security Center 14 Web Console. 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	klnagent	UDP	إشارات الإدارة من خادم الإدارة إلى وكلاء الشبكة	إدارة الأجهزة العميلة. يمكنك تغيير رقم المنفذ الافتراضي في إعدادات نهج عميل الشبكة.
15000	klnagent	بث بروتوكول حزم بيانات المستخدم (UDP)	الحصول على بيانات حول وكلاء الشبكة الآخرين ضمن مجال البث نفسه (ثم يتم إرسال البيانات إلى خادم الإدارة)	تسليم التحديثات وحزم التثبيت.
15001	klnagent	UDP	استقبال طلبات البث المتعدد من نقطة توزيع (إذا كانت قيد الاستخدام)	استلام التحديثات وحزم التثبيت من نقطة التوزيع. يمكنك تغيير رقم المنفذ الافتراضي في نافذة خصائص نقطة التوزيع.

يوضح الجدول الموجود أدناه المنافذ التي يجب فتحها على جهاز مدار مثبت عليه عميل شبكة والتي تعمل كنقطة توزيع. يجب أن تكون المنافذ المدرجة مفتوحة على أجهزة نقطة التوزيع بالإضافة إلى المنافذ التي يستخدمها عملاء الشبكة (انظر الجدول أعلاه).

المنافذ التي يستخدمها عميل الشبكة وتعمل كنقطة توزيع

رقم المنفذ	اسم العملية التي تفتح المنفذ	البروتوكول	غرض المنفذ	النطاق
13000	klnagent	TCP (TLS))	تلقي اتصالات من عملاء الشبكة	إدارة الأجهزة العميلة وتسليم التحديثات وحزم التثبيت.

				يمكنك تغيير رقم المنفذ الافتراضي في خصائص نقطة التوزيع.
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 خصائص نقطة التوزيع.
15111 (فقط إذا كانت خدمة وكيل KSN تعمل على الجهاز)	ksnproxy	UDP	تلقي طلبات من الأجهزة المدارة إلى الخادم الوكيل KSN	خادم وكيل KSN. يمكنك تغيير رقم المنفذ الافتراضي في خصائص نقطة التوزيع.

المنافذ المستخدمة بواسطة وحدة تحكم الويب لـ Kaspersky Security Center 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 Kaspersky Security Center 14

رقم المنفذ	اسم الخدمة	البروتوكول	غرض المنفذ	النطاق
2001	KSCWebConsolePlugin	HTTPS	منفذ API الذي تستخدمه عمليات البرنامج الإضافي للإدارة لتلقي الطلبات من KSCWebConsoleManagementService	تشغيل عمليات node.exe الخاصة بإدارة المكونات الإضافية
1329، 2003	KSCWebConsoleManagementService	HTTPS	منافذ API المستخدمة في استقبال الطلبات من خدمة KSCWebConsole التي تعمل على نفس الجهاز.	تحديث مكونات Kaspersky Security Center 14 Web Console
2005	KSCWebConsole	HTTPS	منفذ API مستخدم في استقبال الطلبات من خدمة KSCWebConsoleManagementService التي تعمل على نفس الجهاز.	تشغيل عمليات node.exe من Kaspersky Security Center 14 Web Console
8200	–	HTTP	منفذ API مستخدم في إنشاء شهادات عبر HashiCorp Vault (لمزيد من التفاصيل عنها، يُرجى الرجوع إلى موقع ويب HashiCorp Vault)	تثبيت Kaspersky Security Center 14 Web Console وتحديث مكونات Kaspersky Security Center 14 Web Console
4150، 4151، 4152	KSCWebConsoleMessageQueue	HTTPS	منافذ API الخاصة بـ Message Broker المستخدمة للاتصال بين عمليات كل من Kaspersky Security Center 14 Web Console والمكونات الإضافية للإدارة	التفاعل بين Kaspersky Security Center 14 Web Console ومكونات الإدارة الإضافية.

التثبيت:

يصف هذا القسم تثبيت Kaspersky Security Center وكذلك Kaspersky Security Center 14 Web Console.

سيناريو التثبيت الرئيسي

باتباع هذا السيناريو، يمكنك تثبيت خادم إدارة Kaspersky Security Center 14 Linux وKaspersky Security Center 14 Web Console، وإجراء الإعداد الأولي لخادم الإدارة باستخدام معالج البدء السريع، وتثبيت تطبيقات Kaspersky على الأجهزة المدارة باستخدام الحماية

المتطلبات الأساسية

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

إذا كنت تريد تجربة برنامج Kaspersky Security Center 14 Linux أولاً، فيمكنك الحصول على نسخة تجريبية مجانية لمدة 30 يومًا على موقع ويب Kaspersky.

المراحل

يستمر سيناريو التثبيت الرئيسي على مراحل:

1. **تحديد هيكل لحماية المؤسسة**

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

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

2. **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.

3. **تثبيت نظام إدارة قواعد البيانات (DBMS)**

   قم بتثبيت نظام إدارة قواعد البيانات الذي سيستخدمه Kaspersky Security Center، أو استخدم نظامًا حاليًا.

4. **تكوين منافذ**

   تأكد من أن كل المنافذ الضرورية مفتوحة للتفاعل بين المكونات طبقًا 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.

5. **تثبيت Kaspersky Security Center**

   حدد جهاز Linux الذي تنوي استخدامه كخادم إدارة، وتأكد من أن الجهاز يستوفي متطلبات البرامج والأجهزة، ثم قم بتثبيت Kaspersky Security Center على الجهاز. يتم تثبيت إصدار خادم عميل الشبكة مع خادم الإدارة تلقائيًا.

6. **تثبيتKaspersky Security Center 14 Web Console ومكونات الإدارة الإضافية**

   حدد جهاز Linux الذي تنوي استخدامه كمحطة عمل للمسؤول ، وتأكد من أن الجهاز يستوفي متطلبات البرامج والأجهزة، ثم قم بتثبيت Kaspersky Security Center 14 Web Console على الجهاز. يمكنك تثبيت Kaspersky Security Center 14 Web Console على نفس الجهاز المثبت عليه خادم الإدارة أو على جهاز مختلف.

قم بتنزيل المكوّن الإضافي Kaspersky Endpoint Security لمكوّن الويب الإضافي الخاص بإدارة نظام Linux ثم ثبّته على نفس الجهاز حيث تم تثبيت Kaspersky Security Center 14 Web Console.

7 تثبيت Kaspersky Endpoint Security الخاص بنظام Linux وعميل الشبكة على جهاز خادم الإدارة

بشكل افتراضي، لا يعتبر التطبيق جهاز خادم الإدارة جهازًا مُدارًا. لحماية خادم الإدارة من الفيروسات والتهديدات الأخرى، ولإدارة الجهاز مثل أي جهاز آخر مُدار، نوصي بتثبيت Kaspersky Endpoint Security الخاص بنظام Linux وعميل الشبكة الخاص بنظام Linux على جهاز خادم الإدارة. في هذه الحالة، يتم تثبيت عميل الشبكة الخاص بنظام Linux ويعمل بشكل مستقل عن إصدار خادم عميل الشبكة الذي ثبّته مع خادم الإدارة.

8 إجراء الإعداد الأولي

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

9 اكتشاف أجهزة الشبكة

اكتشف الأجهزة يدويًا. يستلم Kaspersky Security Center Linux عناوين وأسماء جميع الأجهزة التي تم اكتشافها في الشبكة. بعد ذلك يمكنك استخدام Kaspersky Security Center Linux لتثبيت تطبيقات وبرامج Kaspersky المتوفرة من موردين آخرين في الأجهزة المكتشفة. يبدأ Kaspersky Security Center Linux اكتشاف الأجهزة بشكل منتظم، مما يعني أنه في حالة ظهور أي مثيلات جديدة في الشبكة، سيتم اكتشافها تلقائيًا.

10 ترتيب الأجهزة في مجموعات الإدارة

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

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

11 تعيين نقاط التوزيع

يتم تعيين نقاط التوزيع إلى مجموعات الإدارة تلقائيًا ولكن يمكنك تعيينها يدويًا عند الضرورة. نوصيك باستخدام نقاط التوزيع في الشبكات واسعة النطاق لتقليل التحميل على خادم الإدارة، وفي الشبكات المشتملة على بنية موزعة لتوفير وصول خادم الإدارة إلى الأجهزة (أو مجموعات الأجهزة) المتصلة من خلال قنوات ذات معدلات نقل منخفضة.

12 تثبيت عميل الشبكة وتطبيقات أمان على أجهزة متصلة بالشبكة.

يستلزم نشر الحماية على شبكة مؤسسة تثبيت عميل الشبكة وتطبيقات الأمان على الأجهزة التي تم اكتشافها بواسطة خادم الإدارة أثناء اكتشاف الأجهزة.

لتثبيت التطبيقات عن بُعد، قم بتشغيل معالج نشر الحماية.

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

قبل أن تبدأ تثبيت عميل الشبكة وتطبيقات الأمان على الأجهزة المتصلة بالشبكة، تأكد أن هذه الأجهزة يمكن الوصول إليها (تم تشغيلها).

13 نشر مفاتيح الترخيص على الأجهزة العميلة

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

14 تكوين سياسات تطبيق Kaspersky

لتطبيق إعدادات مختلفة للتطبيق على أجهزة مختلفة، يمكنك استخدام إدارة أمان مرتكزة على الجهاز و/أو إدارة أمان مرتكزة على المستخدم. يمكن تنفيذ إدارة الأمان المرتكزة على الجهاز باستخدام السياسات والمهام. لا يمكنك تطبيق المهام إلا على الأجهزة التي تلبي الشروط المحددة. ولوضع شروط تصفية الأجهزة، استخدام تحديدات الأجهزة وكذلك العلامات.

15 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.

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 DBMSs.

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

إذا كنت تستخدم MariaDB، فأنت بحاجة إلى تكوين الإعدادات الموصى بها للعمل الأمثل لنظام DBMS مع Kaspersky Security Center.

تكوين خادم MariaDB x64 للعمل مع Kaspersky Security Center 14 Linux

إذا كنت تستخدم خادم MariaDB مع Kaspersky Security Center، مكّن دعم تخزين InnoDB وMEMORY، وكذلك ترميزي UTF-8 وUCS-2.

الإعدادات الموصى بها لملف my.cnf

لتكوين ملف my.cnf:

1. افتح ملف my.cnf في أي محرر نصوص.

2. أدخل السطور التالية في ملف my.cnf:

```
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، تكون المكونات الإضافية المحسنة `join_cache_incremental`، و`join_cache_hashed`، و`join_cache_bka` مفعّلة. 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 قيمها مشغلة ، فهذا يعني أن المكونات الإضافية المحسنة مفعلة.

إذا لم تكن هذه السطور موجودة أو كانت قيمها معطلة ، فأنت بحاجة إلى فعل ما يلي:

a. افتح ملف my.cnf في أي محرر نصوص.

b. أضف السطور التالية في ملف my.cnf:

```
'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.

تثبيت Kaspersky Security Center

يصف هذا الإجراء كيفية تثبيت Kaspersky Security Center.

قبل التثبيت:

- تثبيت نظام إدارة قواعد البيانات.
- تأكد أن الجهاز الذي ترغب في تثبيت Kaspersky Security Center عليه يعمل بإحدى توزيعات Linux المدعومة.

استخدم ملف التثبيت—ksc64_[version_number]_amd64.deb or ksc64-[version_number].x86_64.rpm—الذي يوافق توزيعة Linux المثبتة على جهازك. سوف تستقبل ملف التثبيت بتنزيله من موقع Kaspersky.

لتثبيت Kaspersky Security Center:

1. افتح سطر الأوامر وقم بتشغيل الأوامر المتوفرة في هذه التعليمات من حساب يتمتع بالمزايا الإدارية.

2. أنشئ مجموعة 'kladmins' وحساب لا يتمتع بالمزايا الإدارية 'ksc'. يجب أن يكون الحساب جزءًا من مجموعة 'kladmins'. لفعل ذلك، أجر الأوامر التالية بالترتيب:

```
adduser ksc #
groupadd kladmins #
gpasswd -a ksc kladmins #
usermod -g kladmins ksc #
```

3. قم بتشغيل تثبيت Kaspersky Security Center. أدخل أحد الأوامر التالية، ويعتمد ذلك على توزيعة Linux لديك:

- `apt install /<path>/ksc64_[رقم الإصدار]_amd64.deb #`
- `yum install /<path>/ksc64-[version_number].x86_64.rpm -y #`

4. قم بتشغيل تكوين Kaspersky Security Center:

```
opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl/ #
```

5. اقرأ اتفاقية ترخيص المستخدم النهائي (EULA) وسياسة الخصوصية. يتم عرض النص في نافذة سطر الأوامر. اضغط على شريط المسافة لعرض جزء النص التالي. ثم عند المطالبة، أدخل القيم التالية:

a. اكتب y إذا كنت قد قرأت شروط اتفاقية ترخيص المستخدم النهائي (EULA). اكتب n إذا كنت لا تقبل بنود اتفاقية ترخيص المستخدم النهائي (EULA). لاستخدام Kaspersky Security Center، يجب أن تقبل بنود اتفاقية ترخيص المستخدم النهائي (EULA).

b. اكتب y إذا كنت تفهم وتقبل بنود سياسة الخصوصية، وتوافق على أن يتم التعامل مع بياناتك ونقلها كما هو موصوف في سياسة الخصوصية (ويشمل ذلك إلى بلاد الطرف الثالث). اكتب n إذا كنت لا تقبل بنود سياسة الخصوصية. لاستخدام Kaspersky Security Center، يجب أن تقبل شروط سياسة الخصوصية.

6. عند المطالبة، أدخل الإعدادات التالية:

a. أدخل اسم DNS أو عنوان IP الثابت لخادم الإدارة.

b. أدخل رقم منفذ خادم الإدارة. يتم استخدام المنفذ 14000 بشكل افتراضي.

c. أدخل رقم منفذ SSL لخادم الإدارة. يتم استخدام المنفذ 13000 بشكل افتراضي.

d. قم بتقييم العدد التقريبي للأجهزة التي ترغب في إدارتها:

- إذا كان لديك من 1 إلى 100 جهاز متصل بالشبكة، فادخل إلى جهاز واحد.
- إذا كان لديك من 101 إلى 1000 جهاز متصل بالشبكة، فادخل إلى جهازين.
- إذا كان لديك أكثر من 1000 جهاز متصل بالشبكة، فادخل إلى ثلاثة أجهزة.

e. أدخل اسم مجموعات الأمان للخدمات. بشكل افتراضي، يتم استخدام مجموعة 'kladmins'.

f. أدخل اسم الحساب لبدء خدمة خادم الإدارة. يجب أن يكون الحساب عضوًا في مجموعة الأمان المدخلة. بشكل افتراضي، يتم استخدام حساب 'ksc'.

g. أدخل اسم الحساب لبدء الخدمات الأخرى. يجب أن يكون الحساب عضوًا في مجموعة الأمان المدخلة. بشكل افتراضي، يتم استخدام حساب 'ksc'.

h. أدخل عنوان IP للجهاز المثبت عليه قاعدة البيانات.

i. أدخل رقم منفذ قاعدة البيانات. يتم استخدام هذا المنفذ في التواصل مع خادم الإدارة. يتم استخدام المنفذ 3306 بشكل افتراضي.

j. أدخل اسم قاعدة البيانات.

k. أدخل معلومات تسجيل الدخول لحساب إدارة قاعدة البيانات الذي ستستخدمه للوصول إلى قاعدة البيانات.

l. أدخل كلمة المرور لحساب إدارة قاعدة البيانات الذي ستستخدمه في الوصول إلى قاعدة البيانات.
انتظر حتى تنتهي إضافة الخدمات وتبدأ في العمل بشكل تلقائي:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. أنشئ حسابًا يكون هو مسؤول خادم الإدارة. أدخل اسم المستخدم وكلمة المرور.
يجب أن تتوافق كلمة المرور مع القواعد التالية:

- لا يمكن أن تكون كلمة المرور أقل من 8 حروف ولا أكثر من 16 حرفًا.
- يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
  - الأحرف الكبيرة (A-Z)
  - الأحرف الصغيرة (a-z)
  - الأعداد (0-9)
  - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

يتم إضافة المستخدم ويتم تثبيت Kaspersky Security Center.

تأكيد الخدمة

استخدم الأوامر التالية في التحقق إذا ما كانت الخدمة تعمل أم لا:

- `systemctl status klnagent_srv.service #`
- `systemctl status kladminserver_srv.service #`
- `systemctl status klactprx_srv.service #`
- `systemctl status klwebsrv_srv.service #`

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) على الأجهزة التي تعمل بنظام التشغيل Linux. يجب قبل التثبيت أن تقوم بتثبيت نظام لإدارة قواعد البيانات وخادم إدارة Kaspersky Security Center.

استخدم أحد ملفات التثبيت التالية الذي يتوافق مع توزيع Linux المثبت على جهازك:

- لـ Debian — ksc-web-console- [build_number] .x86_64.deb
- لأنظمة التشغيل المستندة إلى RPM — ksc-web-console- [build_number] .x86_64.rpm
- لـ Alt 8 SP — ksc-web-console- [build_number] -alt8p.x86_64.rpm

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 (EULA) في حزمة التثبيت (ملف /var/opt/kaspersky/ksc-web-console/license-<XX>.txt حيث <XX> هي رمز لغة). 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 المعلمات مع العنوان والمنفذ الافتراضيين:

```
{
"العنوان": "127.0.0.1"،
"المنفذ": 8080،
"خادم KSC موثوق":
"|var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer/|13299|127.0.0.1",
"acceptEula": حقيقي
{
```

عند تثبيت Kaspersky Security Center 14 Web Console على نظام التشغيل Linux ALT، يجب عليك تحديد رقم منفذ غير 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 توزيعة 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-[build_number].x86_64.deb $
```

- لتثبيت Kaspersky Security Center 14 Web Console من ملف بامتداد rpm، أدخل الأوامر التالية:

```
sudo rpm -ivh --nodeps ksc-web-console-[build_number].x86_64.rpm $
```

أو

```
sudo alien -i ksc-web-console-[build_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-[build_number].x86_64.rpm $
```

  - بالنسبة للأجهزة التي تعمل بنظام التشغيل المستند إلى Debian:

```
sudo dpkg -i ksc-web-console-[build_number].x86_64.deb $
```

يبدأ هذا فك 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/.

5. أعد تشغيل جميع خدمات Kaspersky Security Center 14 Web Console عن طريق تشغيل الأمر التالي:

```
*sudo systemctl restart KSC $
```

وعندما يكتمل التثبيت، يمكنك استخدام المستعرض في فتح Kaspersky Security Center 14 Web Console وتسجيل الدخول إليه.

معلمات 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 —أ. أي ملف بامتداد .json يحتوي على معلمات لتوصيل Kaspersky Security Center 14 Web Console بخادم الإدارة.

إليك مثالاً على ملف استجابة يحتوي على أقل مجموعة من المعلمات مع العنوان والمنفذ الافتراضيين:

```
}
"العنوان": "127.0.0.1"،
"المنفذ": 8080،
"defaultLangId": 1049,
"enableLog": false,
"خادم KSC موثوق":
"|var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer/|13299|127.0.0.1",
```

```
{
"messageQueueAccount": "المجموعة 1: المستخدم 5"
"pluginAccount": "المجموعة 1: المستخدم 4"،
"serviceWebConsoleAccount": "المجموعة 1: المستخدم 3"،
"managementServiceAccount": "المجموعة 1: المستخدم 2"،
"webConsoleAccount": "المجموعة 1: المستخدم 1"،
"certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
"acceptEula": true,
```

عند تثبيت Kaspersky Security Center 14 Web Console على نظام التشغيل tne 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.

معلمات تثبيت Kaspersky Security Center 14 Web Console على أجهزة تعمل بنظام Linux

المعلمة	الوصف	القيم المتوفرة
العنوان	نوان خادم Kaspersky Security Center 14 Web Console (مطلوب).	قيمة السلسلة.
المنفذ	رقم المنفذ الذي يستخدمه خادم Kaspersky Security Center 14 Web Console في التوصيل بخادم الإدارة (مطلوب).	قيمة رقمية.
defaultLangId	لغة واجهة المستخدم (الافتراضي هو 1033).	الرمز الرقمي للغة: • الألمانية: 1031 • الإنجليزي: 1033 • الأسبانية: 3082 • الأسبانية (المكسيك): 2058 • الفرنسية: 1036 • اليابانية: 1041 • الكازاخستانية: 1087 • البولندية: 1045 • البرتغالية (البرازيل): 1046 • الروسية: 1049 • اللغة التركية: 1055 • الصينية المبسطة: 4 • الصينية التقليدية: 31748 في حال عدم تحديد قيمة، سيتم استخدام اللغة الإنجليزية (3
enableLog	سواء تم تفعيل تسجيل نشاط Kaspersky Security Center 14 Web Console أم لا.	قيمة منطقية: • true—التسجيل مفعل (هذا هو الاختيار الافتراضي

		• false—التسجيل غير مفعل.
موثوق	قائمة بخوادم الإدارة الموثوقة المسموح لها بالاتصال بـ Kaspersky Security Center 14 Web Console. يجب تعريف كل خادم إدارة بالمعلمات التالية: • 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 يتم الفصل بين المعلمات باستخدام أشرطة عمودية. في حال تحديد عدة خوادم إدارة، افصل بينهم باستخدام شريطين عموديين (أنبوبين).	قيمة السلسلة للتنسيق التالي: " عنوان الخادم|المنفذ|مسار الش مثال: 13299|/cert/server-1.cer|Server" 3299|/cert/server-2.cer|Server 2
acceptEula	سواء كنت ترغب في قبول شروط اتفاقية ترخيص المستخدم النهائي أو عدم قبولها. يحتوي الملف على شروط اتفاقية ترخيص المستخدم النهائي التي يتم تنزيلها مع ملف التثبيت.	قيمة منطقية: • صحيح—لقد قرأت شروط اتفاقية ترخيص المستخدم وقبلتها. • false—لا أقبل شروط اتفاقية الترخيص (الاختيار
certDomain	إذا كنت ترغب في إنشاء شهادة جديدة، استخدم هذا المعامل في تحديد اسم النطاق الذي سيتم إنشاء شهادة جديدة له.	قيمة السلسلة.
certPath	إذا كنت ترغب في استخدام شهادة حالية، استخدم هذا المعامل في تحديد مسار ملف الشهادة.	قيمة السلسلة. حدد المسار ent_srv/1093/cert/klserver.cer/" لاستخدام الشهادة الحالية. للحصول على شهادة مخصصة، الشهادة المخصصة.
keyPath	إذا كنت ترغب في استخدام شهادة حالية، استخدم هذا المعامل في تحديد مسار ملف المفتاح.	قيمة السلسلة.
webConsoleAccount	اسم الحساب الذي تعمل بموجبه خدمة KSCWebConsole.	قيمة السلسلة في التنسيق التالي: " اسم المجموعة مثال: "Group1: User1" . إذا لم يتم تحديد أي قيمة، فإن أداة تثبيت enter 14 Web Console تنشئ حسابًا جديدًا بالاسم الافتراضي uid
managementServiceAccount	اسم الحساب المميز الذي تعمل بموجبه خدمة KSCWebConsoleManagement.	قيمة السلسلة في التنسيق التالي: " اسم المجموعة مثال: "Group1: User1" . إذا لم يتم تحديد أي قيمة، فإن أداة تثبيت enter 14 Web Console تنشئ حسابًا جديدًا بالاسم الافتراضي %uid
serviceWebConsoleAccount	اسم الحساب الذي تعمل بموجبه خدمة KSCSvcWebConsole.	قيمة السلسلة في التنسيق التالي: " اسم المجموعة مثال: "Group1: User1" .

		إذا لم يتم تحديد أي قيمة، فإن أداة تثبيت Web Console 14 تنشئ حسابًا جديدًا بالاسم الافتراضي `%uid`
`pluginAccount`	اسم الحساب الذي تعمل بموجبه خدمة KSCWebConsolePlugin.	قيمة السلسلة في التنسيق التالي: `"اسم المجموعة: اسم المستخدم"`. مثال: `"Group1: User1"`. إذا لم يتم تحديد أي قيمة، فإن أداة تثبيت Web Console 14 تنشئ حسابًا جديدًا بالاسم الافتراضي `%uid`
`messageQueueAccount`	اسم الحساب الذي تعمل بموجبه خدمة KSCWebConsoleMessageQueue.	قيمة السلسلة في التنسيق التالي: `"اسم المجموعة: اسم المستخدم"`. مثال: `"Group1: User1"`. إذا لم يتم تحديد أي قيمة، فإن أداة تثبيت Web Console 14 تنشئ حسابًا جديدًا بالاسم الافتراضي `%uid`

إذا قمت بتحديد معلمات `webConsoleAccount` أو `managementServiceAccount` أو `serviceWebConsoleAccount` أو `pluginAccount` أو `messageQueueAccount`، فتأكد من أن حسابات المستخدمين المخصصة تنتمي إلى نفس مجموعة الأمان. إذا لم يتم تحديد هذه المعلمات، فإن برنامج التثبيت Kaspersky Security Center 14 Web Console يقوم بإنشاء مجموعة أمان افتراضية، ثم ينشئ حسابات مستخدمين بأسماء افتراضية في هذه المجموعة.

حسابات للعمل باستخدام نظام إدارة قواعد البيانات (DBMS)

يوفر الجدول التالي معلومات حول خصائص الحسابات المختارة للعمل مع MariaDB DBMS.

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

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

نظام إدارة قواعد البيانات: MariaDB

موقع نظام إدارة قواعد بيانات DBMS	محلي أو عن بُعد.	محلي أو عن بُعد.
من ينشئ قاعدة بيانات KAV	المثبّت (تلقائيًا).	المسؤول (يدويًا).
الحساب الذي يعمل بموجبه المثبّت	محلي أو مجال، مع حقوق المسؤول المحلي.	محلي أو مجال، مع حقوق المسؤول المحلي.
حساب خدمة خادم إدارة	محلي أو مجال.	محلي أو مجال.
حقوق حساب DBMS الداخلي الذي يستخدمه المثبت وخدمة خادم الإدارة للوصول إلى نظام إدارة قواعد البيانات	الوصول إلى الجذر مطلوب.	منح الكل لقاعدة بيانات KAV و تحديد و عرض المشاهدة و و إجراء لجداول النظام.

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 الخاصة بمجموعة تجاوز الفشل.

يتقدم نشر تطبيقات Kaspersky في مراحل:

1. **إنشاء حساب لخدمات Kaspersky Security Center**

   أنشئ حسابًا جديدًا أو حدد حساب مستخدم مجال موجود حيث سيتم تشغيل خدمات Kaspersky Security Center بموجبه. أضف الحساب المحدد في مجموعة المسؤولين المحليين على كل العقد وعلى خادم الملفات.

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.

   تعليمات 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.

   تعليمات كيفية: تحضير عقد لمجموعة تجاوز الفشل من Kaspersky

4. **تثبيت نظام إدارة قواعد البيانات (DBMS)**

   لديك خياران:

   - إذا كنت ترغب في استخدام مجموعة MariaDB Galera، فلن تحتاج إلى جهاز كمبيوتر مخصص لـ DBMS. قم بتثبيت مجموعة MariaDB Galera على كل العقد.
   - إذا كنت ترغب في استخدام أي نظام DBMS مدعوم آخر، فثبّت نظام DBMS المحدد 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.

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 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.

في مجموعة تجاوز الفشل من Kaspersky، تتم إدارة جميع خدمات Kaspersky Security Center تلقائيًا. لا تحاول إعادة تشغيل الخدمات يدويًا.

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 يعمل بنظام Linux بنظام ملف EXT4. 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). إذا كنت تستخدم مجموعة MariaDB Galera كنظام DBMS، فلا يلزم وجود كمبيوتر مخصص لهذا الغرض.

تبديل الشروط:

تبدل مجموعة تجاوز الفشل إدارة حماية أجهزة العميل من العقدة المفعلة إلى العقدة الخاملة في حالة حدوث أي من الأحداث التالية على العقدة المفعلة:

- العقدة المفعلة معطلة بسبب عطل في البرامج أو الأجهزة.
- تم إيقاف العقدة المفعلة مؤقتًا لأنشطة الصيانة.
- فشلت واحدة على الأقل من خدمات (أو عمليات) Kaspersky Security Center أو تم إنهاؤها عمدًا من قِبل المستخدم. خدمات Kaspersky Security Center هي التالية: kladminserver وklnagent وklactprx وklwebsrv.
- تم قطع اتصال الشبكة بين العقدة المفعلة والتخزين على خادم الملفات أو إنهاؤه.

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. تثبيت وتكوين خادم NFS:

- يجب تمكين الوصول إلى خادم الملفات لكلا العقدتين في إعدادات خادم NFS.
- يجب أن يحتوي بروتوكول NFS على الإصدار 4.0 أو 4.1.
- الحد الأدنى لمتطلبات Linux kernel:
  - 3.19.0-25، إذا كنت تستخدم NFS 4.0
  - 4.4.0-176، إذا كنت تستخدم NFS 4.1

3. على خادم الملفات، أنشئ مجلدين وشاركهما باستخدام NFS. 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.

   قم بتشغيل الأوامر التالية:

```
sudo yum install nfs-utils
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
sudo chown ksc:kladmins /mnt/KlFocStateShare
sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
sudo chmod -R 777 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >>
"/etc/exports
sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
"(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports
sudo cat /إلخ/الصادرات
sudo exportfs -a
sudo rpcbind بدء نظام
sudo nfs تبدأ خدمة
```

   قم بتمكين التشغيل التلقائي عن طريق تشغيل الأمر التالي:

```
sudo systemctl rpcbindg تمكين
```

4. أعد تشغيل خادم الملفات.

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. لجعل العقد تعمل كعملاء NFS، قم بتثبيت حزمة nfs-utils على كل عقدة.

   قم بتشغيل الأمر التالي:

```
sudo yum install nfs-utils
```

3. قم بإنشاء نقاط تحميل عن طريق تشغيل الأوامر التالية:

```
sudo mkdir -p /mnt/KlFocStateShare
sudo mkdir -p /mnt/KlFocDataShare_klfoc
```

4. تحقق من إمكانية تحميل المجلدات المشتركة بنجاح. [خطوة اختيارية]

قم بتشغيل الأوامر التالية:

```
sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {الخادم}:{المسار
إلى مجلد /mnt/KlFocStateShare} KlFocStateShare
sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {الخادم}:{المسار
إلى مجلد /mnt/KlFocDataShare_klfoc } KlFocDataShare_klfoc
```

هنا، تكون مساراتعبارة عن {الخادم}:{المسار إلى مجلد KlFocStateShare}و{الخادم}:{path to the KlFocDataShare_klfoc folder} مسارات الشبكة إلى المجلدات المشتركة على خادم الملفات.

بعد أن يتم تحميل المجلدات المشتركة بنجاح، قم بإلغاء تحميلها عن طريق تشغيل الأوامر التالية:

```
sudo umount /mnt/KlFocStateShare
sudo umount /mnt/KlFocDataShare_klfoc
```

5. تطابق نقاط التحميل والمجلدات المشتركة:

```
sudo vi /etc/fstab
{الخادم}: {المسار إلى مجلد KlFocStateShare} /mnt/KlFocStateShare nfs
vers=4,nolock,local_lock=none,auto,user,rw 0 0
{الخادم}: {المسار إلى مجلد KlFocDataShare_klfoc} /mnt/KlFocDataShare_klfoc nfs
vers=4,nolock,local_lock=none,noauto,user,rw 0 0
```

هنا، تكون مساراتعبارة عن {الخادم}:{المسار إلى مجلد KlFocStateShare}و{الخادم}:{path to the KlFocDataShare_klfoc folder} مسارات الشبكة إلى المجلدات المشتركة على خادم الملفات.

6. أعد تشغيل كلا العقدتين.

7. قم بتحميل المجلدات المشتركة عن طريق تشغيل الأوامر التالية:

```
mount /mnt/KlFocStateShare
mount /mnt/KlFocDataShare_klfoc
```

8. تأكد من أن أذونات الوصول إلى المجلدات المشتركة تنتمي إلى ksc:kladmins.

قم بتشغيل الأمر التالي:

```
/sudo ls -la /mnt
```

9. قم بأحد الإجراءات التالية:

- على كل عقد، قم بإنشاء محول شبكة افتراضي. على سبيل المثال، قم بتشغيل الأوامر التالية:

a. اكتشف أسماء الواجهات عن طريق تشغيل الأمر التالي:

```
ifconfig
```

b. قم بتشغيل البرنامج النصي التالي (فيما يلي يتم توفير أسماء الواجهة كأمثلة):

```
bin/bash/!#

PHYSICAL_IFACE=ens160
VIRTUAL_IFACE=macvlan1

ip link del $VIRTUAL_IFACE > /dev/null 2>&1

ip link add link $PHYSICAL_IFACE $VIRTUAL_IFACE type macvlan
إذا كان [ "ne "0- "?$" ]؛ فمن ثم
يؤدي حدوث خطأ في صوت الصدى إلى إضافة محول افتراضي جديد $VIRTUAL_IFACE!
هل تريد الخروج $؟
fi

يؤدي رابط ip إلى تعطيل $VIRTUAL_IFACE
إذا كان [ "ne "0- "?$" ]؛ فمن ثم
يؤدي حدوث خطأ في صوت الصدى إلى إضافة محول افتراضي $VIRTUAL_IFACE!
هل تريد الخروج $؟
fi
```

c. قم بتشغيل الأمر التالي:

```
ip addr add {IP address of the virtual network adapter} dev {name of the
                                                    {virtual network adapter
```

يجب أن يكون عنوان IP شاغرًا عندما تنشئ محول الشبكة الافتراضية. يجب أن يكون لمحولات الشبكة الافتراضية على كلا العقدتين نفس عنوان IP.

d. تحقق من أن محول الشبكة الافتراضية قد تم إنشاؤه بنجاح.

قم بتشغيل الأوامر التالية:

```
تعيين رابط ip macvlan1
ifconfig
```

e. قم بتعطيل محول الشبكة الافتراضية عن طريق تشغيل الأمر التالي:

```
يؤدي رابط ip إلى تعطيل macvlan1
```

- 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 وUDP13000 وTCP 13291 وTCP 13299 وTCP 17000.

العقد جاهزة. لنشر مجموعة تجاوز الفشل Kaspersky، اتبع التعليمات الإضافية الواردة في السيناريو.

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

يصف هذا الإجراء كيفية تثبيت Kaspersky Security Center على عقد 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.

استخدم ملف التثبيت—ksc64_[version_number]_amd64.deb or ksc64-[version_number].x86_64.rpm—الذي يوافق توزيعة Linux المثبتة على جهازك. سوف تستقبل ملف التثبيت بتنزيله من موقع Kaspersky.

يمكن فقط لمستخدم من مجموعة مجالات KLAdmins تثبيت Kaspersky Security Center على كل عقدة.

التثبيت على العقدة الأساسية (النشطة)

لتثبيت Kaspersky Security Center على العقدة الأساسية:

1. تأكد أن الجهاز الذي ترغب في تثبيت Kaspersky Security Center عليه يعمل بإحدى توزيعات Linux المدعومة.

2. افتح سطر الأوامر وقم بتشغيل الأوامر المتوفرة في هذه التعليمات من حساب يتمتع بالمزايا الإدارية.

3. قم بتشغيل تثبيت Kaspersky Security Center. أدخل أحد الأوامر التالية، ويعتمد ذلك على توزيعة Linux لديك:

- `sudo apt install /<path>/ksc64_[version_number]_amd64.deb`
- `sudo yum install /<path>/ksc64-[version_number].x86_64.rpm -y`

4. قم بتشغيل تكوين Kaspersky Security Center:

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

5. اقرأ اتفاقية ترخيص المستخدم النهائي (EULA) وسياسة الخصوصية. يتم عرض النص في نافذة سطر الأوامر. اضغط على شريط المسافة لعرض جزء النص التالي. ثم عند المطالبة، أدخل القيم التالية:

a. اكتب y إذا كنت قد قرأت شروط اتفاقية ترخيص المستخدم النهائي (EULA). اكتب n إذا كنت لا تقبل بنود اتفاقية ترخيص المستخدم النهائي (EULA). لاستخدام Kaspersky Security Center، يجب أن تقبل بنود اتفاقية ترخيص المستخدم النهائي (EULA).

b. اكتب y إذا كنت تفهم وتقبل بنود سياسة الخصوصية، وتوافق على أن يتم التعامل مع بياناتك ونقلها كما هو موصوف في سياسة الخصوصية (ويشمل ذلك إلى بلاد الطرف الثالث). اكتب n إذا كنت لا تقبل بنود سياسة الخصوصية. لاستخدام Kaspersky Security Center، يجب أن تقبل شروط سياسة الخصوصية.

6. حدد **عقدة المجموعة الأساسية** كوضع تثبيت خادم الإدارة.

7. عند المطالبة، أدخل الإعدادات التالية:

a. أدخل المسار المحلي لنقطة التحميل لمشاركة الحالة.

b. أدخل المسار المحلي لنقطة التحميل لمشاركة البيانات.

c. اختر وضع اتصال مجموعة تجاوز الفشل: من خلال محول شبكة افتراضية أو موازن تحميل خارجي.

d. إذا كنت تستخدم محول شبكة افتراضية، فأدخل اسمه.

e. عندما تتم مطالبتك بإدخال اسم DNS لخادم الإدارة أو عنوان IP الثابت، أدخل عنوان IP الخاص بمحول الشبكة الافتراضية أو عنوان IP الخاص بموازن التحميل الخارجي.

f. أدخل رقم منفذ خادم الإدارة. يتم استخدام المنفذ 14000 بشكل افتراضي.

g. أدخل رقم منفذ SSL لخادم الإدارة. يتم استخدام المنفذ 13000 بشكل افتراضي.

h. قم بتقييم العدد التقريبي للأجهزة التي ترغب في إدارتها:

- إذا كان لديك من 1 إلى 100 جهاز متصل بالشبكة، فادخل إلى جهاز واحد.
- إذا كان لديك من 101 إلى 1000 جهاز متصل بالشبكة، فادخل إلى جهازين.
- إذا كان لديك أكثر من 1000 جهاز متصل بالشبكة، فادخل إلى ثلاثة أجهزة.

i. أدخل اسم مجموعات الأمان للخدمات. بشكل افتراضي، يتم استخدام مجموعة 'kladmins'.

j. أدخل اسم الحساب لبدء خدمة خادم الإدارة. يجب أن يكون الحساب عضوًا في مجموعة الأمان المدخلة. بشكل افتراضي، يتم استخدام حساب 'ksc'.

k. أدخل اسم الحساب لبدء الخدمات الأخرى. يجب أن يكون الحساب عضوًا في مجموعة الأمان المدخلة. بشكل افتراضي، يتم استخدام حساب 'ksc'.

l. أدخل عنوان IP للجهاز المثبت عليه قاعدة البيانات.

m. أدخل رقم منفذ قاعدة البيانات. يتم استخدام هذا المنفذ في التواصل مع خادم الإدارة. يتم استخدام المنفذ 3306 بشكل افتراضي.

n. أدخل اسم قاعدة البيانات.

o. أدخل معلومات تسجيل الدخول لحساب إدارة قاعدة البيانات الذي ستستخدمه للوصول إلى قاعدة البيانات.

p. أدخل كلمة المرور لحساب إدارة قاعدة البيانات الذي ستستخدمه في الوصول إلى قاعدة البيانات.

انتظر حتى تنتهي إضافة الخدمات وتبدأ في العمل بشكل تلقائي:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. أنشئ حسابًا يكون هو مسؤول خادم الإدارة. أدخل اسم المستخدم وكلمة المرور. لا يمكن أن تكون كلمة المرور أقل من 8 حروف ولا أكثر من 16 حرفًا.

تتم إضافة المستخدم ويتم تثبيت Kaspersky Security Center على العقدة الأساسية.

التثبيت على العقدة الثانوية (الخاملة)

لتثبيت Kaspersky Security Center على العقدة الثانوية:

1. تأكد أن الجهاز الذي ترغب في تثبيت Kaspersky Security Center عليه يعمل بإحدى توزيعات Linux المدعومة.
2. افتح سطر الأوامر وقم بتشغيل الأوامر المتوفرة في هذه التعليمات من حساب يتمتع بالمزايا الإدارية.
3. قم بتشغيل تثبيت Kaspersky Security Center. أدخل أحد الأوامر التالية، ويعتمد ذلك على توزيعة Linux لديك:
   - `sudo apt install /<path>/ksc64_[version_number]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[version_number].x86_64.rpm -y`
4. قم بتشغيل تكوين Kaspersky Security Center:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. اقرأ اتفاقية ترخيص المستخدم النهائي (EULA) وسياسة الخصوصية. يتم عرض النص في نافذة سطر الأوامر. اضغط على شريط المسافة لعرض جزء النص التالي. ثم عند المطالبة، أدخل القيم التالية:

   a. اكتب y إذا كنت قد قرأت شروط اتفاقية ترخيص المستخدم النهائي (EULA). اكتب n إذا كنت لا تقبل بنود اتفاقية ترخيص المستخدم النهائي (EULA). لاستخدام Kaspersky Security Center، يجب أن تقبل بنود اتفاقية ترخيص المستخدم النهائي (EULA).

   b. اكتب y إذا كنت تفهم وتقبل بنود سياسة الخصوصية، وتوافق على أن يتم التعامل مع بياناتك ونقلها كما هو موصوف في سياسة الخصوصية (ويشمل ذلك إلى بلاد الطرف الثالث). اكتب n إذا كنت لا تقبل بنود سياسة الخصوصية. لاستخدام Kaspersky Security Center، يجب أن تقبل شروط سياسة الخصوصية.

6. حدد **عقدة المجموعة الثانوية** كوضع تثبيت خادم الإدارة.
7. عند المطالبة، أدخل المسار المحلي إلى نقطة التحميل لمشاركة الحالة.

تم تثبيت Kaspersky Security Center على العقدة الثانوية.

تأكيد الخدمة

استخدم الأوامر التالية في التحقق إذا ما كانت الخدمة تعمل أم لا:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`

- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

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 النشطة، انتقل إلى /opt/kaspersky/ksc64/sbin.
2. افتح سطر الأوامر، ثم قم بتشغيل أحد الأوامر التالية:
   - لإيقاف المجموعة، قم بتشغيل: `klfoc -stopcluster --stp klfoc`
   - لبدء المجموعة، قم بتشغيل: `klfoc -startcluster --stp klfoc`

   يتم بدء تشغيل نظام مجموعة تجاوز الفشل أو إيقافه، بناءً على الأمر الذي تقوم بتشغيله.

المحافظة على إحدى العقد

للحفاظ على إحدى العقد:

1. على العقدة المفعلة، قم بإيقاف مجموعة تجاوز الفشل باستخدام الأمر `klfoc -stopcluster --stp klfoc`.
2. في العقدة التي تريد صيانتها، انتقل إلى /opt/kaspersky/ksc64/sbin.
3. افتح سطر الأوامر، ثم افصل العقدة عن المجموعة من خلال تشغيل الأمر `detach_node.sh` .
4. على العقدة المفعلة ، ابدأ تشغيل نظام مجموعة تجاوز الفشل باستخدام الأمر `klfoc -startcluster --stp klfoc`.
5. أداء أنشطة الصيانة.
6. على العقدة المفعلة، قم بإيقاف مجموعة تجاوز الفشل باستخدام الأمر `klfoc -stopcluster --stp klfoc`.
7. في العقدة التي تمت صيانتها، انتقل إلى /opt/kaspersky/ksc64/sbin.
8. افتح سطر الأوامر، ثم قم بإرفاق العقدة بالمجموعة من خلال تشغيل الأمر `attach_node.sh` .
9. على العقدة المفعلة ، ابدأ تشغيل نظام مجموعة تجاوز الفشل باستخدام الأمر `klfoc -startcluster --stp klfoc`.

   يتم الاحتفاظ بالعقدة وإرفاقها بمجموعة تجاوز الفشل.

شهادات للعمل مع Kaspersky Security Center

يحتوي القسم على معلومات حول شهادات Kaspersky Security Center وكيفية إصدار واستبدال شهادات Kaspersky Security Center 14 Web Console وكيفية تجديد شهادة خادم الإدارة إذا كان الخادم يتفاعل مع Kaspersky Security Center 14 Web Console.

حول شهادات Kaspersky Security Center

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

- شهادة خادم الإدارة
- شهادة خادم الويب
- 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 klsetsrvcert أو من خلال قسم خصائص خادم الإدارة في Kaspersky Security Center 14 Web Console وفقا لنوع الشهادة. عند استخدام الأداة المساعدة klsetsrvcert، فعليك تحديد نوع الشهادة باستخدام إحدى القيم التالية:

- C—الشهادة العامة للمنفذين 13000 و13291.
- CR—شهادة الاحتياطي المشترك للمنفذين 13000 و13291.

شهادات خادم الإدارة

مطلوب شهادة خادم الإدارة للأغراض التالية:

- مصادقة خادم الإدارة عند الاتصال بـ Kaspersky Security Center 14 Web Console
- تفاعل آمن بين خادم الإدارة عميل الشبكة على الأجهزة المدارة.
- المصادقة عندما تكون خوادم الإدارة الأساسية متصلة بخوادم الإدارة الثانوية

ويتم إنشاء شهادة خادم الإدارة تلقائيًا أثناء تثبيت مكون خادم الإدارة ويتم تخزينها في المجلد /var/opt/kaspersky/klnagent_srv/1093/cert/. أنت تحدد شهادة خادم الإدارة عند إنشاء ملف استجابة لتثبيت Kaspersky Security Center 14 Web Console. تسمى هذه الشهادة بالمشتركة ("C").

شهادة خادم الإدارة صالحة لمدة 397 يومًا. يُنشئ Kaspersky Security Center شهادة احتياطية مشتركة ("CR") 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.

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

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

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.

شهادة خادم الويب

يتم استخدام نوع خاص من الشهادات بواسطة خادم الويب، وهو أحد مكونات خادم إدارة Kaspersky Security Center Administration Server. هذه الشهادة مطلوبة لنشر حزم تثبيت وكيل الشبكة التي تقوم بتنزيلها لاحقًا على الأجهزة المُدارة. بالنسبة لهذا الغرض، يمكن لخادم الويب استخدام شهادات مختلفة.

يستخدم خادم الويب إحدى الشهادات التالية، بترتيب الأولوية:

1. شهادة خادم الويب المخصصة التي حددتها يدويًا عن طريق Kaspersky Security Center 14 Web Console
2. شهادة خادم الإدارة المشتركة ("C")

شهادة Kaspersky Security Center 14 Web Console

يمتلك خادم Kaspersky Security Center 14 Web Console (المشار إليه فيما يلي باسم Web Console) شهادته الخاصة. عند فتح موقع ويب، يتحقق المستعرض مما إذا كان اتصالك موثوقًا به أم لا. تسمح لك شهادة Web Console بمصادقة Web Console وتُستخدم لتشفير حركة المرور بين المستعرض ووحدة تحكم الويب.

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

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

متطلبات الشهادات المخصصة المستخدمة في Kaspersky Security Center

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

متطلبات شهادات Kaspersky Security Center

نوع الشهادة	المتطلبات	تعليقات
الشهادة المشتركة، الشهادة الاحتياطية المشتركة ("C"، "CR")	الحد الأدنى لطول المفتاح: 2048. القيود الأساسية: • مرجع معتمد: صحيح • قيد طول المسار: لا شيء استخدام المفتاح: • توقيع إلكتروني • توقيع الشهادة • تشفير المفتاح	معلمة استخدام المفتاح الموسع اختيارية. يمكن لقيمة قيد طول المسار أن تختلف عن "لا شيء"، ولكنها لا تقل عن "1".

	• توقيع CRL استخدام المفتاح الموسع (اختياري): مصادقة الخادم، مصادقة العميل.	
شهادة خادم الويب	استخدام المفتاح الموسع : مصادقة الخادم. تتضمن حاوية PEM / PKCS # 12 التي تم تحديد الشهادة منها السلسلة الكاملة للمفاتيح العامة. الاسم البديل للموضوع (SAN) للشهادة موجود؛ أي أن قيمة حقل `subjectAltName` صالحة. تستوفي الشهادة المتطلبات الفعالة لمتصفحات الويب المفروضة على شهادات الخادم، فضلاً عن المتطلبات الأساسية الحالية لمنتدى CA/Browser.	لايمكن تطبيقه.
شهادة Kaspersky Security Center 14 Web Console	تتضمن حاوية PEM التي تم تحديد الشهادة منها السلسلة الكاملة للمفاتيح العامة. الاسم البديل للموضوع (SAN) للشهادة موجود؛ أي أن قيمة حقل `subjectAltName` صالحة. تستوفي الشهادة المتطلبات الفعالة لمتصفحات الويب المفروضة على شهادات الخادم، فضلاً عن المتطلبات الأساسية الحالية لمنتدى CA/Browser.	لا يتم دعم الشهادات المشفرة بواسطة Kaspersky Security Center 14 Web Console.

إعادة إصدار شهادة Kaspersky Security Center 14 Web Console

تضع معظم المستعرضات حدًا على مدة الصلاحية للشهادة. وكي تكون ضمن ذلك الحد، يتم تحديد مدة صلاحية شهادة Kaspersky Security Center 14 Web Console إلى 397 يومًا. يمكنك استبدال أي شهادة موجودة مستلمة من جهة إصدار شهادات معتمدة بإصدار شهادة جديدة موقعة ذاتيًا بشكل يدوي. كحل بديل، يمكنك إعادة إصدار شهادة Kaspersky Security Center 14 Web Console المنتهية لديك.

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

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

لإعادة إصدار شهادة Kaspersky Security Center 14 Web Console المنتهية:

أعد تثبيت Kaspersky Security Center 14 Web Console من خلال تنفيذ أحد الإجراءات التالية:

- إذا كنت ترغب في استخدام نفس ملف التثبيت الخاص بـ Kaspersky Security Center 14 Web Console، فأزلKaspersky Security Center 14 Web Console، ثم قم بتثبيت نفس إصدار Kaspersky Security Center 14 Web Console.
- إذا كنت تريد استخدام ملف تثبيت لإصدار تمت ترقيته، فقم بتشغيل أمر الترقية.

يتم إعادة إصدار Kaspersky Security Center 14 Web Console لمدة صلاحية أخرى مدتها 397 يومًا.

استبدال شهادة Kaspersky Security Center 14 Web Console

بشكل افتراضي، عندما تقوم بتثبيت Kaspersky Security Center 14 Web Console Server (يُشار إليه أيضًا باسم Kaspersky Security Center 14 Web Console)، يتم إنشاء شهادة متصفح للتطبيق تلقائيًا. يمكنك استبدال الشهادة التي تم إنشاؤها بشكل تلقائي بأخرى مخصصة.

لاستبدال شهادة Kaspersky Security Center 14 Web Console بأخرى مخصصة:

1. قم بإنشاء ملف استجابة جديد مطلوب لتثبيت Kaspersky Security Center 14 Web Console.
2. في هذا الملف، حدد المسارات إلى ملف الشهادة المخصص وملف المفتاح باستخدام معلمة `certPath` ومعلمة `keyPath`.
3. أعد تثبيت Kaspersky Security Center 14 Web Console من خلال تحديد ملف الاستجابة الجديد. قم بأحد الإجراءات التالية:

- إذا كنت ترغب في استخدام نفس ملف التثبيت الخاص بـ Kaspersky Security Center 14 Web Console، فأزل Kaspersky Security Center 14 Web Console، ثم قم بتثبيت نفس إصدار Kaspersky Security Center 14 Web Console.
- إذا كنت تريد استخدام ملف تثبيت لإصدار تمت ترقيته، فقم بتشغيل أمر الترقية.

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 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.

السيناريو: تحديد شهادة خادم الإدارة المخصصة

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

إذا حددت مدة صلاحية أطول من 397 يومًا 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 أيضًا سلسلة الثقة الكاملة والمفتاح الخاص، والتي يجب تخزينها في ملف بامتداد pfx أو p12. بالنسبة للشهادة الجديدة، يجب استيفاء المتطلبات المذكورة في الجدول أدناه.

نوع الشهادة: الشهادة المشتركة، والشهادة الاحتياطية المشتركة ("C"، "CR")

المتطلبات:

- 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.

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 اتصالهم وسيظهر "خطأ في مصادقة خادم الإدارة". لتحديد الشهادة الجديدة واسترجاع الاتصال، استخدم خط الأوامر الأداة المساعدة klmover.

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 معلمات الأداة المساعدة klsetsrvcert في الجدول أدناه.

قيم معلمات 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؛
-f <time>	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.
-i <<inputfile	حاوية تحتوي على الشهادة والمفتاح الخاص بتنسيق PKCS#12 (ملف بامتداد .p12 أو .pfx).
-p <<password	كلمة المرور المستخدمة لحماية الحاوية p12. يتم تخزين الشهادة والمفتاح الخاص في الحاوية ، وبالتالي، فإن كلمة المرور مطلوبة لفك تشفير الملف مع الحاوية.
-o <chkopt>	معلمات التحقق من صحة الشهادة (مفصولة بفاصلة منقوطة). لاستخدام شهادة مخصصة بدون إذن التوقيع، حدد -o NoCA في الأداة المساعدة klsetsrvcert. هذا مفيد للشهادات الصادرة عن مرجع مصدق عام.
-g <<dnsname	سيتم إنشاء شهادة جديدة لاسم DNS المحدد.
-r <<calistfile	قائمة جهة إصدار الشهادة الجذرية الموثوقة، بتنسيق PEM.
-l <<logfile	ملف إخراج النتائج. بشكل افتراضي، يتم إعادة توجيه الإخراج إلى دفق إخراج قياسي.

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

```
klsetsrvcert -t C -i <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 klsetsrvcert، تحتاج إلى إنشاء اتصال SSL بين عملاء الشبكة وخادم الإدارة لأن الاتصال مقطوع.

لتحديد شهادة خادم الإدارة الجديدة واستعادة الاتصال:

في موجّه الأوامر، شغل الأداة التالية:

```
klmover [-عنوان <عنوان الخادم>] [-pn <رقم المنفذ1>] [-ps < رقم منفذ SSL>] [-nossl] [-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 klsetsrvcert

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

تحديد مجلد مشترك

بعد تثبيت خادم الإدارة، يمكنك تحديد موقع المجلد المشترك، في خصائص خادم الإدارة. افتراضيًا، يتم إنشاء المجلد المشترك على الجهاز باستخدام خادم الإدارة. 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.

حول ترقية Kaspersky Security Center Linux

يمكنك تثبيت الإصدار 14 من خادم الإدارة على جهاز مثبت عليه إصدار قديم من خادم الإدارة (بدءًا من الإصدار 13). عند الترقية إلى الإصدار 14، يتم حفظ جميع البيانات والإعدادات من الإصدار السابق لخادم الإدارة.

أثناء الترقية، يُحظر تمامًا الاستخدام المتزامن لنظام إدارة قواعد البيانات بواسطة خادم الإدارة وتطبيق آخر.

يمكنك ترقية إصدار خادم الإدارة باستخدام إحدى الطرق التالية:

- باستخدام ملف تثبيت Kaspersky Security Center
- من خلال إنشاء النسخة الاحتياطية لبيانات خادم الإدارة، وتثبيت إصدار خادم الإدارة الجديد، واستعادة بيانات خادم الإدارة من النسخة الاحتياطية

إذا كانت شبكتك تتضمن العديد من خوادم الإدارة، فيجب عليك ترقية كل خادم يدويًا. لا يدعم Kaspersky Security Center Linux الترقية المركزية.

عند ترقية Kaspersky Security Center Linux من إصدار سابق، يتم الاحتفاظ بجميع المكونات الإضافية المثبتة لتطبيقات Kaspersky المدعومة. تتم ترقية المكون الإضافي لخادم الإدارة والمكون الإضافي لوكيل الشبكة تلقائيًا.

ترقية Kaspersky Security Center Linux باستخدام ملف التثبيت

لترقية خادم الإدارة من إصدار سابق (بدءًا من الإصدار 13) إلى الإصدار 14، يمكنك تثبيت إصدار جديد فوق إصدار سابق باستخدام ملف تثبيت Kaspersky Security Center .

لترقية إصدار سابق من خادم الإدارة إلى الإصدار 14 باستخدام ملف التثبيت:

1. قم بتنزيل ملف تثبيت Kaspersky Security Center بحزمة كاملة للإصدار 14 من خلال موقع Kaspersky الإلكتروني:
   - للأجهزة التي تعمل بنظام تشغيل مستند إلى RPM — ksc64- <version number> -11247.x86_64.rpm
   - للأجهزة التي تعمل بنظام تشغيل مستند إلى Debian — ksc64_ <version number> -11247_amd64.deb
2. قم بترقية حزمة التثبيت باستخدام مدير الحزم الذي تستخدمه على خادم الإدارة. على سبيل المثال، يمكنك استخدام الأوامر التالية في محطة سطر الأوامر ضمن حساب بامتيازات الجذر:
   - بالنسبة للأجهزة التي تعمل بنظام لتشغيل مستند إلى RPM:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<رقم الإصدار>-11247.rpm.x86_64
     ```
   - بالنسبة للأجهزة التي تعمل بنظام تشغيل مستند إلى Debian:
     ```
     $ sudo dpkg -i ksc64_<رقم الإصدار>-11247_amd64.deb
     ```

   بعد تنفيذ الأمر بنجاح، يتم إنشاء البرنامج النصي /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. يتم عرض الرسالة حول ذلك في المحطة.
3. قم بتشغيل البرنامج النصي /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl لتكوين خادم الإدارة الذي تمت ترقيته.
4. اقرأ اتفاقية الترخيص وسياسة الخصوصية، التي تظهر في محطة سطر الأوامر. إذا كنت توافق على جميع شروط اتفاقية الترخيص وسياسة الخصوصية:
   a. أدخل "Y" لتأكيد أنك قد قرأت وفهمت وقبول شروط وأحكام اتفاقية ترخيص المستخدم النهائي (EULA) بالكامل.
   b. أدخل "Y" مرة أخرى لتأكيد أنك قد قرأت وفهمت وقبول سياسة الخصوصية التي تصف معالجة البيانات بالكامل.

   سيستمر تثبيت التطبيق على جهازك بعد إدخالك "Y" مرتين.

5. أدخل "1" لتحديد وضع تثبيت خادم الإدارة القياسي.

توضح الصورة أدناه آخر خطوتين.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

قبول شروط اتفاقية ترخيص المستخدم النهائي (EULA) وسياسة الخصوصية، وتحديد وضع تثبيت خادم الإدارة القياسي في محطة سطر الأوامر

بعد ذلك، يقوم النص بتكوين وإنهاء ترقية خادم الإدارة. أثناء الترقية، لا يمكنك تغيير إعدادات خادم الإدارة التي تم تعديلها قبل الترقية.

6. للأجهزة المثبت عليها إصدار عميل شبكة قديم، قم بإنشاء وتشغيل مهمة التثبيت عن بُعد للإصدار الجديد من عميل الشبكة.

نوصي بترقية Network Agent لنظام Linux إلى نفس إصدار Kaspersky Security Center Linux.

بعد إتمام مهمة التثبيت عن بُعد، سيتم ترقية إصدار عميل الشبكة.

ترقية Kaspersky Security Center Linux من خلال النسخ الاحتياطي

لترقية خادم الإدارة من إصدار سابق (بدءًا من الإصدار 13) إلى الإصدار 14، يمكنك إنشاء نسخة احتياطية من بيانات خادم الإدارة واستعادة هذه البيانات بعد تثبيت Kaspersky Security Center لإصدار جديد. في حالة حدوث مشكلة أثناء التثبيت، يمكنك استعادة الإصدار السابق من خادم الإدارة باستخدام النسخة الاحتياطية لبيانات خادم الإدارة التي تم إنشاؤها قبل الترقية.

لترقية إصدار قديم من خادم الإدارة إلى الإصدار 14 باستخدام النسخة الاحتياطية:

1. قبل الترقية، انسخ بيانات خادم الإدارة احتياطيًا بإصدار أقدم من التطبيق.
2. قم بإلغاء تثبيت الإصدار الأقدم من Kaspersky Security Center.
3. قم بتثبيت الإصدار 14 من Kaspersky Security Center على خادم الإدارة السابق.
4. قم باستعادة بيانات خادم الإدارة من النسخة الاحتياطية التي تم إنشاؤها قبل الترقية.
5. للأجهزة المثبت عليها إصدار عميل شبكة قديم، قم بإنشاء وتشغيل مهمة التثبيت عن بُعد للإصدار الجديد من عميل الشبكة.

نوصي بترقية Network Agent لنظام Linux إلى نفس إصدار Kaspersky Security Center Linux.

بعد إتمام مهمة التثبيت عن بُعد، سيتم ترقية إصدار عميل الشبكة.

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 تضف إلا خادم إدارة واحد، لن يتم عرض إلا حقلي تسجيل الدخول وكلمة المرور.

3. قم بأحد الإجراءات التالية:

- لتسجيل الدخول إلى خادم الإدارة الفعلي، أدخل اسم المستخدم وكلمة المرور للمسؤول المحلي.
- إذا تم إنشاء واحد أو أكثر من خوادم الإدارة الافتراضية على الخادم وتريد تسجيل الدخول إلى خادم افتراضي:

  a. انقر على **إعدادات متقدمة**.

  b. اكتب اسم خادم الإدارة الظاهري الذي حددته أثناء إنشاء الخادم الإفتراضي .

  c. أدخل اسم المستخدم وكلمة المرور للمسؤول الذي لديه حقوق على خادم الإدارة الإفتراضي.

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 Linux.

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.

معالج البدء السريع

يتيح لك Kaspersky Security Center Linux 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.
- 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 المدارة.

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 على**بدء معالج البدء السريع**.

سيطالبك المعالج بإجراء التكوين الأولي لخادم الإدارة. اتبع إرشادات المعالج. انتقل عبر المعالج من خلال استخدام زر **التالي**.

الخطوة 1. تحديد إعدادات اتصال الإنترنت

حدد إعدادات الوصول إلى الإنترنت الخاص بـ Kaspersky Security Center Linux.

حدد خانة الاختيار **استخدام الخادم الوكيل** إذا كنت ترغب في استخدام خادم وكيل عند الاتصال بالإنترنت. إذا تم تحديد خانة الاختيار هذه، فستتوفر الحقول لإدخال الإعدادات. حدد الإعدادات التالية لاتصال خادم الوكيل:

- **العنوان**
- **رقم المنفذ**
- **تجاوز الخادم الوكيل للعناوين المحلية**

لن يتم استخدام خادم وكيل للاتصال بالأجهزة في الشبكة المحلية.

- **مصادقة الخادم الوكيل**

إذا تم تحديد خانة الاختيار تلك، يمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.
يتوفر حقل الإدخال هذا إذا تم تحديد خانة الاختيار **استخدام الخادم الوكيل**.

- **اسم المستخدم** (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 اختيار **مصادقة الخادم الوكيل**).

- **كلمة المرور** (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 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 Linux التالية:

- **عن طريق إدخال رمز التنشيط الذي تملكه**

رمز التنشيط هو تسلسل فريد مكون من 20 حرفًا أبجديًا رقميًا. تقوم بإدخال رمز تنشيط لإضافة مفتاح يقوم بدوره بتنشيط Kaspersky Security Center Linux. 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 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 قسم **العمليات** ← **الترخيص** ← **تراخيص KASPERSKY** من القائمة الرئيسية.

- **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 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 قسم **العمليات** ← **الترخيص** ← **تراخيص KASPERSKY** من القائمة الرئيسية.

- عن طريق تأجيل تفعيل التطبيق

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 3. 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 4. تكوين إشعارات البريد الإلكتروني

قم بتكوين تسليم الإخطارات المتعلقة بالأحداث المسجلة أثناء تشغيل تطبيقات Kaspersky على الأجهزة العميلة. وستُستخدم هذه الإعدادات كإعدادات افتراضية لسياسات التطبيق.

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 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** و**كلمة 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 الجديدة بالنقر فوق الزر **إرسال رسالة اختبار**.

الخطوة 5. إغلاق معالج البدء السريع

لإغلاق المعالج، انقر على زر **إنهاء**.

بعد الانتهاء من معالج البدء السريع، يمكنك تشغيل معالج نشر الحماية لتثبيت برامج الخصوصية أو عميل الشبكة تلقائيًا على الأجهزة الموجودة على شبكتك.

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 مسبقًا). 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 حديثًا في قسم **المهام**. يمكنك بدء هذه المهمة يدويًا لاحقًا. 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

يمكنك بدء تشغيل معالج نشر الحماية يدويًا في أي وقت.

لبدء معالج نشر الحماية يدويًا،

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 تقم بإضافة المفتاح إلى حزمة التثبيت**

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**

يتم توزيع المفتاح على الأجهزة بالإضافة إلى حزمة التثبيت.

لا نوصي بقيامك بتوزيع المفتاح باستخدام هذه الطريقة؛ لأن حقوق الوصول للقراءة المشتركة ممكّنة لمستودع حزم التثبيت.

إذا كانت حزمة التثبيت 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**

إذا تم تحديد هذا الخيار، فسوف يتم إنشاء مهمة التثبيت عن بُعد لمجموعة أجهزة.

- **تحديد أجهزة للتثبيت**

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 العميلة:

- **استخدام عميل الشبكة**

إذا كان هذا الخيار مفعلاً، سيتم تسليم حزم التثبيت إلى الأجهزة العميلة بواسطة عميل الشبكة المثبت على الأجهزة العميلة هذه.
في حال تعطيل هذا الخيار، سيتم تسليم حزم التثبيت باستخدام أدوات نظام التشغيل Linux
ننصح بتفعيل هذا الخيار إذا تم تعيين المهمة إلى الأجهزة المثبت عليها عملاء الشبكة.
يتم تمكين هذا الخيار افتراضيًا.

- **استخدام موارد نظام التشغيل عبر نقاط التوزيع**

إذا تم تفعيل هذا الخيار، سيتم نقل حزم التثبيت إلى الأجهزة العميلة باستخدام أدوات نظام التشغيل من خلال نقاط التوزيع. يمكنك تحديد هذا الخيار إذا كانت توجد نقطة توزيع واحدة على الأقل في الشبكة.

في حالة تفعيل هذا الخيار **استخدام عميل الشبكة**، يتم تسليم الملفات بواسطة أدوات نظام التشغيل فقط في حالة عدم توفر موارد عميل الشبكة.

يتم تفعيل هذا الخيار افتراضيًا لمهام التثبيت عن بُعد التي تم إنشاؤها على خادم إدارة افتراضي.

حدد الإعداد الإضافي:

لا تقم بإعادة تثبيت التطبيق إذا كان مثبتًا بالفعل

إذا تم تفعيل هذا الخيار، لن يتم عادة تثبيت التطبيق المحدد إذا كان مثبتًا بالفعل على الجهاز العميل هذا.

إذا تم تفعيل هذا الخيار، سيتم تثبيت التطبيق بأية حال.

يتم تمكين هذا الخيار افتراضيًا.

الخطوة 6. 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 Linux 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 7. نقل الأجهزة إلى الأجهزة المُدارة

حدد إذا ما كان يجب نقل الأجهزة إلى مجموعة إدارة بعد تثبيت عميل الشبكة أم لا.

- **عدم نقل الأجهزة**

تبقى الأجهزة في المجموعات الموجودة فيها حاليًا. والأجهزة التي لم يتم وضعها في مجموعة تبقى دون تخصيص.

- **نقل الأجهزة غير المخصصة إلى مجموعة**

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 8. تحديد الحسابات للوصول إلى الأجهزة

أضف الحسابات التي سيتم استخدامها لبدء مهمة التثبيت عن بُعد:

- **لا يلزم وجود حساب (تم تثبيت عميل الشبكة)**

إذا تم تحديد هذا الخيار، فلا يلزم تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

إذا لم يتم تثبيت كيل الشبكة على الأجهزة العميلة، فلن يتوفر هذا الخيار.

- **يُلزم وجود حساب (عميل الشبكة غير مستخدم)**

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 9. 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.

انقر على **موافق** لإكمال الخطوة الأخيرة من معالج نشر الحماية.

تكوين خادم الإدارة

يصف هذا القسم عملية التكوين وخصائص خادم إدارة Kaspersky Security Center Linux.

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.

تكوين قائمة السماح بعناوين IP لتسجيل الدخول إلى Kaspersky Security Center

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). ومع ذلك، يمكنك تكوين خادم الإدارة بحيث يمكن للمستخدمين الاتصال به فقط من الأجهزة ذات عناوين IP المسموح بها. في هذه الحالة، حتى إذا سرق متطفل حساب Kaspersky Security Center، فلن يتمكن من تسجيل الدخول إلى Kaspersky Security Center لأن عنوان IP الخاص بجهاز الدخيل ليس في قائمة السماح.

يتم التحقق من عنوان IP عندما يقوم المستخدم بتسجيل الدخول إلى Kaspersky Security Center أو تشغيل تطبيق يتفاعل مع خادم الإدارة عبر Kaspersky Security Center OpenAPI. يحاول جهاز المستخدم إنشاء اتصال بخادم الإدارة في هذه اللحظة. إذا لم يكن عنوان IP للجهاز مدرجًا في قائمة السماح، فسيحدث خطأ في المصادقة ويعلمك حدث KLAUD_EV_SERVERCONNECT أنه لم يتم إنشاء اتصال بخادم الإدارة.

متطلبات قائمة السماح لعناوين IP

يتم التحقق من عناوين IP فقط عندما تحاول التطبيقات التالية الاتصال بخادم الإدارة:

- خدمة وحدة تحكم الويب

  إذا قمت بتسجيل الدخول إلى Kaspersky Security Center من خلال Web Console، فيمكنك 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 Kaspersky Security Center على جهاز واحد وتم تثبيت خادم وحدة التحكم على الويب على جهاز آخر، فإن جدار الحماية يساعد على منع المتطفلين من التدخل.

- تتفاعل التطبيقات مع خادم الإدارة عبر كائنات أتمتة klakaut

- التطبيقات التي تتفاعل مع خادم الإدارة عبر OpenAPI، مثل Kaspersky Anti Targeted Attack Platform أو Kaspersky Security for Virtualization

لذلك، حدد عناوين الأجهزة التي تم تثبيت التطبيقات المذكورة أعلاه عليها.

يمكنك تعيين عناوين IPv4 وIPv6. لا يمكنك تحديد نطاقات عناوين IP.

كيفية إنشاء قائمة السماح بعناوين IP

إذا لم تقم بتعيين قائمة السماح مسبقًا، فاتبع الإرشادات أدناه.

لإنشاء قائمة السماح بعناوين IP لتسجيل الدخول إلى Kaspersky Security Center:

1. على جهاز خادم الإدارة، قم بتشغيل موجه الأوامر ضمن حساب له حقوق المسؤول.

2. غيّر دليلك الحالي إلى مجلد تثبيت Kaspersky Security Center (عادةً، /opt/kaspersky/ksc64/sbin/).

3. أدخل الأمر التالي، باستخدام حقوق المسؤول:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<عناوين IP>" -t s
```

حدد عناوين IP التي تفي بالمتطلبات المذكورة أعلاه. يجب فصل عدة عناوين IP بفاصلة منقوطة.

مثال على كيفية السماح لجهاز واحد فقط بالاتصال بخادم الإدارة:

```
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؛198.51.100.0؛203.0.113.0" -ts
```

4. قم بإعادة تشغيل خدمة خادم الإدارة.

يمكنك معرفة ما إذا كنت قد نجحت في تكوين قائمة السماح بعناوين IP في سجل الحدث Syslog 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:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<عناوين IP>" -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 198.51.100.0 IP. 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؛203.0.113.0" -ts
```

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.

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\adminkit\logs\sc.syslog.

تعيين الحد الأقصى لعدد الأحداث في مستودع الأحداث

من القسم **مستودع الأحداث** في النافذة خصائص خادم الإدارة، يمكنك تحرير إعدادات تخزين الأحداث في قاعدة بيانات خادم الإدارة من خلال تقييد عدد سجلات الأحداث أو مدة تخزين السجل. عندما تحدد الحد الأقصى لعدد الأحداث، يقوم التطبيق بحساب مقدار تقريبي لمساحة التخزين المطلوبة للرقم المحدد. يمكنك استخدام هذا الحساب التقريبي لتقييم ما إذا كانت لديك مساحة خالية كافية على القرص لتجنب تجاوز سعة قاعدة البيانات. السعة الافتراضية لقاعدة بيانات خادم الإدارة هي 400,000 حدث. أقصى سعة موصى بها لقاعدة البيانات هي 45 مليون حدث.

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.

لتقييد 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**. حدد الحد الأقصى لعدد الأحداث المخزّنة في قاعدة البيانات.

3. انقر على زر **حفظ**.

النسخ الاحتياطي والاستعادة لبيانات خادم الإدارة

النسخ الاحتياطي للبيانات يسمح بنقل خادم الإدارة من جهاز إلى آخر دون فقان 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.

لاحظ أن المكونات الإضافية للإدارة المثبتة لا يتم نسخها احتياطيًا. بعد استعادة بيانات خادم الإدارة من نسخة احتياطية، تحتاج إلى تنزيل وإعادة تثبيت المكونات الإضافية للتطبيقات المدارة.

يمكنك إنشاء نسخة احتياطية من بيانات خادم الإدارة بإحدى الطرق التالية:

- من خلال إنشاء مهمة نسخ احتياطي للبيانات وتشغيلها من خلال Kaspersky Security Center 14 Web Console.
- 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، توجد الأداة المساعدة في أساس مجلد الوجهة المحدد عند تثبيت التطبيق (عادةً،

/opt/kaspersky/ksc64/sbin/klbackup/).

يتم حفظ البيانات التالية في النسخة الاحتياطية لخادم الإدارة:

- قاعدة بيانات خادم الإدارة (السياسات والمهام وإعدادات التطبيق والأحداث المحفوظة في خادم الإدارة).
- تفاصيل التكوين الخاصة ببنية مجموعات الإدارة والأجهزة العميلة.
- تخزين حزم توزيع التطبيقات للتثبيت عن بُعد.
- شهادة خادم الإدارة.

ولا يمكن استعادة بيانات خادم الإدارة إلا باستخدام أداة klbackup المساعدة.

إنشاء مهمة نسخ احتياطي لبيانات خادم الإدارة

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.

يمكن إنشاء مهمة النسخ الاحتياطي لبيانات خادم الإدارة في نسخة مفردة فقط. إذا تم بالفعل إنشاء مهمة النسخ الاحتياطي لبيانات خادم الإدارة من أجل خادم الإدارة، فلن يتم عرضها في نافذة تحديد نوع المهمة.

لإنشاء مهمة نسخ احتياطي لبيانات خادم الإدارة:

1. انتقل إلى **الأجهزة** ← **المهام**.
2. انقر على **إضافة**.

   يبدأ تشغيل معالج إضافة مهمة.
3. في الصفحة الأولى من المعالج في قائمة **التطبيق**، حدد **Kaspersky Security Center 14**، وفي قائمة **نوع المهمة** حدد **النسخ الاحتياطي لبيانات خادم الإدارة**.
4. في الصفحة المقابلة في المعالج، حدد المعلومات التالية:
   - مجلد لتخزين النسخ الاحتياطية
   - كلمة مرور للنسخ الاحتياطي (اختياري)
   - الحد الأقصى لعدد النسخ الاحتياطية المراد حفظها
5. 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 لاحقًا في أي وقت.
6. انقر على زر **إنهاء**.

   يتم إنشاء المهمة وعرضها في قائمة المهام.

الأداة المساعدة لنسخ البيانات احتياطيًا واستعادتها (klbackup)

يمكنك نسخ بيانات خادم الإدارة للنسخ الاحتياطي واسترجاعها في المستقبل باستخدام أداة klbackup المساعدة التي تعد جزءًا من حزمة توزيع Kaspersky Security Center.

ويمكن تشغيل أداة klbackup المساعدة في وضع من الوضعين التاليين:

- التفاعلي
- غير التفاعلي

النسخ الاحتياطي للبيانات واستعادتها في الوضع التفاعلي

لإنشاء نسخة احتياطية من بيانات خادم الإدارة في الوضع التفاعلي:

1. قم بتشغيل الأداة المساعدة klbackup الموجودة في مجلد تثبيت Kaspersky Security Center (عادةً، /opt/kaspersky/ksc64/sbin/klbackup).

   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 كلمة المرور ومجلد الوجهة للنسخ الاحتياطي ثم انقر على زر **التالي** لبدء النسخ الاحتياطي.

لاستعادة بيانات خادم الإدارة في الوضع التفاعلي:

1. قم بتشغيل الأداة المساعدة klbackup الموجودة في مجلد تثبيت Kaspersky Security Center (عادةً، /opt/kaspersky/ksc64/sbin/klbackup). 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.
   - 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 klbackup التي تحتوي على مجموعة المفاتيح المطلوبة من سطر الأوامر بالجهاز المثبت عليه خادم الإدارة.

بناء جملة سطر الأوامر للأداة المساعدة:

```
klbackup -path BACKUP_PATH [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD] [[-online
```

إذا لم يتم تحديد كلمة مرور في سطر الأوامر بأداة klbackup 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 klbackup المساعدة الأذون 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 بأرشيف بيانات خادم الإدارة. على سبيل المثال، إذا كان مفتاح `-path` 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`—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`—Back up 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 الإدارة وخادم قاعدة البيانات إلى جهاز آخر

إذا كنت بحاجة إلى استخدام خادم الإدارة على جهاز جديد، فيمكنك نقله بإحدى الطرق التالية:

- انقل خادم الإدارة وخادم قاعدة البيانات إلى جهاز جديد.
- احتفظ بخادم قاعدة البيانات على الجهاز السابق وانقل خادم الإدارة فقط إلى جهاز جديد.

لنقل خادم الإدارة وخادم قاعدة البيانات إلى جهاز جديد:

1. على الجهاز السابق، أنشئ نسخة احتياطية من بيانات خادم الإدارة.

   للقيام بذلك، يمكنك تشغيل مهمة النسخ الاحتياطي للبيانات من خلال Kaspersky Security Center 14 Web Console أو تشغيل الأداة المساعدة klbackup.

2. حدد جهازًا جديدًا لتثبيت خادم الإدارة عليه. تأكد من أن الأجهزة والبرامج الموجودة على الجهاز المحدد تفي بمتطلبات خادم الإدارة و Kaspersky Security Center 14 Web Console و Network Agent. تحقق أيضًا من توفر المنافذ المستخدمة في خادم الإدارة.

3. على الجهاز الجديد، قم بتثبيت نظام إدارة قاعدة البيانات (DBMS) الذي سيستخدمه خادم الإدارة.

   عند تحديد DBMS، ضع في اعتبارك عدد الأجهزة التي يغطيها خادم الإدارة.

4. قم بتثبيت خادم الإدارة على الجهاز الجديد.

   لاحظ أنه إذا قمت بنقل خادم قاعدة البيانات إلى الجهاز الجديد ، فحدد العنوان المحلي كعنوان IP للجهاز الذي تم تثبيت قاعدة البيانات عليه (العنصر "h" في تعليمات تثبيت Kaspersky Security Center). إذا كنت بحاجة إلى الاحتفاظ بخادم قاعدة البيانات على الجهاز السابق ، فأدخل عنوان IP للجهاز السابق في العنصر "h" من تعليمات تثبيت Kaspersky Security Center.

5. بعد اكتمال التثبيت، قم باستعادة بيانات خادم الإدارة على الجهاز الجديد باستخدام الأداة المساعدة klbackup.

إذا كنت تستخدم SQL Server كنظام DBMS على الأجهزة السابقة والجديدة، فلاحظ أن إصدار SQL Server المثبت على الجهاز الجديد يجب أن يكون هو نفسه أو أحدث من إصدار SQL Server المثبت على الجهاز السابق. خلاف ذلك، لا يمكنك استعادة بيانات خادم الإدارة على الجهاز الجديد.

6. افتح Kaspersky Security Center 14 Web Console واتصل بخادم الإدارة.

7. تحقق من أن جميع أجهزة العميل متصلة بخادم الإدارة.

8. قم بإلغاء تثبيت خادم الإدارة وخادم قاعدة البيانات من الجهاز السابق.

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).

4. في سطر القائمة، انقر على **خادم إدارة افتراضي جديد**.

5. 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.

6. من قائمة المستخدمين، حدد مسؤول خادم الإدارة الافتراضي. يمكنك، إذا كنت ترغب، أن تقوم بتعديل أحد الحسابات الموجودة بالفعل قبل تخصيص دور المدير له أو إنشاء حساب مستخدم جديد.

7. انقر على **حفظ**.

يتم إنشاء خادم الإدارة الافتراضي الجديد وإضافته إلى مجموعة الإدارة وعرضه في تبويب **خوادم الإدارة**.

إذا كنت متصلاً بخادم الإدارة الأساسي في Kaspersky Security Center 14 Web Console، ولا يمكنك الاتصال بخادم إدارة افتراضي يُدار بواسطة خادم إدارة ثانوي، يمكنك استخدام إحدى الطرق التالية:

- **قم بتعديل تثبيت Kaspersky Security Center 14 Web Console الحالي لإضافة الخادم الثانوي إلى قائمة خوادم الإدارة الموثوقة**. ستتمكن بعد ذلك من الاتصال بخادم الإدارة الافتراضي في Kaspersky Security Center 14 Web Console.

1. على الجهاز الذي تم تثبيت Kaspersky Security Center 14 Web Console عليه، قم بتشغيل ملف تثبيت ksc-web-console-<version number>.<build number>.exe من حساب يتمتع بمزايا إدارية.
2. سيبدأ معالج الإعداد.
3. في الصفحة الأولى من المعالج، حدد خيار **ترقية**.
4. في صفحة **Modification type** ، حدد خيار **تحرير إعدادات الاتصال**.
5. في صفحة **خوادم الإدارة الموثوقة**، أضف خادم الإدارة الثانوي المطلوب.
6. في الصفحة الأخيرة من المعالج، انقر على **تعديل** لتطبيق الإعدادات الجديدة.
7. بعد اكتمال إعادة تكوين التطبيق بنجاح، انقر على زر **إنهاء**.

- استخدم Kaspersky Security Center 14 Web Console للاتصال مباشرة بخادم الإدارة الثانوي حيث تم إنشاء الخادم الإفتراضي. ستتمكن بعد ذلك من تبديل خادم الإدارة الافتراضي في Kaspersky Security Center 14 Web Console.
- استخدم وحدة التحكم الإدارية المستندة إلى MMC للاتصال مباشرة بالخادم الإفتراضي.

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.

في التسلسل الهرمي، لا يمكن أن يعمل خادم إدارة Kaspersky Security Center Linux إلا كخادم ثانوي يُدار بواسطة خادم إدارة أساسي لـ Kaspersky Security Center المستند إلى Windows أو Kaspersky Security Center Cloud Console.

يمكن للتكوين الرئيسي/التابع لاثنين من خوادم الإدارة توفير الخيارات التالية:

- يرث خادم الإدارة الثانوي السياسات والمهام من خادم الإدارة الرئيسي، وهذا يمنع تكرار الإعدادات.
- يمكن أن يشمل تحديد أجهزة على خادم الإدارة الرئيسي أجهزة من خوادم الإدارة الثانوية.
- يمكن أن تحتوي التقارير الموجودة على خادم الإدارة الرئيسي على بيانات (تشمل معلومات تفصيلية) من خوادم الإدارة الثانوية.

إنشاء تسلسل هرمي من خوادم الإدارة: إضافة خادم إدارة تابع

في التسلسل الهرمي، لا يمكن أن يعمل خادم إدارة Kaspersky Security Center Linux إلا كخادم ثانوي يُدار بواسطة خادم إدارة أساسي لـ Kaspersky Security Center المستند إلى Windows أو Kaspersky Security Center Cloud Console.

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، انقر على 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، املأ 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).

إذا تم تحديد هذا الخيار، يبدأ خادم الإدارة الأساسي الاتصال بخادم الإدارة الثانوي. وبخلاف ذلك، يبدأ خادم الإدارة الثانوي الاتصال بخادم الإدارة الأساسي.

- **استخدام الخادم الوكيل**

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". يتم إنشاء الاتصال بين خوادم الإدارة الأولية والثانوية عبر المنفذ 13000. يتم استلام المهام والسياسات من خادم الإدارة الرئيسي وتطبيقها. يتم عرض خادم الإدارة الثانوي على خادم الإدارة الرئيسي في مجموعة الإدارة التي تم إضافته إليها.

إضافة خادم إدارة تابع (يتم هذا على خادم الإدارة الثانوي المستقبلي)

إذا لم تتمكن من التوصيل بخادم الإدارة الثانوي المستقبلي (كأن يكون غير متوفر أو غير متصل مؤقتًا مثلاً)، لا يزال بإمكانك إضافة خادم إدارة تابع.

لإضافة خادم إدارة تابع غير متوفر للتوصيل عبر Kaspersky Security Center 14 Web Console:

1. أرسل ملف الشهادة لخادم الإدارة الأساسي المستقبلي إلى مسؤول النظام في المكتب حيث يوجد خادم الإدارة الثانوي المستقبلي. (يمكنك، على سبيل المثال، كتابة الملف إلى جهاز خارجي مثل ذاكرة البيانات، أو إرساله عبر البريد الإلكتروني.)

   يوجد ملف الشهادة على خادم الإدارة الأساسي المستقبلي على /var/opt/kaspersky/klnagent_srv/1093/cert/.

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 سابقًا 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**.

   g. في حال إجراء الاتصال بخادم الإدارة الثانوي المستقبلي عبر خادم وكيل، حدد خيار **استخدام الخادم الوكيل** وحدد إعدادات الاتصال.

   h. انقر على **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 أيضًا، ولكنها تظهر باللون الرمادي وغير متوفرة في الإدارة في هذه القائمة.

إذا كنت متصلاً بخادم الإدارة الأساسي في Kaspersky Security Center 14 Web Console، ولا يمكنك الاتصال بخادم إدارة افتراضي يُدار بواسطة خادم إدارة ثانوي، يمكنك استخدام إحدى الطرق التالية:

- **قم بتعديل تثبيت Kaspersky Security Center 14 Web Console الحالي لإضافة الخادم الثانوي إلى قائمة خوادم الإدارة الموثوقة**. ستتمكن بعد ذلك من الاتصال بخادم الإدارة الافتراضي في Kaspersky Security Center 14 Web Console.

  1. على الجهاز الذي تم تثبيت Kaspersky Security Center 14 Web Console عليه، قم بتشغيل ملف تثبيت ksc-web-console-<version number>.<build number>.exe من حساب يتمتع بمزايا إدارية.
  2. سيبدأ معالج الإعداد.
  3. في الصفحة الأولى من المعالج، حدد خيار **ترقية**.
  4. في صفحة **Modification type** ، حدد خيار **تحرير إعدادات الاتصال**.
  5. في صفحة **خوادم الإدارة الموثوقة**، أضف خادم الإدارة الثانوي المطلوب.
  6. في الصفحة الأخيرة من المعالج، انقر على **تعديل** لتطبيق الإعدادات الجديدة.
  7. بعد اكتمال إعادة تكوين التطبيق بنجاح، انقر على زر **إنهاء**.

- استخدم Kaspersky Security Center 14 Web Console للاتصال مباشرة بخادم الإدارة الثانوي حيث تم إنشاء الخادم الإفتراضي. ستتمكن بعد ذلك من تبديل خادم الإدارة الافتراضي في Kaspersky Security Center 14 Web Console.

- استخدم وحدة التحكم الإدارية المستندة إلى MMC للاتصال مباشرة بالخادم الإفتراضي.

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. 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 علامة التبويب **حماية المصادقة**.

4. في علامة التبويب **حماية المصادقة**، 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**.

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 أيضًا كيفية تمكين المصادقة الثنائية لحسابك الخاص.

إذا قمت بتمكين المصادقة الثنائية لحسابك، يمكنك المتابعة إلى مرحلة تمكين المصادقة الثنائية لجميع المستخدمين.

المتطلبات الأساسية

قبل ان تبدا:

- تأكد من أن حساب المستخدم الخاص بك يتمتع بحقوق تعديل قوائم التحكم في الوصول للكائن مباشرة من **الميزات العامة: أذونات المستخدم**المجال الوظيفي لتعديل إعدادات الأمان في حسابات 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**

   بعد أن تمكن المصادقة الثنائية لحسابك، يمكنك تمكين المصادقة الثنائية لجميع المستخدمين.

4. **تمكين المصادقة الثنائية لجميع المستخدمين**

   يجب على المستخدمين الذين تم تمكين التحقق المزدوج لهم استخدامه في تسجيل الدخول إلى خادم الإدارة.

5. **تحرير اسم مُصدِر رمز الأمان**

   إذا كان لديك عدة خوادم إدارة بأسماء متماثلة، فقد تضطر إلى تغيير أسماء مُصدري رموز الأمان للتعرف بشكل أفضل على خوادم الإدارة المختلفة.

6. **استثناء حسابات المستخدمين التي لا تحتاج إلى تمكين المصادقة الثنائية لها**

   إذا لزم الأمر، فيمكنك استبعاد المستخدمين من التحقق المزدوج. المستخدمين الذين لديهم حسابات مستثناة لا يتعين عليهم استخدام المصادقة الثنائية لتسجيل الدخول إلى خادم الإدارة.

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 لحساب

يوفر Kaspersky Security Center Linux 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. 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 المُصدر. اسم مُصدر رمز الأمان يُستخدم كمُعرّف لخادم الإدارة في تطبيق المصادقة. يمكنك تغيير اسم مُصدر رمز الأمان. اسم مُصدر رمز الأمان له قيمة افتراضية مماثلة لاسم خادم الإدارة. اسم المُصدر يُستخدم كمُعرّف لخادم الإدارة في تطبيق المصادقة. إذا قمت بتغيير اسم مُصدر رمز الأمان، يجب عليك إصدار مفتاح سري جديد وتمريره 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 مزامنة 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 تمكين 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 لخادم 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 تبدأ في تمكين المصادقة الثنائية لحسابك، تأكد من تثبيت تطبيق المصادقة 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. انتقل إلى **المستخدمون والأدوار** ← **المستخدمون**.
2. انقر على اسم حسابك.
3. في نافذة إعدادات المستخدم التي تفتح، حدد تبويب **حماية الحساب**.
4. في علامة 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 للكائن للمجال الوظيفي **الميزات العامة: أذونات المستخدم** وإذا كان مصرحًا 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 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 فصاعدًا، مستخدمو خادم الإدارة، بما في ذلك المستخدمين الذين تمت إضافتهم بعد تمكين المصادقة الثنائية لجميع المستخدمين، يتعين عليهم تكوين المصادقة الثنائية لحساباتهم، باستثناء المستخدمين الذين تم استثنائهم من المصادقة الثنائية.

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 للكائن مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.

لتعطيل المصادقة الثنائية لحساب مستخدم:

1. 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 للكائن مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**. إذا لم تكن المصادقة الثنائية ممكنة لحسابك، يجب عليك تمكين المصادقة الثنائية لحسابك قبل تعطيلها لجميع المستخدمين.

لتعطيل المصادقة الثنائية لجميع المستخدمين:

1. في 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 مستخدمين من المصادقة الثنائية إذا كان لديك حق تعديل قوائم التحكم في الوصول للكائن مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.

إذا تم استثناء حساب مستخدم من قائمة المصادقة الثنائية لجميع المستخدمين، لن يتعين على هذا المستخدم استخدام المصادقة الثنائية.

استثناء الحسابات من المصادقة الثنائية لجميع المستخدمين قد يكون ضروريًا لحسابات الخدمة التي لا يمكنها تمرير رمز الأمان أثناء المصادقة.

إذا كنت ترغب في استثناء بعض حسابات المستخدمين من المصادقة الثنائية:

1. 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، في جدول استثناءات المصادقة الثنائية، انقر على زر **إضافة**.

3. 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. 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 مُصدِر 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 وتمريره إلى تطبيق المصادقة.

لتحديد اسم جديد لمصدِر 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 مُصدِر رمز الأمان** سيفتح.

4. حدد اسم مُصدِر رمز أمان جديد.

5. انقر على زر **موافق**.

بهذا تم تحديد اسم مُصدر رمز أمان جديد لخادم الإدارة.

تغيير عدد محاولات إدخال كلمة المرور المسموح بها

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

افتراضيًا، يكون الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به هو 10. يمكنك تغيير عدد المحاولات المسموح به لإدخال كلمة مرور، كما هو موضح في هذا القسم.

قم بما يلي لتغيير عدد محاولات إدخال كلمة المرور المسموح بها:

1. شغّل سطر أوامر Linux على جهاز خادم الإدارة.

2. بالنسبة للأداة المساعدة klscflag، شغّل الأمر التالي:

```
sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
```

حيث أن ع عبارة عن عدد من المحاولات لإدخال كلمة مرور.

3. لتطبيق التغييرات، أعد تشغيل خدمة خادم الإدارة.

تم تغيير الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به.

تغيير بيانات اعتماد DBMS

قد تحتاج أحيانًا إلى تغيير بيانات اعتماد DBMS، مثلاً من أجل إجراء تدوير لبيانات الاعتماد لأغراض أمنية.

لتغيير بيانات اعتماد DBMS في بيئة Linux باستخدام الأداة المساعدة klsrvconfig:

1. شغّل سطر أوامر Linux.

2. حدد الأداة المساعدة klsrvconfig في نافذة سطر الأوامر المفتوحة:

```
sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
```

3. حدد اسم حساب جديد. يجب أن تحدد بيانات اعتماد حساب يوجد في DBMS.

4. أدخل كلمة مرور جديدة.

5. حدد كلمة المرور الجديدة للتأكيد.

تم تغيير بيانات اعتماد DBMS.

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 يتم فتحها، 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 على **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.

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 المُستخدمة 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 بتمكين أو تعطيل الخيارات المطلوبة.

4. انقر فوق **حفظ**.

بعد ذلك، تعرض وحدة التحكم أقسامًا في القائمة الرئيسية وفقًا للخيارات الممكنة. على سبيل المثال ، إذا قمت بتمكين **عرض تنبيهات EDR**، فسيظهر قسم المراقبة **المراقبة والإبلاغ** ← **التنبيهات** في القائمة الرئيسية.

اكتشاف الأجهزة المتصلة بالشبكة

يصف هذا القسم البحث عن أجهزة الشبكة واكتشافها.

يتيح لك Kaspersky Security Center العثور على أجهزة بناءً معيار محدد. يمكنك حفظ نتائج البحث في ملف نصي.

تتيح لك ميزة البحث والاكتشاف العثور على الأجهزة التالية:

- الأجهزة المُدارة في مجموعات الإدارة لخادم إدارة Kaspersky Security Center وخوادم الإدارة الثانوية فيه.
- الأجهزة غير المخصصة التي يديرها خادم إدارة Kaspersky Security Center وخوادم الإدارة الثانوية.

سيناريو: اكتشاف الأجهزة المتصلة بالشبكة

يجب عليك إجراء عملية اكتشاف الأجهزة قبل تثبيت تطبيقات الأمان. 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**

   عند إكمال معالج البدء السريع، أجري اكتشاف الجهاز يدويًا.

2. **تكوين الاستقصاءات المستقبلية**

   تأكد من أن استقصاء نطاق IP ذلك ممكن وأن جدول الاستقصاء يلبي احتياجات مؤسستك. عند تكوين جدول الاستقصاء، استخدم التوصيات لتكرار استقصاء الشبكة.

   كما يمكنك أيضًا تمكين استقصاء Zeroconf إذا كانت شبكتك تتضمن أجهزة IPv6.

3. **إعداد القواعد لإضافة الأجهزة المكتشفة إلى مجموعات الإدارة (اختياري)**

   إذا ظهرت أجهزة جديدة على شبكتك، فسيتم اكتشافها أثناء الاستقصاءات المنتظمة وسيتم تضمينها تلقائيًا في المجموعة **الأجهزة غير المخصصة**. إذا أردت، يمكنك إعداد القواعد لنقل هذه الأجهزة تلقائيًا إلى المجموعة **الأجهزة المُدارة**. يمكنك أيضًا إنشاء قواعد الاستبقاء.

   إذا تخطيت مرحلة إعداد هذه القاعدة، فستنتقل 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 Linux الأجهزة الموجودة على الشبكة ويوفر لك معلومات حولها.
- يتم إعداد الاستقصاءات المستقبلية ويتم إجراؤها وفقًا للجدول المحدد.

يتم ترتيب الأجهزة المكتشفة حديثًا وفقًا للقواعد التي تم تكوينها. (أو، إذا لم يكن هناك أي قواعد مكونة، فستبقى الأجهزة في مجموعة **الأجهزة غير المخصصة**).

استقصاء نطاق IP

يحاول Kaspersky Security Center إجراء تحليل اسم عكسي لكل عنوان IPv4 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 حال عدم تكوين هذه المنطقة، لن يظهر استقصاء الشبكة الفرعية لعنوان IP أي نتائج.

في البداية يحصل Kaspersky Security Center على نطاقات IP للاستقصاء من إعدادات الشبكة للجهاز المثبت عليه. إذا كان عنوان الجهاز هو 192.168.0.1 وكان قناع الشبكة الفرعية هو 255.255.255.0، فإن Kaspersky Security Center يدرج الشبكة 192.168.0.0/24 في قائمة عناوين الاستقصاء تلقائيًا. يستقصي Kaspersky Security Center جميع العناوين من 192.168.0.1 إلى 192.168.0.254.

إذا تم تمكين استقصاء نطاق IP فقط، سيكتشف Kaspersky Security Center الأجهزة بعناوين IPv4 فقط. إذا كانت شبكتك تتضمن أجهزة بعناوين IPv6، فقم بتشغيل استقصاء Zeroconf للأجهزة.

عرض وتعديل إعدادات استقصاء نطاق IP

لعرض وتعديل خصائص استقصاء نطاق IP:

1. انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **نطاقات IP**.
2. انقر على زر **خصائص**.

   ستفتح 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 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 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. يستقصي Kaspersky Security Center جميع العناوين من 192.168.0.1 إلى 192.168.0.254. يمكنك تعديل نطاقات IP المعينة تلقائيًا أو إضافة نطاقات IP مخصصة.

يمكنك إنشاء نطاق لعناوين IPv4 فقط. إذا قمت بتمكين استقصاء شبكة لا تتطلب تكوينًا، فسيقوم Kaspersky Security Center باستقصاء الشبكة بالكامل.

لإضافة نطاق IP جديد:

1. 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**

اسم نطاق IP. قد ترغب في تحديد نطاق IP نفسه كاسمه، مثل "192.168.0.0/24".

- **الفاصل الزمني لعنوان IP أو عنوان الشبكة الفرعية والقناع**

عين نطاق IP عن طريق تحديد إما بداية عناوين IP ونهايتها أو عنوان الشبكة الفرعية وقناع الشبكة الفرعية. يمكنك كذلك تحديد أحد نطاقات IP الحالية بالنقر على زر **استعراض**.

- **مدة بقاء عنوان IP (بالساعات)**

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. 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 لـ Kaspersky Security Center استقصاء الشبكات التي تحتوي على أجهزة بعناوين IPv6. في هذه الحالة، لا يتم تحديد نطاقات IP، كما يقوم Kaspersky Security Center باستقصاء الشبكة بالكامل باستخدام شبكة تكوين صفرية (يشار إليها أيضًا باسم Zeroconf). لبدء استخدام Zeroconf، يجب عليك تثبيت أداة استعراض avahi على جهاز Linux الذي يجري استقصاء الشبكات – خادم الإدارة أو نقطة توزيع.

لتمكين استقصاء شبكة لا تتطلب تكوينًا:

1. انتقل إلى **الاكتشاف والنشر** ← **اكتشاف** ← **نطاقات IP**.

2. انقر على زر **خصائص**.

3. في النافذة المفتوحة، شغّل زر استخدام زر تبديل **استخدم شبكة لا تتطلب تكوينًا لاستقصاء شبكات IPv6**.

بعد ذلك، يبدأ Kaspersky Security Center في استقصاء شبكتك. في هذه الحالة، يتم تجاهل نطاقات IP المحددة.

علامات الجهاز

يصف هذا القسم علامات الجهاز ويوفر تعليمات لإنشائها وتعديلها وكذلك لوضع علامات على الأجهزة يدويًا أو تلقائيًا.

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 يدويًا أو تلقائيًا. يمكنك استخدام وضع العلامات يدويًا عندما ترغب في وضع علامة على جهاز محدد. يتم إجراء وضع العلامات التلقائي بواسطة Kaspersky Security Center وفقًا لقواعد وضع العلامات المحددة.

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 تقوم بتعيين علامة `[CentOS]` على جميع الأجهزة التي تعمل بنظام تشغيل CentOS. يمكنك بعد ذلك استخدام هذه العلامة عند إنشاء تحديد جهاز. سيساعدك هذا في فرز جميع أجهزة CentOS وتعيين مهمة لها.

يتم إزالة علامة تلقائيًا من جهاز في الحالات التالية:

- عندما يتوقف الجهاز عن تلبية شروط القاعدة التي تخصص العلامة.
- عندما يتم تعطيل القاعدة التي تخصص العلامة أو حذفها.

قائمة العلامات وقائمة القواعد على كل خادم إدارة مستقلة عن جميع خوادم الإدارة الأخرى، بما في ذلك خادم إدارة أساسي أو خوادم إدارة ظاهرية ثانوية. لا يتم تطبيق القاعدة إلا على الأجهزة التي توجد في خادم الإدارة نفسه الذي تم إنشاء القاعدة عليه.

إنشاء علامة لجهاز

لإنشاء علامة لجهاز:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **العلامات** ← **علامات الجهاز**.
2. انقر على **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 على زر **حذف**.

4. في النافذة التي تفتح، انقر على **نعم**.

سيتم حذف علامة الجهاز. يتم إزالة العلامة المحذوفة بشكل تلقائي من جميع الأجهزة التي تخصيصها إليها.

لا يتم إزالة العلامة التي حذفتها بشكل تلقائي من قواعد وضع العلامات تلقائيًا. بعد حذف العلامة، لا يتم تخصيصها إلى جهاز جديد إلا عندما يفي الجهاز بمتطلبات قاعدة تخصص العلامة.

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 التبويب **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 على **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 حرفًا.
   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 تلقائيًا

لإنشاء قاعدة لوضع علامات على الأجهزة تلقائيًا:

1. اعرض قواعد وضع العلامات على الأجهزة تلقائيًا.

2. انقر على **إضافة**.
ستفتح 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 حرفًا.

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 حرفًا.

4. انقر على زر **إضافة** في قسم الشروط من أجل إضافة شرط جديد.
ستفتح نافذة إعدادات شرط جديد.

5. أدخل اسم الشرط.
يتعذر أن يكون الاسم أكثر من 256 حرفًا. يجب أن يكون الاسم فريدًا داخل القاعدة.

6. قم بإعداد بدء تشغيل القاعدة حسب الشروط التالية. يمكنك تحديد العديد من الشروط.

- **الشبكة**: خصائص الشبكة للجهاز، مثل اسم DNS للجهاز، أو تضمين الجهاز في 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.
- **سجل التطبيقات**—وجود تطبيقات لبائعين 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 لشرط واحد على الأقل.

8. انقر على **حفظ**لحفظ التغييرات.

يتم فرض تطبيق القاعدة التي تم إنشائها حديثًا على الأجهزة المُدارة بواسطة خادم الإدارة المحدد. إذا كانت إعدادات الجهاز مستوفية لشروط القاعدة، يتم تعيين العلامة إلى الجهاز.

يتم تطبيق القاعدة بعد ذلك في الحالات التالية:

- بشكل تلقائي ودوري، حسب حمل العمل على الخادم

- بعد أن تنتهي من تحرير القاعدة
- عندما تبدأ تشغيل القاعدة يدويًا
- بعد أن يكتشف خادم الإدارة تغييرًا في إعدادات جهاز يفي بشروط القاعدة أو إعدادات مجموعة تحتوي على هذا الجهاز

يمكن إنشاء العديد من قواعد وضع العلامات. يمكن تعيين جهاز فردي بالعديد من العلامات إذا قمت بإنشاء العديد من قواعد وضع العلامات وإذا تم استيفاء الشروط الخاصة بهذه القواعد في وقت واحد. يمكنك عرض قائمة بجميع العلامات التي تم تعيينها في خصائص الجهاز.

قواعد التشغيل لوضع العلامات على الأجهزة تلقائيًا

عند تشغيل قاعدة، العلامة المحددة في خصائص هذه القاعدة يتم تخصيصها إلى الأجهزة التي تلبي القواعد المحددة في خصائص القاعدة نفسها. يمكنك لا يمكنك تشغيل إلا القواعد المفعلة.

لتشغيل قواعد وضع العلامات على الأجهزة تلقائيًا:

1. اعرض قواعد وضع العلامات على الأجهزة تلقائيًا.
2. حدد خانات الاختيار الموجودة بجوار القواعد المفعلة التي ترغب في تشغيلها.
3. انقر على زر **تشغيل القاعدة** .

سيتم تشغيل القواعد المحددة.

حذف قاعدة لوضع علامات على الأجهزة تلقائيًا

لحذف قاعدة لوضع علامات على الأجهزة تلقائيًا:

1. اعرض قواعد وضع العلامات على الأجهزة تلقائيًا.
2. حدد خانة الاختيار الموجودة بجوار القاعدة التي ترغب في حذفها.
3. انقر على **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 .

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 Linux 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 وGoogle Chrome وMozilla Firefox. وغيرها).

إنشاء علامة تطبيق

إنشاء علامة تطبيق:

1. في القائمة الرئيسية، انتقل إلى **العمليات** ← **تطبيقات الطرف الثالث** ← **علامات التطبيق**.
2. انقر على **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 **تم تعيين علامة**.

4. بالنسبة للعلامات التي ترغب في تخصيصها، حدد خانات الاختيار في عمود **تم 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 خانات 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 على زر **حذف**.

4. في النافذة التي يتم فتحها، انقر على **موافق**.

سيتم حذف علامة التطبيق. يتم إزالة العلامة المحذوفة بشكل تلقائي من جميع التطبيقات التي تخصيصها إليها.

نشر تطبيقات Kaspersky

يصف هذا القسم تشغيل تطبيقات Kaspersky على أجهزة العميل في مؤسستك من خلال Kaspersky Security Center 14 Web Console.

السيناريو: نشر تطبيقات Kaspersky

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.

يتقدم نشر تطبيقات Kaspersky في مراحل:

1. **تنزيل مكون الإدارة الإضافي للويب للتطبيق**

   نزّل مكون الإدارة الإضافي للويب لتطبيق Kaspersky Endpoint Security for Linux من موقع Kaspersky الإلكتروني ثم أضف المكون الإضافي إلى Kaspersky Security Center 14 Web Console.

2. **تنزيل حزمة التثبيت وإنشائها لعميل الشبكة**

   نزّل حزمة تثبيت عميل الشبكة من موقع Kaspersky الإلكتروني ثم أنشئ حزمة تثبيت عميل الشبكة.

   يمكنك استخدام حزمة التوزيع التي تم تنزيلها لتثبيت عميل الشبكة محليًا. للقيام بذلك، اتبع التعليمات الواردة في وثائق Kaspersky Endpoint Security for Linux .

3. **تنزيل وإنشاء حزمة التثبيت لتطبيق Kaspersky Endpoint Security for Linux**

   نزّل حزمة توزيعة Kaspersky Endpoint Security for Linux من موقع Kaspersky الإلكتروني ثم أنشئ حزمة تثبيت Kaspersky Endpoint Security for Linux.

4. **إنشاء حزم تثبيت مستقلة (اختياري)**

   إذا تعذّر تثبيت تطبيقات Kaspersky عن طريق Kaspersky Security Center Linux على بعض الأجهزة، مثل أجهزة الموظفين البعيدة، فيمكنك إنشاء حزم تثبيت مستقلة للتطبيقات. إذا كنت تستخدم الحزم المستقلة في تثبيت تطبيقات Kaspersky، يمكن تجاهل المرحلتين 5 و6 أدناه.

5. **إنشاء مهمة التثبيت عن بُعد وتكوينها وتشغيلها**

   هذه الخطوة جزء من معالج حماية النشر. 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.

6. **إنشاء المهام وتكوينها**

   يجب تكوين مهمة التحديث لتطبيق Kaspersky Endpoint Security for Linux.

   هذه الخطوة 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 ، فتأكد من أن الجدول الزمني للمهمة يلبي متطلباتك. (بشكل افتراضي ، يتم تعيين البدء المجدول للمهمة **يدويًا**، ولكن قد ترغب في اختيار خيار آخر.)

7. **إنشاء السياسات**

   أنشئ السياسة لـ Kaspersky Endpoint Security for Linux يدويًا أو من خلال معالج البدء السريع. يمكنك استخدام الإعدادات الافتراضية للسياسة، كما يمكنك كذلك تعديل الإعدادات الافتراضية للسياسة وفق احتياجاتك في أي وقت.

8. **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.

إضافة المكونات الإضافية لتطبيقات Kaspersky

لنشر تطبيق Kaspersky مثل Kaspersky Endpoint Security for Linux، يجب أن تضيف مكون الإدارة الإضافي للويب للتطبيق وأن تثبته.

لإضافة وتثبيت مكون الإدارة الإضافي للويب لتطبيق Kaspersky:

1. نزّل مكون الإدارة الإضافي للويب لتطبيق Kaspersky Endpoint Security for Linux من موقع Kaspersky الإلكتروني.
2. افتح Kaspersky Security Center 14 Web Console.
3. في القائمة المنسدلة **إعدادات وحدة التحكم** ، حدد **المكونات الإضافية للويب**.
   سيتم عرض قائمة بالمكونات الإضافية للإدارة المتاحة.
4. انقر على زر زر **إضافة من ملف**.
   سيتم عرض نافذة **إضافة من ملف**.
5. انقر على زر **رفع ملف مضغوط** .
6. حدد الملف المضغوط الذي تم تنزيله من المكون الإضافي للويب.
7. انقر على زر **رفع التوقيع** .
8. حدد الملف النصي TXT الذي تم تنزيله من توقيع المكون الإضافي للويب.
9. انقر على زر **إضافة**.
   Kaspersky Security Center يتحقق من الملفات المرفوعة ثم يضيف المكون الإضافي للويب ويثبته.
10. عندما يكتمل التثبيت، انقر على **موافق**.

يتم تثبيت مكون الإدارة الإضافي للويب بالتكوين الافتراضي ويتم عرضه في قائمة مكونات الإدارة الإضافية للويب.

إنشاء حزم التثبيت من ملف

يمكنك استخدام حزم التثبيت المخصصة للقيام بما يلي:

- لتثبيت أي تطبيق على جهاز عميل (مثل محرر نص)، عن طريق مهمة مثلاً.

- من أجل إنشاء حزمة تثبيت مستقلة.

حزمة التثبيت المخصصة عبارة عن مجلد به مجموعة من الملفات. المصدر لإنشاء حزمة تثبيت مخصصة هو ملف أرشيف. يحتوي ملف الأرشيف على ملف أو ملفات يجب تضمينها في حزمة التثبيت المخصصة.

أثناء إنشاء حزمة تثبيت مخصصة، يمكنك تحديد معلمات سطر الأوامر، مثلاً لتثبيت التطبيق في وضع صامت.

لإنشاء حزمة تثبيت مخصصة:

1. قم بأحد الإجراءات التالية:

- انتقل إلى **الاكتشاف والنشر ← التوزيع والتعيين ← حزم التثبيت** .
- انتقل إلى **العمليات← المستودعات← حزم التثبيت**.

يتم عرض قائمة حزم التثبيت المتوفرة على خادم الإدارة.

2. انقر على **إضافة**.

يبدأ معالج الحزمة الجديدة. انتقل عبر المعالج من خلال استخدام زر **التالي**.

3. في الصفحة الأولى من المعالج ، حدد **قم بإنشاء حزمة تثبيت من ملف**.

4. في الصفحة التالية للمعالج، حدد اسم الحزمة ثم انقر على زر **استعراض**.

5. في النافذة التي يتم فتحها، اختر ملف أرشيف موجود 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).

يبدأ رفع الملف إلى خادم الإدارة.

6. إذا حددت ملفًا لتطبيق Kaspersky، فقد يُطلب منك قراءة اتفاقية ترخيص المستخدم النهائي (EULA) الخاصة بالتطبيق والموافقة عليها. للمتابعة، يجب عليك الموافقة على اتفاقية ترخيص المستخدم النهائي (EULA). حدد خيار **قبول بنود وأحكام اتفاقية ترخيص المستخدم النهائي هذه** فقط إذا كنت قد قرأت شروط اتفاقية ترخيص المستخدم النهائي وفهمتها ووافقت عليها بالكامل.

بالإضافة إلى ذلك، قد يُطلب منك قراءة سياسة الخصوصية والموافقة عليها. للمتابعة، يجب عليك الموافقة على سياسة الخصوصية. حدد خيار **أوافق على سياسة الخصوصية** فقط إذا فهمت ووافقت على أنه سيتم التعامل مع بياناتك ونقلها (يتضمن النقل إلى دول أخرى) كما هو موضح في سياسة الخصوصية.

7. 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.

8. انقر على زر **إنهاء** لإغلاق المعالج.

يتم تنزيل حزمة التثبيت التي قمت بإنشائها إلى مجلد الحزم الفرعي الخاص بـمجلد خادم الإدارة المشترك. بعد التنزيل تظهر حزمة التثبيت 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 الموضوعة 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.
- قم بتغيير معلمات سطر الأوامر.

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 Linux. يمكنك إنشاء حزم تثبيت تطبيقات مستقلة لتطبيقات Kaspersky وتطبيقات الجهات الخارجية. لإنشاء حزمة تثبيت مستقلة لتطبيق جهة ثالثة، يجب عليك إنشاء حزمة تثبيت مخصصة.

تأكد من أن حزمة التثبيت المستقلة غير متاحة لأشخاص آخرين.

لإنشاء حزمة تثبيت مستقلة:

1. قم بأحد الإجراءات التالية:
   - اذهب إلى **الاكتشاف والنشر** ← **التوزيع والتعيين** ← **حزم التثبيت**.
   - 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. يوصى بتمكين هذا الخيار في حالة عدم التأكد من تثبيت وكيل الشبكة على الجهاز من عدمه. إذا كان عميل الشبكة مثبتًا بالفعل على الجهاز، بعد تثبيت حزمة التثبيت المستقلة مع عميل الشبكة، فسيتم 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، على سبيل المثال، إذا كنت 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 جهاز العميل إلى أي مجموعة إدارة بعد تثبيت عميل الشبكة، لا تغير اختيار الخيار.

إذا كنت ترغب في نقل جهاز العميل بعد تثبيت عميل الشبكة، حدد خيار **نقل الأجهزة غير المخصصة إلى هذه المجموعة** ثم حدد مجموعة إدارة ترغب في نقل جهاز 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 يغلق.

يتم إنشاء حزمة التثبيت المستقلة ووضعها في المجلد الفرعي PkgInst الخاص بـمجلد خادم الإدارة المشترك. يمكنك عرض قائمة الحزم المستقلة من خلال النقر على زر **عرض قائمة الحزم المستقلة** أعلى قائمة حزم التثبيت.

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 مذكورة 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**.

تثبيت التطبيقات باستخدام مهمة التثبيت عن بُعد

يسمح لك Kaspersky Security Center Linux 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 DNS وعناوين IP وشبكات IP الفرعية التي ترغب في تعيين المهمة إليها.
- **تعيين مهمة إلى تحديد الجهاز** . في هذه الحالة، يتم تعيين المهمة للأجهزة المضمنة في المجموعة المحددة التي تم إنشائها في وقت سابق. يمكنك تحديد المجموعة المحددة 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.

لتنفيذ التثبيت عن بُعد بشكل صحيح على جهاز لم يتم تثبيت عميل الشبكة عليه، يجب أن تكون المنافذ التالية مفتوحة: أ) TCP 139 و 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

يحتوي هذا القسم على معلومات حول كيفية تثبيت تطبيق عن بُعد على مجموعة إدارة، أو أجهزة ذات عناوين IP محددة، أو مجموعة مختارة من الأجهزة المُدارة.

لتثبيت تطبيق على الأجهزة المحددة:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في الأجهزة ذات الصلة.

2. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

3. انقر على **إضافة**.

يبدأ تشغيل معالج إضافة مهمة.

4. في حقل **نوع المهمة**، حدد **تثبيت التطبيق عن بُعد**.

5. حدد أحد الخيارات التالية:

- **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.

- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**

يمكنك تحديد أسماء 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.

6. اتبع إرشادات المعالج.

ينشئ معالج إضافة مهمة مهمة للتثبيت عن بُعد للتطبيق المحدد في المعالج على أجهزة محددة. إذا حددت الخيار **تعيين مهمة لمجموعة إدارة**، فستكون المهمة مجموعة واحدة.

7. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

عند اكتمال مهمة التثبيت عن بُعد، يتم تثبيت التطبيق المحدد على الأجهزة المحددة.

تثبيت تطبيق من خلال سياسات مجموعة Active Directory

يتيح لك Kaspersky Security Center تثبيت تطبيقات Kaspersky على الأجهزة المدارة باستخدام سياسات مجموعة Active Directory.

يمكنك تثبيت التطبيقات باستخدام سياسات مجموعة Active Directory من خلال حزم التثبيت التي تتضمن عامل الشبكة.

لتثبيت التطبيقات باستخدام سياسات مجموعة Active Directory:

1. قم بتشغيل معالج نشر الحماية. اتبع إرشادات المعالج.

2. في صفحة **إعدادات مهمة التثبيت عن بُعد** الخاصة بمعالج نشر الحماية، قم بتمكين خيار **تعيين تثبيت الحزمة في سياسات مجموعة Active Directory**.

3. في صفحة **حدد حسابات للوصول إلى الأجهزة**، حدد خيار **يُلزم وجود حساب (عميل الشبكة غير مستخدم)**.

4. أضف الحساب الذي يمتلك امتيازات المسؤول على الجهاز المثبت عليه Kaspersky Security Center أو الحساب المضمن مجموعة المجالGroup Policy Creator Owners.

5. منح الأذونات للحساب المحدد:

a. انتقل إلى **لوحة التحكم** ← **الأدوات الإدارية** وافتح **إدارة سياسة المجموعة**.

b. انقر فوق العقدة مع المجال المطلوب.

c. انقر فوق قسم **التفويض**.

d. في القائمة المنسدلة **الإذن**، حدد **ربط عناصر سياسة المجموعة**.

e. انقر فوق **إضافة**.

f. في نافذة **تحديد المستخدم أو الكمبيوتر أو المجموعة** التي تفتح، حدد الحساب المطلوب.

g. انقر فوق **موافق** لإغلاق نافذة **تحديد مستخدم أو كمبيوتر أو مجموعة**.

h. في قائمة **المجموعات والمستخدمين**، حدد الحساب الذي أضفته للتو وانقر فوق **إعدادات متقدمة** ← **إعدادات متقدمة**.

i. في قائمة **إدخالات الأذونات**، انقر نقرًا مزدوجًا فوق الحساب الذي أضفته للتو.

j. امنح الأذونات التالية:

- **إنشاء عناصر المجموعة**
- **حذف عناصر المجموعة**
- **إنشاء كائنات مجموعة حاوية السياسة**
- **حذف كائنات مجموعة حاوية السياسة**

k. انقر فوق **موافق** لحفظ التغييرات.

6. حدد الإعدادات الأخرى باتباع تعليمات المعالج.

7. قم بتشغيل مهمة التثبيت عن بُعد يدويًا أو انتظر حتى تبدأ وفق جدولها.

تبدء سلسلة عمليات التثبيت عن بُعد التالية:

1. عندما تشغيل كل مهمة، يتم إنشاء الكائنات التالية في كل مجال يتضمن أي من الأجهزة العميلة من المجموعة المحددة:

- كائن سياسة المجموعة (GPO) باسم **Kaspersky_AK{GUID}**.
- مجموعة الأمان التي تتوافق مع GPO. تتضمن مجموعة الأمان هذه أجهزة عميلة مغطاة بواسطة المهمة. ويحدد محتوى مجموعة الأمان نطاق GPO.

2. يقوم Kaspersky Security Center بتثبيت تطبيقات Kaspersky المحددة على الأجهزة العميلة مباشرةً من 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 ورابط GPO ومجموعة الأمان المطابقة أيضًا.

إذا أردت تطبيق نظام تثبيت آخر باستخدام Active Directory، يمكنك تكوين الإعدادات المطلوبة يدويًا. على سبيل المثال، قد يكون هذا مطلوبًا في بعض الحالات:

- عندما لا يتمتع مسؤول الحماية ضد الفيروسات بالحقوق اللازمة لإجراء تغييرات على Active Directory لمجالات معينة.
- عندما يجب تخزين حزمة التثبيت الأصلية في مورد شبكة منفصل
- عندما يكون من الضروري ربط GPO بوحدات محددة في Active Directory

تتوفر الخيارات التالية لاستخدام نظام تثبيت بديل من خلال Active Directory:

- إذا كان المطلوب إجراء التثبيت مباشرةً من مجلد Kaspersky Security Center المشترك، ففي خصائص GPO، يجب عليك تحديد ملف .msi الموجود في المجلد الفرعي exec داخل مجلد حزمة التثبيت الخاصة بالتطبيق المطلوب.
- إذا كان يجب وضع حزمة التثبيت في مورد شبكة آخر، يجب عليك نسخ محتوى مجلد exec بالكامل إلى ذلك المورد، لأنه بالإضافة إلى الملف ذي الامتداد .msi، يحتوي المجلد على ملفات التكوين التي تم إنشاؤها عند إنشاء الحزمة. لتثبيت مفتاح الترخيص مع التطبيق، انسخ ملف المفتاح إلى هذا المجلد أيضًا.

تثبيت التطبيقات على خوادم الإدارة الثانوية

لتثبيت تطبيق على خوادم الإدارة الثانوية:

1. قم بتأسيس اتصال مع خادم الإدارة الذي يتحكم في خوادم الإدارة الثانوية ذات الصلة.
2. تأكد من توفر حزمة التثبيت التي تتطابق مع التطبيق الجاري تثبيته على كل خادم من خوادم الإدارة الثانوية المحددة. إذا لم تتمكن من العثور على حزمة التثبيت على أي من الخوادم الثانوية، فقم بتوزيعها. لهذا السبب، قم بإنشاء مهمة باستخدام نوع مهمة **توزيع حزمة التثبيت** .
3. قم بإنشاء مهمة لتثبيت التطبيق عن بعد على خوادم الإدارة الثانوية. حدد نوع المهمة **تثبيت التطبيق على خادم الإدارة الثانوي عن بُعد**.
   ينشئ معالج إضافة مهمة مهمة للتثبيت عن بُعد للتطبيق المحدد في المعالج على خوادم إدارة ثانوية محددة.
4. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

عند اكتمال مهمة التثبيت عن بُعد، يتم تثبيت التطبيق المحدد على خوادم الإدارة الثانوية.

تحديد إعدادات التثبيت عن بُعد على أجهزة Unix

عندما تقوم بتثبيت تطبيق على جهاز Unix باستخدام مهمة تثبيت عن بُعد، يمكنك تحديد إعدادات Unix الخاصة للمهمة. تتوفر هذه الإعدادات في خصائص المهمة بعد إنشاء المهمة.

لتحديد إعدادات Unix الخاصة لمهمة التثبيت عن بُعد:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.
2. انقر على اسم مهمة التثبيت عن بُعد التي ترغب في تحديد إعدادات Unix الخاصة بها.
   ستفتح 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)**

إذا كان لا يمكن استخدام الأمر sudo على الجهاز المستهدف دون تحديد كلمة المرور، حدد هذا الخيار ثم حدد كلمة المرور لحساب الجذر. ينقل Kaspersky Security Center 14 Linux كلمة المرور في نموذج مشفر إلى الجهاز المستهدف، ويفك تشفير كلمة المرور ثم يبدأ إجراء التثبيت نيابةً عن حساب الجذر باستخدام كلمة المرور المحددة.

لا يستخدم Kaspersky Security Center 14 Linux الحساب أو كلمة المرور المحددة لإنشاء اتصال SSH.

- **حدد المسار إلى المجلد المؤقت بأذونات التنفيذ على الجهاز الهدف (للنشر من خلال SSH فقط)**

إذا لم يكن الدليل /tmp على الجهاز المستهدف لديه إذن التنفيذ، حدد هذا الخيار ثم حدد المسار إلى الدليل بإذن التنفيذ. يستخدم Kaspersky Security Center 14 Linux 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.

استبدال تطبيقات الأمان من جهة خارجية

تثبيت تطبيقات الأمان الخاصة بـ Kaspersky عبر Kaspersky Security Center Linux، قد يتطلب 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 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 معالج نشر الحماية. عند تمكين هذا الخيار، يزيل Kaspersky Security Center التطبيقات غير المتوافقة قبل تثبيت تطبيق أمان على جهاز مُدار.

تعليمات المساعدة: إزالة تطبيق غير متوافق 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 المساعدة: إنشاء مهمة

إزالة تحديثات تطبيقات أو برامج عن بُعد

يمكنك إزالة التطبيقات أو تحديثات البرامج على الأجهزة المُدارة التي تعمل بنظام Linux عن بُعد فقط باستخدام عميل الشبكة.

لإزالة تطبيقات أو تحديثات برامج عن بُعد من الأجهزة المحددة:

1. في نافذة التطبيق الرئيسية، اذهب إلى **الأجهزة** ← **المهام**.

2. انقر على **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. 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 خانات الاختيار الموجودة بجوار التطبيقات التي ترغب في إزالتها.

- **إلغاء تثبيت التطبيق من سجل التطبيقات**

افتراضيًا، سترسل عملاء الشبكة إلى خادم الإدارة معلومات عن التطبيقات المثبتة على الأجهزة المُدارة. يتم تخزين قائمة التطبيقات المثبتة في سجل التطبيقات.

لتحديد تطبيق من سجل التطبيقات:

a. انقر على حقل **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 تلقائيًا**

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 تلقائيًا**. إذا تعذر إلغاء التثبيت من خلال الأمر المحدد تلقائيًا، 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 تلقائيًا

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 المُدار بعد إلغاء التثبيت بنجاح، سيتم إعادة تشغيل نظام التشغيل تلقائيًا.

7. حدد كيف ستقوم أجهزة العميل بتنزيل أداة إلغاء التثبيت:

- **استخدام عميل الشبكة**

يتم تسليم الملفات إلى أجهزة العميل بواسطة عميل الشبكة المثبت على أجهزة العميل تلك.

في حال تعطيل هذا الخيار، سيتم تسليم الملفات باستخدام أدوات نظام التشغيل Linux.

ننصح بتفعيل هذا الخيار إذا تم تعيين المهمة إلى الأجهزة المثبت عليها عملاء الشبكة.

- **استخدام موارد نظام التشغيل من خلال خادم الإدارة**

أصبح الخيار قديمًا. استخدم خيار **استخدام عميل الشبكة** أو **استخدام موارد نظام التشغيل عبر نقاط التوزيع** بدلاً من ذلك.

يتم إرسال الملفات إلى الأجهزة العميلة باستخدام أدوات نظام تشغيل خادم الإدارة. يمكنك تفعيل هذا الخيار إذا لم يتم تثبيت عميل شبكة على الجهاز العميل، لكن الجهاز العميل موجود في نفس الشبكة الموجود عليها خادم الإدارة.

- **استخدام موارد نظام التشغيل عبر نقاط التوزيع**

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**

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**

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**

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 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 النظام المطلوب.

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).

- **فرض إغلاق التطبيقات في الجلسات المحظورة**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

9. أضف الحسابات التي سيتم استخدامها لبدء مهمة إلغاء التثبيت عن بُعد إذا كان ذلك ضروريًا:

- **لا يلزم وجود حساب (تم تثبيت عميل الشبكة)**

إذا تم تحديد هذا الخيار، فلا يلزم تحديد الحساب الذي سيتم من خلاله تشغيل مثبت التطبيق. سيتم تشغيل المهمة باستخدام الحساب الذي يتم تشغيل خدمة خادم الإدارة من خلاله.

إذا لم يتم تثبيت كيل الشبكة على الأجهزة العميلة، فلن يتوفر هذا الخيار.

- **يُلزم وجود حساب (عميل الشبكة غير مستخدم)**

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 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 .

14. انقر على زر **حفظ**.

15. قم بتشغيل المهمة يدويًا أو انتظر إلى أن يتم البدء وفقًا للجدول الذي حددته أنت في إعدادات المهمة.

بمجرد إكمال مهمة إلغاء التثبيت عن بُعد، ستتم إزالة التطبيق المحدد من الأجهزة المحددة

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 تثبيت insserv -com
```

يمكّنك هذا من تثبيت حزمة insserv-Compatible وتكوين عميل الشبكة بشكل صحيح.

قم بتشغيل دورة في الدقيقة `insserv- q`-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-Compatible تلقائيًا على جميع الأجهزة الضرورية مرة واحدة. على سبيل المثال، يمكنك استخدام Puppet أو Ansible أو Chef، كما يمكنك إنشاء البرنامج النصي الخاص بك-استخدم أي طريقة مناسبة لك.

بعد تجهيز جهاز SUSE Linux Enterprise Server 15، قم بنشر وتثبيت عميل الشبكة .

تطبيقات Kaspersky: الترخيص والتنشيط

يوضح هذا القسم ميزات Kaspersky Security Center المتعلقة بالتعامل مع مفاتيح الترخيص لتطبيقات Kaspersky المُدارة.

يسمح لك Kaspersky Security Center Linux بإجراء توزيع مركزي لمفاتيح الترخيص الخاصة بتطبيقات Kaspersky على الأجهزة العميلة ومراقبة استخدامها وتجديد تراخيصها.

عند إضافة مفتاح ترخيص باستخدام Kaspersky Security Center، يتم حفظ إعدادات مفتاح الترخيص على خادم الإدارة. وبناءً على هذه المعلومات، يصدر التطبيق تقريرًا حول استخدام مفتاح الترخيص ويقوم بإخطار المسؤول بانتهاء صلاحية الترخيص وانتهاك قيود الترخيص المحددة في خصائص مفاتيح التراخيص. يمكنك تكوين إخطارات استخدام مفاتيح التراخيص في إعدادات خادم الإدارة.

ترخيص التطبيقات المُدارة

يجب إصدار ترخيص لتطبيقات Kaspersky المثبّتة على الأجهزة المُدارة من خلال تطبيق ملف المفتاح أو رمز 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 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 قمت بتمكين الخيار **مفتاح موزع تلقائيًا** لكل مفاتيح التراخيص الثلاثة. تطبيق أمان Kaspersky— على سبيل المثال، تم تثبيت — Kaspersky Endpoint Security for Linux 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:

- 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.

إرشادات الكيفية: إضافة مفتاح ترخيص إلى حزمة التثبيت

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:

- 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 المثبّت محليًا من خلال استخدام الأدوات المتوفرة في واجهة التطبيق. يرجى الرجوع إلى وثائق التطبيق المثبّت.

إضافة مفتاح ترخيص إلى مستودع خادم الإدارة

لإضافة مفتاح ترخيص إلى مستودع خادم الإدارة:

1. في القائمة الرئيسية، انتقل إلى **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 على زر **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 على **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 على زر **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 Linux 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 المفتاح 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 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.

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 المفعل المنشور على جهاز مُدار، سيستمر التطبيق في العمل على الجهاز المُدار.

لحذف ملف مفتاح أو رمز تنشيط من مستودع خادم الإدارة:

1. انتقل إلى **العمليات** ← **الترخيص** ← **تراخيص KASPERSKY** .

2. حدد ملف المفتاح أو رمز التنشيط الذي ترغب في حذفه من المستودع.

3. انقر على زر **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.

لإلغاء EULA لتطبيقات Kaspersky المُدارة:

1. افتح نافذة خصائص خادم الإدارة، ومن تبويب **عام** حدد قسم **اتفاقيات ترخيص المستخدم النهائي** .

يتم عرض قائمة اتفاقيات ترخيص المستخدم النهائي—المقبولة عند إنشاء حزم التثبيت أو عند التثبيت السلس للتحديثات أو عند نشر Kaspersky Security for Mobile.

2. في القائمة، حدد اتفاقية ترخيص المستخدم النهائي التي ترغب في إبطالها.

يمكنك عرض الخصائص التالية لاتفاقية المستخدم النهائي:

- تاريخ قبول اتفاقية المستخدم النهائي
- اسم حساب المستخدم الذي قبل اتفاقية ترخيص المستخدم النهائي

3. انقر على تاريخ قبول أي اتفاقية ترخيص مستخدم نهائي لفتح نافذة خصائصها التي تعرض البيانات التالية:

- اسم حساب المستخدم الذي قبل اتفاقية ترخيص المستخدم النهائي
- تاريخ قبول اتفاقية المستخدم النهائي
- المعرّف الفريد (UID) لاتفاقية ترخيص المستخدم النهائي
- النص الكامل لاتفاقية ترخيص المستخدم النهائي
- قائمة بالكائنات (حزم التثبيت والتحديثات السلسة وتطبيقات الأجهزة المحمولة) المرتبطة باتفاقية ترخيص المستخدم النهائي وأسماء وأنواع كل منها

4. في الجزء الأسفل من نافذة خصائص اتفاقية ترخيص المستخدم النهائي، انقر على زر **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** . ستغلق نافذة خصائص اتفاقية ترخيص المستخدم النهائي، ولن يعد التطبيق مثبتًا.

تجديد تراخيص تطبيقات Kaspersky

يمكنك تجديد ترخيص تطبيق Kaspersky الذي انتهت صلاحيته أو كانت على وشك الانتهاء (في أقل من 30 يومًا).

لتجديد ترخيص منتهي الصلاحية أو على وشك الانتهاء:

1. قم بأحد الإجراءات التالية:

- في القائمة الرئيسية، انتقل إلى **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 وفقًا للجدول التالي:

- 30 أيام قبل انتهاء الصلاحية
- 7 أيام قبل انتهاء الصلاحية
- 3 أيام قبل انتهاء الصلاحية
- 24 ساعة قبل انتهاء الصلاحية
- عندما تنتهي الصلاحية

استخدام Kaspersky Marketplace لاختيار حلول أعمال Kaspersky

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 14 Linux توجيهك إلى صفحة الويب ذات الصلة على موقع Kaspersky الإلكتروني لمعرفة المزيد حول هذا الحل. تتيح لك كل صفحة ويب متابعة عملية الشراء أو تحتوي على إرشادات حول عملية الشراء.

في قسم **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 تلقائيًا.

- **مثالي**

هذا المستوى نموذجي للمؤسسات التي لديها فريق تكنولوجيا معلومات فقط. في هذا المستوى، تحتاج الشركات إلى حلول تمكّنها من مواجهة التهديدات والتهديدات السلعية التي تتحايل على الآليات الوقائية القائمة.

- **خبير**

هذا المستوى نموذجي للمؤسسات التي لديها فريق تكنولوجيا معلومات فقط. إن فريق أمن تكنولوجيا المعلومات ناضج أو أن لدى الشركة فريق SOC (مركز عمليات الأمن). الحلول المطلوبة تمكن الشركات من مواجهة التهديدات المعقدة والهجمات المستهدفة.

- أنواع الأصول التي ترغب في حمايتها.

- **نقاط النهاية**: محطات عمل الموظفين، والآلات المادية والافتراضية، والأنظمة المدمجة
- **الخوادم**: الخوادم المادية والافتراضية
- **السحابة**: البيئات السحابية العامة أو الخاصة أو المختلطة؛ خدمات سحابية
- **الشبكة**: شبكة المنطقة المحلية، والبنية التحتية لتكنولوجيا المعلومات
- **الخدمة**: الخدمات المتعلقة بالأمان التي تقدمها Kaspersky

للعثور على حل أعمال Kaspersky وشرائه:

1. في القائمة الرئيسية، انتقل إلى **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 قِبل المؤسسة. لذلك، نوصي بضبط هذه السياسات والمهام وإنشاء سياسات ومهام أخرى، إذا كانت ضرورية للشبكة لديك.

المتطلبات الأساسية

قبل البدء، تأكد من إجرائك لما يلي:

- خادم إدارة Kaspersky Security Center المُثبت
- تم تثبيت Kaspersky Security Center 14 Web Console
- 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

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.

2. **تكوين المهام للإدارة عن بُعد لتطبيقات Kaspersky**

   تحقق من المهام التي تم إنشاؤها بواسطة معالج البدء السريع وقم بضبطهم إذا لزم الأمر.

   تعليمات الكيفية: إجراء إعداد مهمة جماعية لتحديث Kaspersky Endpoint Security.

   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 الكيفية: تحديد الحد الأقصى لعدد الأحداث .

النتائج

عند إكمال هذا السيناريو، ستتم حماية شبكتك عن طريق تكوين تطبيقات ومهام وأحداث Kaspersky التي يتلقاها خادم الإدارة:

- يتم تكوين تطبيقات Kaspersky وفقًا للسياسات وملفات تعريف السياسة.
- تتم إدارة التطبيقات من خلال مجموعة من المهام.
- يتم تعيين الحد الأقصى لعدد الأحداث التي يمكن تخزينها في قاعدة البيانات.

عند إكمال تكوين حماية الشبكة، يمكنك متابعة تكوين التحديثات المنتظمة للتطبيقات وقواعد بيانات Kaspersky.

حول نُهج إدارة الأمان المرتكزة على الجهاز والمرتكزة على المستخدم

يمكنك إدارة إعدادات الأمان من منطلق مزايا الجهاز ومن منطلق أدوار المستخدم. يُطلق على النهج الأول إدارة الأمان المرتكزة على الجهاز ويُطلق على النهج الثاني إدارة الأمان المرتكزة على المستخدم. لتطبيق إعدادات تطبيق مختلفة على أجهزة مختلفة، يمكنك استخدام أي من نوعي الإدارة أو كليهما معًا.

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.

تمكنك إدارة الأمان المرتكزة على المستخدم من تطبيق إعدادات تطبيق الأمان المختلفة على أدوار المستخدم المختلفة. يمكنك إنشاء عدة أدوار للمستخدم وتعيين دور مستخدم مناسب لكل مستخدم وتحديد إعدادات التطبيق المختلفة للأجهزة التي يملكها المستخدمون ذوي الأدوار المختلفة. على سبيل المثال، قد ترغب في تطبيق إعدادات تطبيق مختلفة على أجهزة المحاسبين والمتخصصين في قسم الموارد البشرية. ونتيجة لذلك، عند تنفيذ إدارة الأمان المرتكزة على المستخدم، فكل قسم من—أقسام الحسابات و الموارد البشرية—لديه تكوين الإعدادات الخاصة به لتطبيقات Kaspersky. يحدد تكوين الإعدادات إعدادات التطبيق التي يمكن تغييرها عن طريق المستخدمين والتي يتم تحديدها وقفلها بالقوة عن طريق المسؤول.

باستخدامك لنهج إدارة الأمان المرتكز على المستخدم يمكنك تطبيق إعدادات التطبيق المحددة للمستخدمين الفرديين. قد يكون هذا مطلوبًا عندما يكون للموظف دورًا فريدًا في الشركة أو عندما تريد مراقبة 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 العميلة في مكتب محلي.

يمكنك أيضًا الجمع بين أساليب إدارة الأمان المرتكزة على الجهاز والمرتكزة على المستخدم. على سبيل المثال: يمكنك تكوين سياسة تطبيق محددة لكل مجموعة إدارة ثم إنشاء ملفات تعريف السياسة لدور مستخدم واحد أو عدة أدوار مستخدم في مؤسستك. في هذه الحالة يتم تطبيق السياسات وملفات تعريف السياسة بالترتيب التالي:

1. يتم تطبيق السياسات التي تم إنشاؤها لإدارة الأمان المرتكزة على الجهاز.
2. يتم تعديلهم بواسطة ملفات تعريف السياسة وفقًا لأولويات ملف تعريف السياسة.
3. يتم تعديل السياسات بواسطة ملفات تعريف السياسة المرتبطة بأدوار المستخدم.

نشر وإعداد السياسة: نهج مرتكز على الجهاز

عند قيامك بإكمال هذا السيناريو، سيتم تكوين التطبيقات على جميع الأجهزة المُدارة وفقًا لسياسات التطبيق وملفات تعريف السياسة التي تحددها.

المتطلبات الأساسية

قبل البدء، تأكد من تثبيت خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console. قد ترغب أيضًا في اعتبار إدارة الأمان المرتكزة على المستخدم كخيار بديل أو إضافي للنهج المرتكز على المستخدم. اعرف المزيد عن نهجي الإدارة.

المراحل

يتكون سيناريو الإدارة المرتكزة على الجهاز لتطبيقات Kaspersky من الخطوات التالية:

1. **تكوين سياسات التطبيق**

   قم بتكوين إعدادات تطبيقات Kaspersky المثبّتة على الأجهزة المُدارة من خلال إنشاء سياسة لكل تطبيق. سيتم نشر مجموعة السياسات إلى الأجهزة العميلة.

   عندما تقوم بتكوين حماية شبكتك في معالج البدء السريع، سينشئ Kaspersky Security Center السياسة الافتراضية لـ Kaspersky Endpoint Security for Linux. إذا قمت باستكمال عملية التكوين باستخدام هذا المعالج، فليس عليك إنشاء سياسة جديدة لهذا التطبيق.

   إذا كانت لديك بنية هرمية للعديد من خوادم الإدارة و/أو مجموعات الإدارة، فإن خوادم الإدارة الثانوية ومجموعات الإدارة الفرعية ترث السياسات من خادم الإدارة الرئيسي بشكلٍ افتراضي. يمكنك فرض الوراثة من خلال المجموعات الفرعية وخوادم الإدارة الثانوية لمنع أي تعديلات في الإعدادات المكونة في سياسة المنبع. إذا كنت تريد فقط أن يتم توريث جزء من الإعدادات بالقوة، فيمكنك قفلها في سياسة المنبع. ستكون بقية الإعدادات غير المقفلة متاحة للتعديل في السياسات التالية. سوف يتيح لك التسلسل الهرمي للسياسات الذي قمت بإنشائه إدارة الأجهزة بفعالية في مجموعات الإدارة.

   تعليمات المساعدة: 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 التي بها تكوين محدد للمكونات، أو تحمل علاماتمحددة. استخدم العلامات لتصفية الأجهزة التي تستوفي معايير محددة. على سبيل المثال، يمكنك إنشاء علامة تسمى CentOS، وتحديد على جميع الأجهزة التي تعمل بنظام تشغيل CentOS 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 CentOS عن طريق ملف تعريف السياسة الخاص بها.

   تعليمات للمساعدة:

   - إنشاء ملف تعريف سياسة
   - إنشاء قاعدة تفعيل ملف تعريف سياسة

3. **نشر السياسات وملفات تعريف السياسة على الأجهزة المدارة**

   بشكلٍ افتراضي، يقوم Kaspersky Security Center تلقائيًا بمزامنة خادم الإدارة مع الأجهزة المُدارة كل 15 دقيقة. وأثناء المزامنة، يتم نشر السياسات وملفات تعريف السياسة الجديدة أو التي تم تغييرها إلى الأجهزة المُدارة. يمكنك تجنب المزامنة التلقائية وتشغيل المزامنة يدويًا باستخدام أمر فرض المزامنة. عند اكتمال المزامنة يتم تسليم السياسات وملفات تعريف السياسة وتطبيقها على تطبيقات Kaspersky المثبتة.

   يمكنك التحقق مما إذا قد تم تسليم السياسات وملفات تعريف السياسة إلى جهاز أم لا. يحدد Kaspersky Security Center تاريخ ووقت التسليم في خصائص الجهاز.

   تعليمات المساعدة: المزامنة المفروضة

النتائج

عند اكتمال السيناريو المرتكز على 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.

المتطلبات الأساسية

قبل البدء، تأكد من نجاح تثبيت خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console وإكمال سيناريو النشر الرئيسي. قد ترغب أيضًا في اعتبار إدارة الأمان المرتكزة على المستخدم كخيار بديل أو إضافي للنهج المرتكز على المستخدم. اعرف المزيد عن نهجي الإدارة.

المعالجة

يتكون سيناريو الإدارة المرتكزة على المستخدم لتطبيقات Kaspersky من الخطوات التالية:

1. **تكوين سياسات التطبيق**

   قم بتكوين إعدادات تطبيقات Kaspersky المثبّتة على الأجهزة المُدارة من خلال إنشاء سياسة لكل تطبيق. سيتم نشر مجموعة السياسات إلى الأجهزة العميلة.

   عندما تقوم بتكوين حماية شبكتك في معالج البدء السريع، سينشئ Kaspersky Security Center السياسة الافتراضية لـ Kaspersky Endpoint Security. إذا قمت باستكمال عملية التكوين باستخدام هذا المعالج، فليس عليك إنشاء سياسة جديدة لهذا التطبيق.

   إذا كانت لديك بنية هرمية للعديد من خوادم الإدارة و/أو مجموعات الإدارة، فإن خوادم الإدارة الثانوية ومجموعات الإدارة الفرعية ترث السياسات من خادم الإدارة الرئيسي بشكلٍ افتراضي. يمكنك فرض الوراثة من خلال المجموعات الفرعية وخوادم الإدارة الثانوية لمنع أي تعديلات في الإعدادات المكونة في سياسة المنبع. إذا كنت إلا ترغب إلا في أن يتم توريث جزء من الإعدادات بالقوة، يمكنك قفلها في سياسة المنبع. ستكون بقية الإعدادات غير المقفلة متاحة للتعديل في السياسات التالية. سوف يتيح لك التسلسل الهرمي للسياسات الذي قمت بإنشائه إدارة الأجهزة بفعالية في مجموعات الإدارة.

   تعليمات المساعدة: إنشاء سياسة

2. **تحديد مالكي الأجهزة**

   قم بتعيين الأجهزة المُدارة إلى المستخدمين المقابلين.

   تعليمات المساعدة: تعيين مستخدم كمالك لجهاز

3. **تعيين أدوار المستخدم القياسية لمؤسستك**

   فكر في الأنواع المختلفة للعمل التي عادةً ما يجريها موظفو مؤسستك. يجب أن تقسم جميع الموظفين وفق أدوارهم. يمكنك على سبيل المثال تقسيمهم بناءً على أقسامهم أو مهنهم أو مناصبهم. ستحتاج بعد ذلك إلى إنشاء دور مستخدم لكل مجموعة. ضع في حسبانك أن كل دور مستخدم سيكون له ملف تعريف السياسة الخاص به ويحتوي على إعدادات التطبيق المحددة لهذا الدور.

4. **إنشاء أدوار المستخدم**

   قم بإنشاء دور مستخدم وتكوينه لكل مجموعة من الموظفين مما قد حددته في الخطوة السابقة أو استخدم أدوار المستخدم المحددة مسبقًا. ستحتوي أدوار المستخدم على مجموعة من حقوق الوصول إلى مزايا التطبيق.

   تعليمات المساعدة: إنشاء دور لمستخدم

5. **تعريف نطاق كل دور مستخدم**

   لكل دور من أدوار المستخدم التي تم إنشاؤها، قم بتحديد المستخدمين و/أو مجموعات الأمان ومجموعات الإدارة. لا تنطبق الإعدادات المرتبطة بدور مستخدم إلا على الأجهزة التي تنتمي إلى المستخدمين الذين يملكون هذا الدور، وفقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

   تعليمات المساعدة: تحرير نطاق دور المستخدم

6. **إنشاء ملفات تعريف السياسة**

إنشاء ملف تعريف سياسة لكل دور مستخدم في مؤسستك. ملفات تعريف السياسة تحدد الإعدادات التي سيتم تطبيقها إلى التطبيقات المثبتة على أجهزة المستخدمين حسب دور كل مستخدم.

تعليمات المساعدة: إنشاء ملف تعريف سياسة

7 **ربط ملفات تعريف السياسة بأدوار المستخدم**

اربط ملفات تعريف إنشاء السياسة التي تم إنشاؤها بأدوار المستخدم. بعد ذلك سيصبح ملفات تعريف السياسة نشطًا لمستخدم له الدور المحدد. سيتم تطبيق الإعدادات في ملفات تعريف السياسة إلى تطبيقات Kaspersky المثبتة على أجهزة المستخدم.

تعليمات المساعدة: ربط ملفات تعريف السياسة بأدوار

8 **نشر السياسات وملفات تعريف السياسة على الأجهزة المدارة**

بشكلٍ افتراضي، يقوم Kaspersky Security Center تلقائيًا بمزامنة خادم الإدارة مع الأجهزة المُدارة كل 15 دقيقة. وأثناء المزامنة، يتم نشر السياسات وملفات تعريف السياسة الجديدة أو التي تم تغييرها إلى الأجهزة المُدارة. يمكنك تجنب المزامنة التلقائية وتشغيل المزامنة يدويًا باستخدام أمر فرض المزامنة. عند اكتمال المزامنة يتم تسليم السياسات وملفات تعريف السياسة وتطبيقها على تطبيقات Kaspersky المثبتة.

يمكنك التحقق مما إذا قد تم تسليم السياسات وملفات تعريف السياسة إلى جهاز أم لا. يحدد Kaspersky Security Center تاريخ ووقت التسليم في خصائص الجهاز.

تعليمات المساعدة: المزامنة المفروضة

النتائج

عند اكتمال السيناريو المرتكز على المستخدم، يتم تكوين تطبيقات Kaspersky وفقًا للإعدادات التي تم تحديدها ونشرها من خلال التسلسل الهرمي السياسات وملفات تعريف السياسة.

بالنسبة لمستخدم جديد، ستحتاج إلى إنشاء حساب جديد والتخصيص للمستخدم أحد أدوار المستخدم التي تم إنشاؤها، وتخصيص الأجهزة إلى المستخدم. سيتم تلقائيًا تطبيق سياسات التطبيق الذي تم تكوينه وملفات تعريف السياسة على أجهزة هذا المستخدم.

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 **استخدم التأخير العشوائي لبدء المهام تلقائيًا** محددة.

إعدادات سياسة عميل الشبكة

لتكوين سياسة عميل الشبكة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **السياسات وملفات التعريف**.
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:

- 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 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 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 وفقًا لمستوى الأهمية في الأقسام التالية في علامة التبويب **تكوين الحدث**:

- **خلل وظيفي**
- **تحذير**
- **معلومات**

في قسم البحث، تعرض القائمة أنواع الأحداث ومدّة تخزين الحدث الافتراضية 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. إلا أنه يمكنك تغيير إعدادات محددة لأنواع الأحداث المطلوبة.

على سبيل المثال ، في **تحذير** يمكنك تكوين **وقع 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 لتثبيت التطبيقات وتنزيل التحديثات عن بُعد). لتكوين **وقع حادث** الحدث، انقر فوقه وحدد مكان تخزين الأحداث التي وقعت وكيفية الإخطار بها.

إذا اكتشف عميل الشبكة حادثًا، فيمكنك إدارة هذا الحادث باستخدام إعدادات جهاز مُدار.

إعدادات التطبيق

إعدادات

في نافذة **الإعدادات**، يمكنك تكوين سياسة عميل الشبكة.

- **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 Linux). 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 افتراضيًا.

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 ممنوعًا في سياسة عميل الشبكة، فلا يمكنك تعديلها.

- **تفاصيل عن التطبيقات التي تم تثبيتها**

إذا تم تمكين هذا الخيار، فسيتم إرسال معلومات التطبيقات المثبتة على أجهزة العميل إلى خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **تفاصيل سجلات الأجهزة**

يقوم عميل الشبكة المثبت على جهاز بإرسال معلومات حول مكونات الجهاز إلى خادم الإدارة. يمكنك عرض تفاصيل المكونات في خصائص الجهاز.

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 أيضًا باسم نبض القلب) إلى 15 دقيقة لكل 10,000 جهاز مُدار.

    إذا تم ضبط الفاصل الزمني للمزامنة على أقل من 15 دقيقة، فسيتم إجراء المزامنة كل 15 دقيقة. إذا تم ضبط الفاصل الزمني للمزامنة على 15 دقيقة أو أكثر، فسيتم إجراء المزامنة في الفاصل الزمني المحدد للمزامنة.

  - **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.

  - **استخدام اتصال SSL**

    في حال تمكين هذا الخيار، يتم إجراء الاتصال بخادم الإدارة من خلال منفذ آمن باستخدام بروتوكول SSL.

    يتم تمكين هذا الخيار افتراضيًا.

  - **استخدم بوابة الاتصال على نقطة التوزيع (إن كانت متاحة) ضمن إعدادات الاتصال الافتراضية**

    إذا تم تمكين هذا الخيار، فسيتم استخدام بوابة الاتصال في نقطة التوزيع بموجب الإعدادات المحددة في خصائص مجموعة الإدارة.

    يتم تمكين هذا الخيار افتراضيًا.

  - **استخدام منفذ UDP**

    إذا 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.

  - **رقم منفذ UDP**

    يمكنك في هذا الحقل إدخال اسم منفذ UDP. رقم المنفذ الافتراضي هو 15000.

    تم استخدام النظام العشري للسجلات.

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 إلا في قسم **ملفات تعريف الاتصال** على الأجهزة التي تعمل بنظام التشغيل Windows:

- **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**

يتم دعم ملفات تعريف الاتصال للأجهزة التي تعمل بنظام Windows فقط. لا نوصي باستخدام هذا الخيار.

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

في مجموعة إعدادات **ملفات تعريف الاتصال**، لا يمكن إضافة أي عناصر جديدة إلى قائمة **ملفات تعريف اتصال خادم الإدارة** بحيث يكون زر **إضافة**غير نشط. لا يمكن تعديل ملفات تعريف الاتصال المحددة مسبقًا أيضًا.

- **تمكين وضع الوجود خارج المكتب عندما يكون خادم الإدارة غير متاح**

في حال تمكين هذا الخيار، وفي حال وجود اتصال عبر ملف التعريف ذلك، ستقوم التطبيقات المثبتة على الجهاز العميل باستخدام ملفات تعريف السياسة للأجهزة التي في وضع الوجود خارج المكتب، بالإضافة إلى سياسات الوجود خارج المكتب. في حالة عدم تحديد سياسة الوجود خارج المكتب للتطبيق، سيتم استخدام السياسة المفعلة.

في حال تعطيل هذا الخيار، ستستخدم التطبيقات السياسات المفعلة.

يتم تعطيل هذا الخيار افتراضيًا.

في القسم الفرعي **جدول الاتصال**، يمكنك تحديد الفواصل الزمنية التي يرسل خلالها عميل الشبكة بيانات إلى خادم الإدارة:

- **الاتصال عند الحاجة**

إذا حددت هذا الخيار، يتم إنشاء الاتصال عندما يتعين على عميل الشبكة إرسال بيانات إلى خادم الإدارة.

يتم تحديد هذا الخيار افتراضيًا.

- **الاتصال في فواصل زمنية محددة**

إذا حددت هذا الخيار، يقوم عميل الشبكة بالاتصال بخادم الإدارة في فترات محددة. ويمكنك إضافة فترات زمنية متعددة للاتصال.

استقصاء الشبكة من خلال نقاط التوزيع

في قسم **استقصاء الشبكة من خلال نقاط التوزيع**، يمكنك تكوين الاستقصاء التلقائي للشبكة. يمكنك استخدام الخيارات التالية لتمكين الاستقصاء وتعيين تردده:

- **شبكة لا تتطلب تكوينًا**

إذا تم تمكين هذا الخيار، فستقوم نقطة التوزيع تلقائيًا باستقصاء الشبكة باستخدام أجهزة IPv6 عن طريق شبكات التكوين الصفري (كما يشار إلى شبكة لا تتطلب تكوينًا). في هذه الحالة، يتم تجاهل استقصاء نطاق IP الذي تم تمكينه، لأن نقطة التوزيع تستقصي الشبكة بالكامل.

لبدء استخدام شبكة لا تتطلب تكوينًا، يجب استيفاء الشروط التالية:

- يجب أن تعمل نقطة التوزيع على نظام Linux.
- يجب عليك تثبيت أداة استعراض avahi على نقطة التوزيع.

إذا تم تعطيل هذا الخيار، فإن نقطة التوزيع لا تستقصي الشبكات مع أجهزة IPv6.

يتم تعطيل هذا الخيار افتراضيًا.

- **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.

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**

إذا تم تمكين هذا الخيار، فلن يتم استخدام خادم الوكيل للاتصال بالأجهزة على الشبكة المحلية.

يتم تعطيل هذا الخيار افتراضيًا.

- **مصادقة الخادم الوكيل**

إذا تم تحديد خانة الاختيار تلك، فيمكنك تحديد بيانات الاعتماد الخاصة بمصادقة الخادم الوكيل في حقول الإدخال.

يتم تعطيل خانة الاختيار هذه بشكل افتراضي.

- **اسم المستخدم**
- **كلمة المرور**

التحديثات (نقاط التوزيع)

في هذا القسم **التحديثات (نقاط التوزيع)** يمكنك تمكي 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.

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 وحدة تحكم Kaspersky Security Center 14 Web 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.

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 DNS كعنوان الجهاز.

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

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

- تعيين تحديد جهاز.

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

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

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

إنشاء مهمة

لإنشاء مهمة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

2. انقر على **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 لاحقًا في أي وقت.

4. انقر على زر **إنهاء**.

يتم إنشاء المهمة وعرضها في قائمة المهام.

بدء مهمة يدويًا

يبدأ التطبيق المهام وفق إعدادات الجدول المحددة في خصائص كل مهمة. يمكنك بدء مهمة يدويًا في أي وقت.

لبدء مهمة يدويًا:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **المهام**.

2. في قائمة المهمة، حدد خانة الاختيار الموجودة بجوار المهمة التي ترغب في بدئها.

3. انقر على زر **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 Linux.

لعرض قائمة المهام،

انتقل إلى **الأجهزة** ← **المهام**.

يتم عرض قائمة المهام. يتم تجميع المهام بأسماء التطبيقات التي ترتبط بها. على سبيل المثال: مهمة تثبيت التطبيق عن بُعد متعلقة بخادم الإدارة، ومهمة تحديث تشير إلى Kaspersky Endpoint Security for Linux.

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 وتحديدها 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).

- **فرض إغلاق التطبيقات في الجلسات المحظورة**

قد تمنع التطبيقات قيد التشغيل إعادة تشغيل الجهاز العميل. على سبيل المثال، إذا تم تحرير ملف في تطبيق معالجة الكلمات ولم يتم حفظه، فلن يسمح التطبيق للجهاز بإجراء إعادة التشغيل.

إذا تم تمكين هذا الخيار، فستُجبر التطبيقات المثبتة على الجهاز المقفول على الإغلاق قبل إعادة تشغيل الجهاز. وكنتيجة لذلك، قد يفقد المستخدمين التغييرات غير المحفوظة التي قاموا بها.

إذا تم تعطيل هذا الخيار، فلن يتم إعادة تشغيل جهاز تم قفله. تشير حالات المهمة على هذا الجهاز إلى أن إعادة تشغيل الجهاز مطلوبة. يجب أن يقوم المستخدمين بإغلاق كافة التطبيقات التي تعمل على الأجهزة المقفولة يدويًا وإعادة تشغيل هذه الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

- إعدادات جدولة المهام:

- **البدء المُجدول**

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **كل N ساعة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالساعات، بداية من الوقت والتاريخ المحددين.

بشكل افتراضي، تعمل المهمة كل 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**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأسابيع، في اليوم المحدد من الأسبوع وفي الوقت المحدد.

بشكل افتراضي، تعمل المهمة كل يوم اثنين، في الوقت الحالي للنظام.

- **كل N دقيقة**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالدقائق، بداية من الوقت المحدد في اليوم الذي تم إنشاء المهمة فيه.

بشكل افتراضي، تعمل المهمة كل 30 دقيقة، بداية من الوقت الحالي للنظام.

- **يوميًا (التوقيت الصيفي غير مدعوم)**

تعمل المهمة بشكل منتظم، حسب الفاصل الزمني المحدد بالأيام. لا يدعم هذا الجدول رصد التوقيت الصيفي (DST). الأمر الذي يعني أنه عند تقديم الساعة أو تأخيرها بمقدار ساعة واحدة في بداية أو نهاية التوقيت الصيفي، فلن يتغير وقت بدء المهمة الفعلي.

لا نوصي باستخدام هذا الجدول. إنه ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center Linux.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 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.

بشكلٍ 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 لمهمة تحديث.

- **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.

- **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** و**مرة** و**فورًا**، 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 المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

- الأجهزة التي سيتم تعيين المهمة إليها:

- **حدد الأجهزة المتصلة بالشبكة التي 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 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 مجموعة الأجهزة المحددة**

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**

املأ حقلي **الحساب** و**كلمة المرور** لتحديد تفاصيل حساب يتم تشغيل المهمة من خلاله. يجب أن يكون للحساب حقوق كافية لهذه المهمة.

- **الحساب**

الحساب الذي يتم تشغيل المهمة من خلاله.

- **كلمة المرور**

كلمة مرور الحساب الذي سيتم تشغيل المهمة من خلاله.

الإعدادات المحددة بعد إنشاء المهمة

يمكنك تحديد الإعدادات التالية بعد إنشاء المهمة فقط.

- إعدادات المهمة الجماعية:

- **التوزيع للمجموعات الفرعية**

هذا الخيار متاح فقط في إعدادات مهام المجموعة.

عند تمكين هذا الخيار، يتضمن نطاق المهمة ما يلي:

- مجموعة الإدارة التي حددتها أثناء إنشاء المهمة.
- مجموعات الإدارة التابعة لمجموعة الإدارة المحددة على أي مستوى لأسفل من خلال التسلسل الهرمي للمجموعة.

عند تعطيل هذا الخيار، فإن نطاق المهمة يتضمن فقط مجموعة الإدارة التي حددتها أثناء إنشاء المهمة.

يتم تمكين هذا الخيار افتراضيًا.

- **توزيع إلى خوادم الإدارة الثانوية والافتراضية**

عند تمكين هذا الخيار، يتم أيضًا تطبيق المهمة الفعالة على خادم الإدارة الأساسي على خوادم الإدارة الثانوية (بما في ذلك الخوادم الافتراضية). إذا كانت هناك مهمة من نفس النوع موجودة بالفعل على خادم الإدارة الثانوي، فسيتم تطبيق كلا المهمتين على خادم الإدارة الثانوي – المهمة الحالية والموروثة من خادم الإدارة الأساسي.

لا يتوفر هذا الخيار إلا عند تمكين خيار **التوزيع للمجموعات الفرعية**.

يتم تعطيل هذا الخيار افتراضيًا.

- إعدادات الجدولة المتقدمة:

- **تفعيل الجهاز قبل بدء المهمة عبر Wake On LAN (بالدقائق)**

يبدأ نظام التشغيل الموجود على الجهاز في الوقت المحدد قبل بدء المهمة. الفترة الزمنية الافتراضية هي خمس دقائق.

قم بتمكين هذا الخيار إذا كنت تريد تشغيل المهمة على جميع الأجهزة العميلة من نطاق المهام، بما في ذلك تلك الأجهزة التي تم إيقاف تشغيلها عندما تكون المهمة على وشك البدء.

إذا كنت تريد إيقاف تشغيل الجهاز تلقائيًا بعد اكتمال المهمة، فقم بتمكين خيار **أغلق الأجهزة بعد الانتهاء من المهمة**. يمكن العثور على هذا الخيار في النافذة نفسها.

يتم تعطيل هذا الخيار افتراضيًا.

- **قم بإيقاف تشغيل الجهاز بعد اكتمال المهمة**

على سبيل المثال، قد ترغب في تمكين هذا الخيار لمهمة تحديث تثبيت والتي تقوم بتثبيت التحديثات على الأجهزة العميلة كل يوم جمعة بعد ساعات العمل، ثم تقوم بإيقاف تشغيل هذه الأجهزة لعطلة نهاية الأسبوع.

يتم تعطيل هذا الخيار افتراضيًا.

- **أوقف المهمة إذا كانت تعمل لمدة أطول من (دقيقة)**

بعد انتهاء الفترة الزمنية المحددة، يتم إيقاف المهمة تلقائيًا، سواء أكانت مكتملة أم لا.

قم بتمكين هذا الخيار إذا كنت تريد مقاطعة (أو إيقاف) المهام التي تستغرق وقتًا طويلاً للتنفيذ.

يتم تعطيل هذا الخيار افتراضيًا. وقت تنفيذ المهمة الافتراضي هو 120 دقيقة.

- إعدادات الإخطار:

- كتلة **تخزين محفوظات المهمة** :

- **تخزين في قاعدة البيانات الخاصة بخادم الإدارة لمدة (بالأيام)**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة على جميع الأجهزة العميلة من نطاق المهام على خادم الإدارة خلال عدد الأيام المحدد. وعند انقضاء هذه الفترة الزمنية، يتم حذف المعلومات من خادم الإدارة.

يتم تمكين هذا الخيار افتراضيًا.

- **تخزين في سجل أحداث نظام التشغيل (OS) على جهاز**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة محليًا في سجل أحداث Syslog لكل جهاز عميل.

يتم تعطيل هذا الخيار افتراضيًا.

- **تخزين في سجل أحداث نظام التشغيل (OS) على خادم إدارة**

يتم تخزين أحداث التطبيق المتعلقة بتنفيذ المهمة على جميع الأجهزة العميلة من نطاق المهام مركزيًا في سجل أحداث Syslog لنظام تشغيل خادم الإدارة (OS).

يتم تعطيل هذا الخيار افتراضيًا.

- **حفظ كل الأحداث**

إذا تم تحديد هذا الخيار، فسيتم حفظ جميع الأحداث المتعلقة بالمهمة في سجلات الأحداث.

- **حفظ الأحداث المتعلقة بتقدم المهمة**

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بتنفيذ المهمة في سجلات الأحداث.

- **حفظ نتائج تنفيذ المهمة فقط**

إذا تم تحديد هذا الخيار، فسيتم حفظ الأحداث المتعلقة فقط بنتائج المهمة في سجلات الأحداث.

- **قم بإخطار المسؤول بنتائج تنفيذ المهمة**

يمكنك تحديد الطرق التي يتلقى بها المسؤولون إخطارات حول نتائج تنفيذ المهام: عن طريق البريد الإلكتروني، والرسائل النصية القصيرة، وعن طريق تشغيل ملف تنفيذي. لتكوين الإخطار، انقر فوق الرابط **إعدادات**.

يتم تعطيل جميع أساليب الإخطارات بصورة افتراضية.

- **إخطار بالأخطاء فقط**

إذا تم تمكين هذا الخيار، فسيتم إخطار المسؤولين فقط عند اكتمال تنفيذ المهمة مع وجود خطأ.

إذا تم تعطيل هذا الخيار، فسيتم إخطار المسؤولين بعد اكتمال تنفيذ كل مهمة.

يتم تمكين هذا الخيار افتراضيًا.

- إعدادات الأمان.
- إعدادات نطاق المهمة.

اعتمادًا على كيفية تحديد نطاق المهام، تكون الإعدادات التالية موجودة:

- **الأجهزة**

إذا تم تحديد نطاق المهمة بواسطة مجموعة إدارة، فيمكنك عرض هذه المجموعة. لا توجد تغييرات متاحة هنا. ومع ذلك، يمكنك إعداد **الاستثناءات من نطاق المهمة**.

إذا تم تحديد نطاق مهمة ما بواسطة قائمة من الأجهزة، فيمكنك تعديل هذه القائمة بإضافة أجهزة وإزالتها.

- **تحديد الجهاز**

يمكنك تغيير تحديد الجهاز الذي يتم تطبيق المهمة عليه.

- **الاستثناءات من نطاق المهمة**

يمكنك تحديد مجموعات الأجهزة التي لا يتم تطبيق المهمة عليها. يمكن أن تكون المجموعات المراد استثنائها مجموعات فرعية فقط من مجموعة الإدارة التي يتم تطبيق المهمة عليها.

- **محفوظات المراجعة**.

بدء معالج تغيير كلمة مرور المهام

بالنسبة إلى مهمة غير محلية، يمكنك تحديد حساب الذي بموجبه يجب تشغيل المهمة. يمكنك تحديد الحساب أثناء إنشاء المهمة أو في خصائص مهمة موجودة. إذا تم استخدام الحساب المحدد وفقًا لتعليمات الأمان للمنظمة، قد تتطلب هذه التعليمات تغيير كلمة مرور الحساب من وقت لآخر. عند انتهاء صلاحية كلمة مرور الحساب وتعيينك لكلمة مرور جديدة، لن تبدأ المهام حتى تحدد كلمة المرور الجديدة الصالحة في خصائص المهمة.

يمكّنك "معالج تغيير كلمة مرور المهام" من استبدال كلمة المرور القديمة تلقائيًا بكلمة مرور جديدة في جميع المهام التي يتم فيها تحديد الحساب. بدلاً من ذلك، يمكنك تغيير كلمة المرور هذه يدويًا في خصائص كل مهمة.

لبدء تشغيل معالج تغيير كلمة مرور المهام:

1. في علامة تبويب **الأجهزة**، حدد **المهام**.
2. انقر على **إدارة بيانات اعتماد الحسابات لبدء المهام** .

اتبع إرشادات المعالج.

الخطوة 1. تحديد أوراق الاعتماد

حدد بيانات اعتماد جديدة صالحة حاليًا في نظامك. عندما تقوم بالتبديل إلى الخطوة التالية من المعالج، يتحقق Kaspersky Security Center ما إذا كان اسم الحساب المحدد مطابقًا لاسم الحساب في خصائص كل مهمة غير المحلية. في حالة تطابق أسماء الحساب، يتم استبدال كلمة المرور في خصائص المهمة تلقائيًا بكلمة المرور الجديدة.

لتحديد الحساب الجديد، حدد خيارًا:

- **استخدام الحساب الحالي**

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 لاتخاذه في الخطوة التالية من المعالج.

الخطوة 2. تحديد إجراء لاتخاذه

إذا لم تحدد كلمة المرور السابقة في الخطوة الأولى من المعالج أو لم تتطابق كلمة المرور القديمة المحددة مع كلمات المرور في خصائص المهمة، يجب عليك اختيار إجراء لاتخاذه للمهام التي تم العثور عليها.

لاختيار إجراء لمهمة:

1. حدد خانة الاختيار الموجودة بجوار المهمة التي ترغب في اتخاذ إجراء لها.
2. اتخذ أحد الإجراءات التالية:
   - لإزالة كلمة المرور في خصائص المهمة، انقر على **حذف بيانات الاعتماد**.
     ستتحول 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**.

عرض نتائج تشغيل المهمة المخزنة على خادم الإدارة

يتيح لك Kaspersky Security Center Linux 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 قسم **عام**.
2. انقر فوق الرابط **النتائج** لفتح النافذة **نتائج المهمة**.

إدارة الأجهزة العميلة

يصف هذا القسم كيفية إدارة الأجهزة في مجموعات الإدارة.

إعدادات جهاز مدار

لعرض إعدادات جهاز مُدار:

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، فسيتصل جهاز العميل فقط بخادم الإدارة لمزامنة البيانات أو نقل المعلومات فقط.

الحد الأقصى لعدد الأجهزة التي تم تحديد خيار **عدم قطع الاتصال عن خادم الإدارة** هو 300.

يتم تعطيل هذا الخيار افتراضيًا على الأجهزة المُدارة. يتم تمكين هذا الخيار افتراضيًا على الجهاز حيث تم تثبيت خادم الإدارة ويظل ممكّنًا حتى إذا حاولت تعطيله.

الشبكة

يعرض قسم **الشبكة** المعلومات التالية عن خصائص الشبكة للجهاز العميل:

- **عنوان IP**

عنوان IP الخاص بالجهاز.

- **مجال Windows**

مجموعة العمل التي تحتوي على الجهاز.

- **اسم DNS**

اسم مجال DNS للجهاز العميل.

- **اسم NetBIOS**

اسم الجهاز 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 أجري 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 الجهاز المحددة من خلال التطبيق

يوفر قسم **حالة الجهاز المحددة من خلال 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 Linux.

التطبيقات

يدرج قسم **التطبيقات** جميع تطبيقات Kaspersky المثبتة على الجهاز العميل: يمكنك النقر على اسم التطبيق لعرض معلومات عامة عن التطبيق وقائمة بالأحداث التي حدث على الجهاز وإعدادات التطبيق.

السياسات النشطة وملفات تعريف السياسة

قسم **السياسات المفعلة وملفات تعريف السياسة** 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** 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.

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**

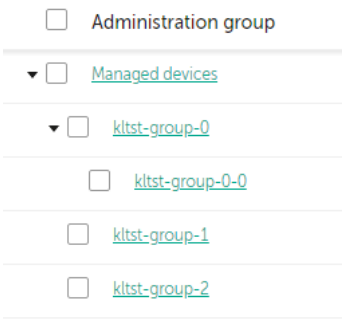
انقر على زر **خصائص** لعرض نقطة التوزيع التي يتفاعل معها الجهاز وتكوينها.

سجل الأجهزة

في القسم **سجل الأجهزة**، يمكنك عرض معلومات عن الأجهزة المثبتة على الجهاز العميل.

إنشاء مجموعات إدارة

فورًا بعد تثبيت Kaspersky Security Center، لا يحتوي الترتيب الهرمي لمجموعات الإدارة إلا على مجموعة إدارة واحدة تسمى **الأجهزة المُدارة**. عند إنشاء ترتيب هرمي لمجموعات الإدارة، يمكنك إضافة أجهزة وأجهزة ظاهرية، إلى مجموعة **الأجهزة المُدارة** وكذلك إضافة المجموعات المتداخلة (انظر الشكل أدناه).



عرض الترتيب الهرمي لمجموعات الإدارة

لإنشاء مجموعة إدارة:

1. 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.

لإنشاء هيكل لمجموعات الإدارة:

1. انتقل إلى **الأجهزة ← التسلسل الهرمي للمجموعات**.

2. انقر على زر **استيراد**.

بدء معالج بنية مجموعة الإدارة الجديدة. اتبع إرشادات المعالج.

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 مسؤولKaspersky Security Center Linux، في قسم **قواعد النقل ←الأجهزة**.

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 Linux (وبخاصةً في مناطق حقوق الوصول والأحداث والتقارير). يجب العثور على حل أخر، على سبيل المثال، من خلال استخدام ملفات تعريف السياسة، والمهام الخاصة بـ تحديدات الأجهزة، وتعيين عملاء الشبكة حسب السيناريو القياسي، وما إلى ذلك.

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 على **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. في علامة تبويب **حالات القاعدة**، حدد معيارًا واحدًا على الأقل يتم من خلاله نقل الأجهزة إلى مجموعة إدارة.

5. انقر على **حفظ**.

يتم إنشاء قاعدة النقل. يتم عرضها في قائمة قواعد النقل. كلما ارتفع المركز في القائمة، زادت أولوية القاعدة. 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 أيضًا تحديد **الاكتشاف والنشر** ← **التوزيع والتعيين**، ثم تحديد **قواعد النقل** في القائمة.
   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**

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. في علامة تبويب **حالات القاعدة**، حدد معيارًا واحدًا على الأقل للأجهزة التي تريد نقلها تلقائيًا.

6. انقر على **حفظ**.

تم إنشاء قاعدة النقل الجديدة. يتم عرضها في قائمة قواعد النقل.

شروط قاعدة نقل الجهاز

عند إنشاء قاعدة أو نسخها لنقل أجهزة العميل إلى مجموعات الإدارة، في علامة التبويب **حالات القاعدة**، يمكنك تعيين الشروط لنقل الأجهزة . لتحديد الأجهزة التي تريد نقلها، يمكنك استخدام المعايير التالية:

- العلامات المخصصة لأجهزة العميل.
- معلمات الشبكة. على سبيل المثال، يمكنك نقل الأجهزة بعناوين IP من نطاق محدد.
- التطبيقات المُدارة المثبتة على أجهزة العميل، على سبيل المثال، عميل الشبكة أو خادم الإدارة.
- الأجهزة الافتراضية، وهي أجهزة العميل.

أدناه، يمكنك العثور على وصف حول كيفية تحديد هذه المعلومات في قاعدة نقل الجهاز.

إذا حددت عدة شروط في القاعدة، فسيعمل عامل التشغيل المنطقي AND وستنطبق جميع الشروط في نفس الوقت. إذا لم تحدد أي خيارات أو احتفظت ببعض الحقول فارغة، فإن هذه الشروط لا تنطبق.

علامة تبويب العلامات

في علامة التبويب هذه، يمكنك تكوين قاعدة نقل الجهاز بناءً على علامات الجهاز التي تمت إضافتها مسبقًا إلى أوصاف أجهزة العميل. للقيام بذلك، حدد العلامات المطلوبة. يمكنك أيضًا تمكين الخيارات التالية:

- **التطبيق على الأجهزة بدون العلامات المحددة**

إذا تم تمكين هذا الخيار، فسيتم استبعاد جميع الأجهزة ذات العلامات المحددة من قاعدة نقل الجهاز. إذا تم تعطيل هذا الخيار، فإن قاعدة نقل الجهاز تنطبق على الأجهزة التي تحتوي على جميع العلامات المحددة.

يتم تعطيل هذا الخيار افتراضيًا.

- **تطبيق في حالة مطابقة علامة محددة واحدة على الأقل**

إذا تم تمكين هذا الخيار، فسيتم تطبيق قاعدة نقل الجهاز على الأجهزة العميلة التي تحتوي على علامة واحدة على الأقل من العلامات المحددة. إذا تم تعطيل هذا الخيار، فإن قاعدة نقل الجهاز تنطبق على الأجهزة التي تحتوي على جميع العلامات المحددة.

يتم تعطيل هذا الخيار افتراضيًا.

علامة تبويب الشبكة

في علامة التبويب هذه، يمكنك تحديد بيانات الشبكة للأجهزة التي تراها قاعدة نقل الجهاز:

- **اسم DNS الخاص بالجهاز**

اسم مجال DNS لجهاز العميل الذي تريد نقله. املأ هذا الحقل إذا كانت شبكتك تتضمن خادم DNS.

- **مجال DNS**

تنطبق قاعدة نقل الجهاز على جميع الأجهزة المضمنة في لاحقة DNS الرئيسية المحددة. املأ هذا الحقل إذا كانت شبكتك تتضمن خادم DNS.

- **نطاق IP**

إذا تم تمكين هذا الخيار، فيمكنك إدخال عناوين IP الأولية والنهائية لنطاق IP الذي يجب تضمين الأجهزة ذات الصلة فيه.

يتم تعطيل هذا الخيار افتراضيًا.

- **عنوان IP للاتصال بخادم الإدارة**

إذا تم تمكين هذا الخيار، يمكنك تعيين عناوين IP التي تتصل بها الأجهزة العميلة بخادم الإدارة. للقيام بذلك، حدد نطاق IP الذي يتضمن جميع عناوين IP الضرورية.

يتم تعطيل هذا الخيار افتراضيًا.

- **تم تغيير ملف تعريف الاتصال**

حدد إحدى القيم التالية:

- **نعم**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي تم تغيير ملف تعريف الاتصال بها.
- **لا**. تنطبق قاعدة نقل الجهاز فقط على أجهزة العميل التي لم يتغير ملف تعريف الاتصال الخاص بها.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

- **تتم إدارته بواسطة خادم إدارة مختلف**

حدد إحدى القيم التالية:

- **نعم**. تنطبق قاعدة نقل الجهاز فقط على أجهزة العميل المُدارة بواسطة خوادم الإدارة الأخرى. تختلف هذه الخوادم عن الخادم الذي تقوم بتكوين قاعدة نقل الجهاز عليه.
- **لا**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي يديرها خادم الإدارة الحالي.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

علامة تبويب التطبيقات

في علامة التبويب هذه، يمكنك تكوين قاعدة نقل الجهاز بناءً على التطبيقات المدارة وأنظمة التشغيل المثبتة على الأجهزة العميلة:

- **تم تثبيت عميل الشبكة**

حدد إحدى القيم التالية:

- **نعم**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي تم تثبيت عميل الشبكة عليها.
- **لا**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة العميلة التي لم يتم تثبيت عميل الشبكة عليها.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

- **التطبيقات**

حدد التطبيقات المُدارة التي يجب تثبيتها على الأجهزة العميلة، لذلك تنطبق قاعدة نقل الجهاز على هذه الأجهزة. على سبيل المثال، يمكنك تحديد **عميل شبكة Kaspersky Security Center 14** أو **خادم إدارة Kaspersky Security Center 14** .

إذا لم تحدد أي تطبيق مُدار، فلن يتم تطبيق الشرط.

- **إصدار نظام التشغيل**

يمكنك استبعاد أجهزة العميل بناءً على إصدار نظام التشغيل. لهذا الغرض، حدد أنظمة التشغيل التي يجب تثبيتها على أجهزة العميل. نتيجة لذلك، يتم تطبيق قاعدة نقل الجهاز على الأجهزة العميلة بأنظمة التشغيل المحددة.

إذا لم تقم بتمكين هذا الخيار، فلن يتم تطبيق الشرط. يتم تعطيل هذا الخيار بشكل افتراضي.

- **حجم نظام التشغيل بالبت**

يمكنك استبعاد أجهزة العميل حسب أحجام بت نظام التشغيل. في حقل **حجم نظام التشغيل بالبت**، يمكنك تحديد إحدى القيم التالية:

- **غير معروف**
- **x86**
- **AMD64**
- **IA64**

للتحقق من حجم بت نظام التشغيل لأجهزة العميل:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← قسم **الأجهزة المُدارة**.
2. انقر على زر **إعدادات الأعمدة** ( ) على اليمين.
3. حدد خيار **حجم نظام التشغيل بالبت**، ثم انقر على زر **حفظ**.

بعد ذلك، يتم عرض حجم بت نظام التشغيل لكل جهاز مُدار.

- **إصدار حزمة خدمة نظام التشغيل**

في هذا الحقل، يمكنك تحديد إصدار حزمة نظام التشغيل (بتنسيق X.Y)، والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز. وبشكل افتراضي، لا يتم تحديد أي قيمة إصدار.

- **شهادة المستخدم**

حدد إحدى القيم التالية:

- **تم التثبيت**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة المحمولة المزودة بشهادة الهاتف المحمول.
- **غير مثبت**. تنطبق قاعدة نقل الجهاز فقط على الأجهزة المحمولة بدون شهادة الهاتف المحمول.
- **لم يتم تحديد قيمة**. الشرط لا ينطبق.

- **إصدار نظام التشغيل**

لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم نسخة مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين قاعدة نقل الجهاز لجميع أرقام النسخة باستثناء الرقم المحدد.

- **رقم إصدار نظام التشغيل**

لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم إصدار مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين قاعدة نقل الجهاز لجميع أرقام الإصدار باستثناء الرقم المحدد.

علامة تبويب الأجهزة الظاهرية

في علامة التبويب هذه، يمكنك تكوين قاعدة نقل الجهاز وفقًا لما إذا كانت أجهزة العميل عبارة عن أجهزة افتراضية أو جزءًا من بنية أساسية لسطح المكتب الافتراضي (VDI):

- **هذا جهاز ظاهري**

يمكنك في القائمة المنسدلة تحديد واحدة مما يلي:

- **N/A**. الشرط لا ينطبق.
- **لا**. نقل الأجهزة التي لا تعد أجهزة ظاهرية.
- **نعم**. نقل الأجهزة التي تعد أجهزة ظاهرية.

- **نوع الجهاز الظاهري**
- **جزء من البنية الأساسية لسطح المكتب الافتراضي**

يمكنك في القائمة المنسدلة تحديد واحدة مما يلي:

- **N/A**. الشرط لا ينطبق.
- **لا**. نقل الأجهزة التي ليست جزءًا من VDI.
- **نعم**. نقل الأجهزة التي تُعد جزءًا من VDI

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. 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 DNS للجهاز.

يجب ألا يحتوي حقل اسم الجهاز على أي حروف خاصة أو backspace أو أي من الحروف 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 أي حروف خاصة أو backspace أو أي من الحروف 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 خانات 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 زر **نقل**.

يتم نقل الأجهزة المحددة إلى مجموعة الإدارة المحددة.

تغيير خادم الإدارة للأجهزة العميلة

يمكنك تغيير خادم الإدارة إلى خادم مختلف لأجهزة العميل المحددة. لهذا الغرض، استخدم مهمة تغيير خادم الإدارة .

لتغيير خادم الإدارة الذي يدير الأجهزة العميلة بخادم آخر:

1. اتصل بخادم الإدارة الذي يتولى إدارة الأجهزة.

2. إنشاء مهمة تغيير خادم الإدارة.

يبدأ تشغيل معالج إضافة مهمة. اتبع إرشادات المعالج. في نافذة **مهمة جديدة** في معالج إضافة مهمة، حدد تطبيق **Kaspersky Security Center 14** ونوع مهمة **تغيير خادم الإدارة** . بعد ذلك ، حدد الأجهزة التي تريد تغيير خادم الإدارة لها:

- **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.

- **تحديد عناوين الجهاز يدويًا أو استيراد العناوين من القائمة**

يمكنك تحديد أسماء 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.

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.

عرض وتكوين الإجراءات عندما تكون حالة الأجهزة غير نشطة

إذا كانت الأجهزة العميلة ضمن مجموعة ما غير نشطة، فبإمكانك الحصول على إشعارات عنها. يمكنك أيضًا حذف مثل هذه الأجهزة تلقائيًا.

لعرض أو تكوين الإجراءات عندما تكون حالة الأجهزة في المجموعة غير نشطة:

1. في القائمة الرئيسية، انتقل إلى **الأجهزة** ← **التسلسل الهرمي للمجموعات**.

2. انقر على اسم مجموعات الإدارة المطلوبة.

ستفتح 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**

سيتم توريث الإعدادات الموجودة في هذا القسم من المجموعة الرئيسية التي تم تضمين الجهاز العميل بها. إذا تم تمكين هذا الخيار، فسيتم قفل الإعدادات الموجودة ضمن **نشاط الجهاز على الشبكة** من إحداث أي تغييرات.

يكون هذا الخيار متاحًا فقط إذا كانت مجموعة الإدارة لديها مجموعة رئيسية.

يتم تمكين هذا الخيار افتراضيًا.

- **فرض توريث الإعدادات في السياسات الفرعية**

سيتم توزيع قيم الإعداد إلى المجموعات الفرعية ولكن في خصائص المجموعات الفرعية يتم قفل هذه الإعدادات.

يتم تعطيل هذا الخيار افتراضيًا.

5. في قسم **نشاط الجهاز**، 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.

6. انقر على **حفظ**.

تم حفظ وتطبيق التغييرات الخاصة بك.

حول حالات الجهاز

يخصص Kaspersky Security Center Linux حالة لكل جهاز مُدار. تعتمد الحالة الخاصة على ما إذا كانت الشروط التي حددها المستخدم قد استوفيت أم لا. في بعض الحالات، عند تعيين حالة لجهازٍ ما، يأخذ Kaspersky Security Center Linux في الاعتبار علامة رؤية الجهاز على الشبكة (انظر الجدول أدناه). إذا لم يعثر Kaspersky Security Center Linux على جهاز على الشبكة في غضون ساعتين، سيتم تعيين علامة رؤية الجهاز إلى غير مرئي.

الحالات كما يلي:

- حرج أو حرج/مرئي
- تحذير أو تحذير/مرئي
- موافق أو موافق/مرئي

يسرد الجدول أدناه الشروط الافتراضية التي يجب استيفائها لتعيين الحالة حرج أو تحذير إلى جهاز، مع جميع القيم المحتملة.

شروط تعيين الحالة إلى الجهاز

الشرط	وصف الشرط	القيم المتوفرة
تطبيق الأمان غير مثبت	عميل الشبكة مثبّت على الجهاز، إلا أن تطبيق الأمان غير مثبّت.	• زر التبديل قيد التشغيل. • زر التبديل متوقف.
تم اكتشاف العديد من الفيروسات	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.	أكثر من 0.
يختلف مستوى الحماية في الوقت الحقيقي عن المستوى الذي تم تعيينه من قِبل المسؤول	الجهاز مرئي على الشبكة، إلا أن مستوى الحماية في الوقت الحقيقي يختلف عن المستوى الذي حدده المسؤول (في الشرط) لحالة الجهاز.	• متوقف. • متوقف مؤقتًا.

• قيد التشغيل.		
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
• زر التبديل متوقف. • زر التبديل قيد التشغيل.	الجهاز مرئي على الشبكة، إلا إن مخزون البرنامج المنفَّذ عبر عميل الشبكة قد اكتشف تطبيقات غير متوافقة مثبتة على الجهاز.	تم تثبيت تطبيقات غير متوافقة
• 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 قريبًا
• 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
• زر التبديل متوقف. • زر التبديل	تم تحديد حالة الجهاز بواسطة التطبيق المدار.	حالة الجهاز المحددة بواسطة التطبيق

		قيد التشغيل.
نفدت مساحة قرص الجهاز	مساحة القرص الشاغرة على الجهاز أقل من القيمة المحددة أو أنه يتعذر مزامنة الجهاز مع خادم الإدارة. يتم تغيير الحالة حرج أو تحذير إلى الحالة جيد عند مزامنة الجهاز بنجاح مع خادم الإدارة وتكون المساحة الفارغة على الجهاز أكبر من أو تساوي القيمة المحددة.	أكثر من 0 ميجابايت
أصبح الجهاز غير مُدار	أثناء اكتشاف الأجهزة، تم التعرف على الجهاز بأنه مرئي على الشبكة، لكن فشلت أكثر من ثلاث محاولات للمزامنة مع خادم الإدارة.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
تم تعطيل الحماية	الجهاز مرئي على الشبكة، إلا إنه قد تم تعطيل تطبيق الأمان على الجهاز لمدة أطول من الفاصل الزمني المحدد.	أكثر من 0 دقائق.
تطبيق الأمان ليس قيد التشغيل	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لا يعمل.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.

يتيح لك Kaspersky Security Center Linux إعداد 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 Linux من الإصدار السابق، فإن قيم شرط **قواعد البيانات قديمة** لتخصيص الحالة تتغير إلى حرجة أو تحذير لا تتغير.

عندما يقوم Kaspersky Security Center Linux 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 لجهازٍ ما.

لتمكين تغيير حالة الجهاز إلى حرجة:

1. افتح نافذة الخصائص من خلال إحدى الطرق التالية:

- في المجلد **السياسات**، في قائمة السياق الخاصة بسياسة خادم إدارة، حدد **خصائص**.
- حدد **خصائص** في قائمة سياق مجموعة الإدارة.

2. في 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.

5. انقر على **موافق**.

عند استيفاء الشروط المحددة، يتم تعيين حالة الجهاز المُدار على تحذير .

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. يكون للسياسة إحدى الحالات التالية:

حالة السياسة

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

تعمل السياسات وفق القواعد التالية:

- يمكن تكوين عدة سياسات بقيم مختلفة لتطبيق واحد.
- يمكن تفعيل سياسة واحدة فقط للتطبيق الحالي.
- يمكن أن يكون للسياسة سياسات فرعية.

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

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

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

تعمل ملفات التعريفية للسياسة وفقًا للقواعد التالية:

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

حول القفل والإعدادات المقفولة

كل إعداد سياسة به رمز زر قفل (🔒). الجدول أدناه يوضح حالات زر القفل:

حالات زر القفل

الحالة	الوصف
Undefined	في حال عرض قفل مفتوح بجوار إعداد وكان زر التبديل معطلاً، هذا الإعداد غير مخصص في السياسة. يمكن لمستخدم أن يغير هذه الإعدادات في واجهة التطبيق المُدار. هذه الأنواع من الإعدادات تسمى غير مقفولة.
Enforce	في حال عرض قفل مقفول بجوار إعداد وكان زر التبديل مفعلاً، هذا الإعداد مطبق على الأجهزة التي تسير السياسة عليها. لا يمكن للمستخدم

	تعديل قيم هذه الإعدادات في واجهة التطبيق المُدار. هذه الأنواع من الإعدادات تسمى مقفولة.

نوصي بشدة بإغلاق الأقفال لإعدادات السياسة التي تريد تطبيقها على الأجهزة المدارة. يمكن إعادة تعيين إعدادات السياسة غير المؤمّنة من خلال إعدادات تطبيق Kaspersky على جهاز مُدار.

يمكنك استخدام زر قفل لإجراء الإجراءات التالية:

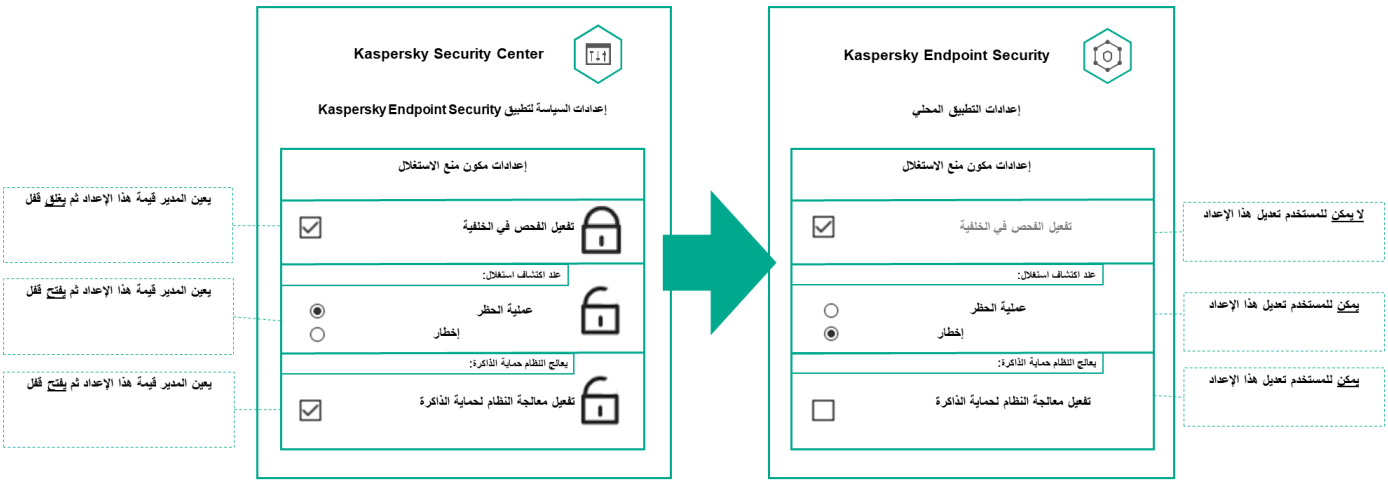
- قفل الإعدادات لسياسة مجموعة إدارة فرعية
- قفل الإعدادات لتطبيق Kaspersky على جهاز مُدار

وبالتالي يتم استخدام إعداد مقفول في تنفيذ الإعدادات الفعالة على جهاز مُدار.

عملية تنفيذ الإعدادات الفعالة تشمل الإجراءات التالية:

- الجهاز المُدار يطبق قيم إعدادات تطبيق Kaspersky.
- الجهاز المُدار يطبق قيم الإعدادات المقفولة لسياسة.

السياسة وتطبيق Kaspersky المحلي يحتويان على نفس مجموعة الإعدادات. عندما تقوم بتكوين إعدادات السياسة، إعدادات تطبيق Kaspersky تغيّر القيم على الجهاز المُدار. لا يمكنك تعديل الإعدادات المقفولة على جهاز مُدار (راجع الشكل أدناه):



الأقفال وإعدادات تطبيق Kaspersky

التسلسل الهرمي للسياسات، واستخدام ملفات تعريف السياسة

يوفّر هذا القسم معلومات عن التسلسل الهرمي للسياسات وملفات تعريف السياسة وتوريثها.

التسلسل الهرمي للسياسات

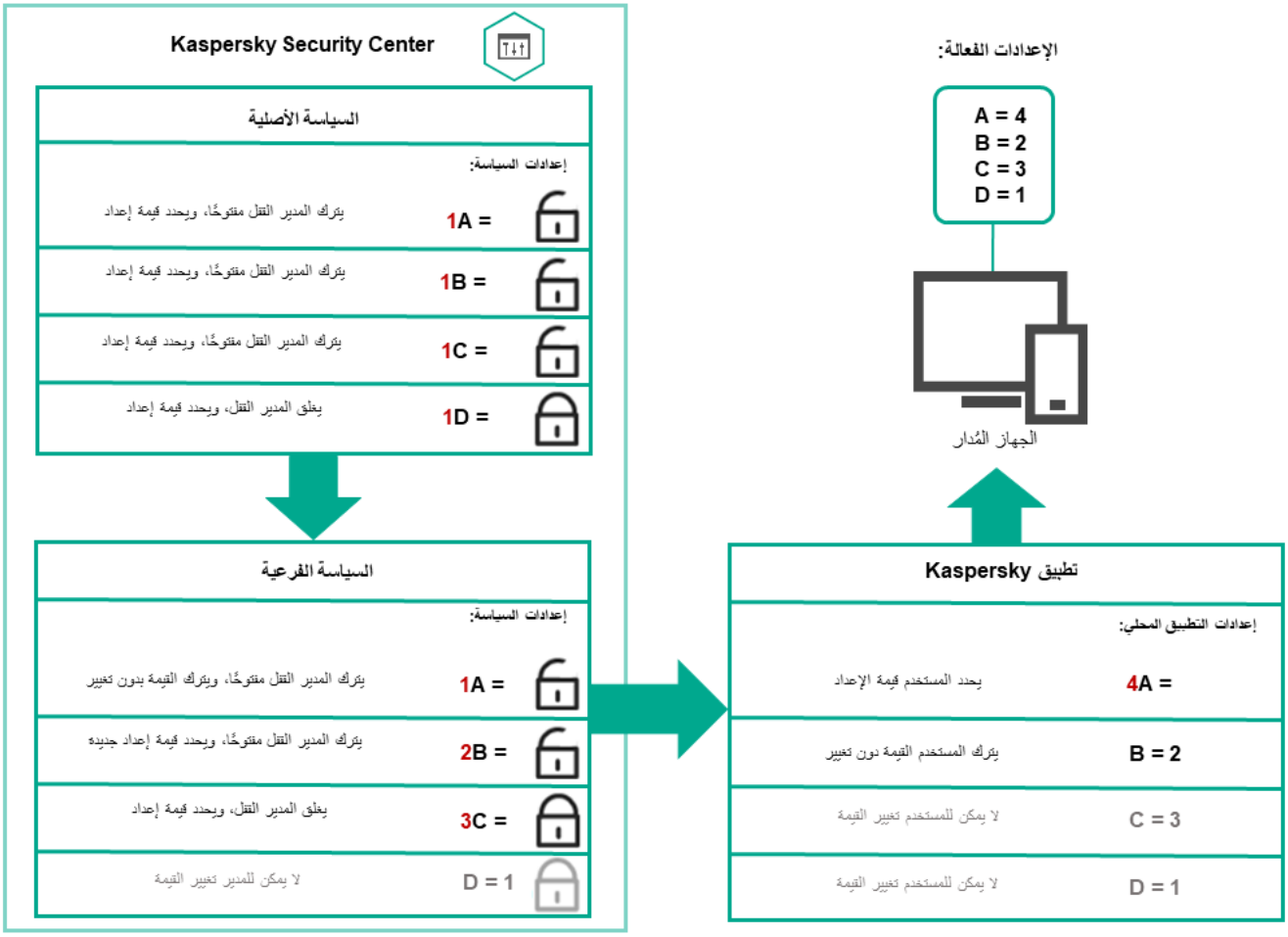
في حال وجود أجهزة مختلفة بحاجة إلى إعدادات مختلفة، يمكنك تنظيم الأجهزة في مجموعات إدارة.

يمكنك تحديد سياسة لمجموعة إدارة واحدة. يمكن أن يتم استيراد إعدادات السياسة. التوريث يعني استقبال قيم إعدادات السياسة في مجموعات فرعية (مجموعات تابعة) من سياسة لمجموعة إدارة من مستوى أعلى (أصلية).

فيما يلي، تتم الإشارة إلى سياسة المجموعة الأصلية أيضًا بالسياسة الأصلية. تتم الإشارة إلى سياسة المجموعة الفرعية (المجموعة التابعة) أيضًا بالسياسة التابعة.

بشكل افتراضي، توجد مجموعة أجهزة مُدارة واحدة على الأقل على خادم الإدارة. إذا كنت ترغب في إنشاء مجموعات مخصصة، يتم إنشاؤها كمجموعات فرعية (مجموعات تابعة) داخل مجموعة الأجهزة المُدارة.

سياسات التطبيق نفسه تتصرف على بعضها وفق تسلسل هرمي لمجموعات الإدارة. الإعدادات المقفولة من سياسة مجموعة إدارة مستوى أعلى (أصلية) سوف تعيد تعيين قيم إعدادات السياسة لمجموعة فرعية (انظر الشكل أدناه).

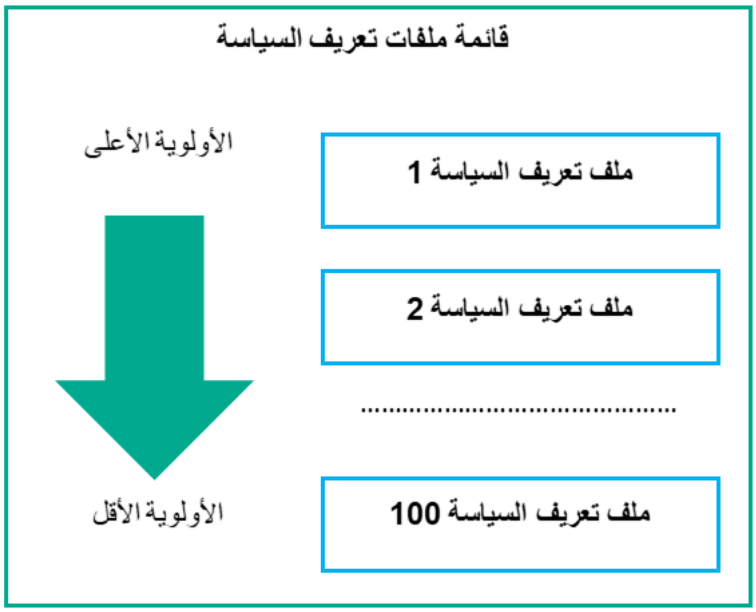


التسلسل الهرمي للسياسات

ملفات تعريف السياسة في التسلسل الهرمي للسياسات

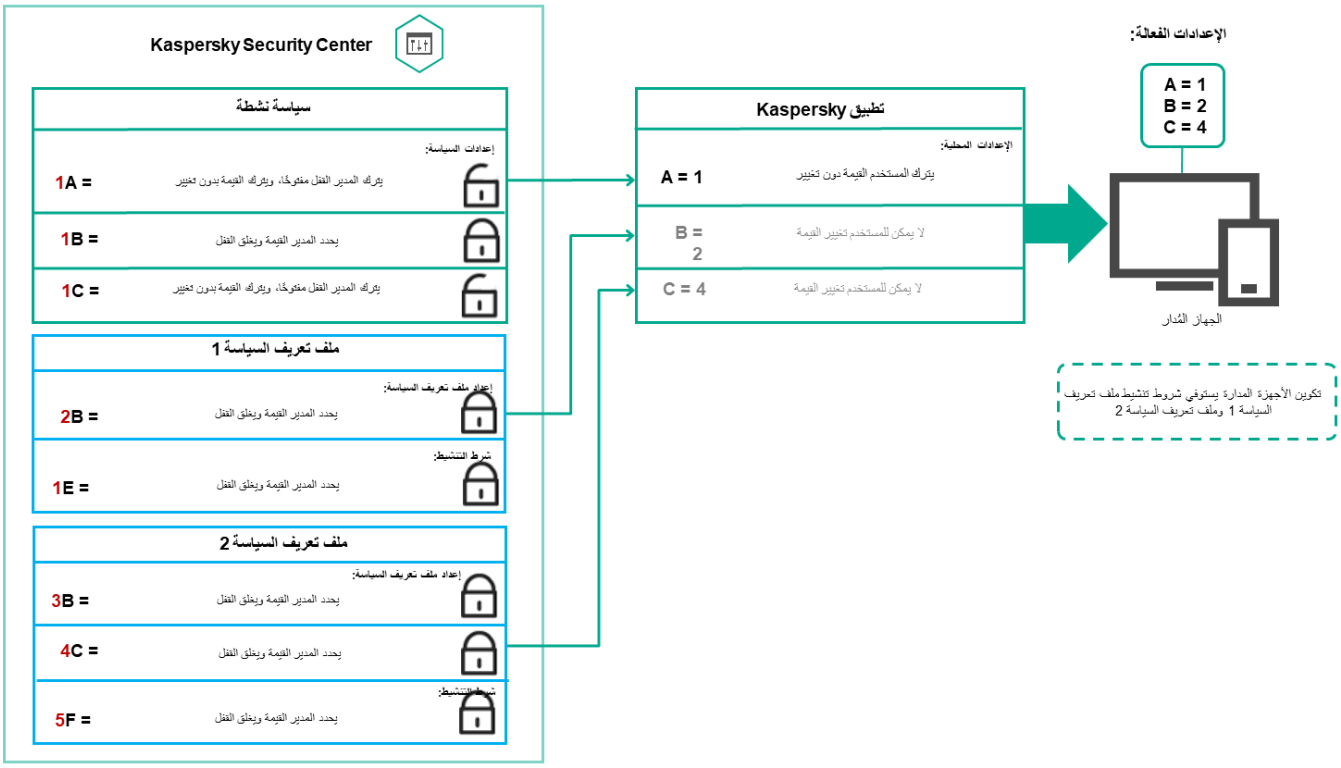
ملفات تعريف السياسة لها شروط تعيين الأولوية التالية:

- وضع الملف في قائمة ملف تعريف السياسة يشير إليه أولويته. يمكنك تغيير أولوية ملف تعريف سياسة. الموضع الأعلى في القائمة يشير إلى الأولوية الأعلى (انظر الشكل أدناه).



تعريف الأولوية لملف تعريف السياسة

- شروط التنشيط لملفات تعريف السياسة لا تعتمد على بعضها. يمكن تنشيط عدة ملفات تعريف سياسة في وقت واحد. في حال وجود عدة ملفات تعريف سياسة تؤثر على الإعداد نفسه، يأخذ الجهاز قيمة الإعداد من ملف تعريف السياسة صاحب أعلى أولوية (انظر الشكل أدناه).

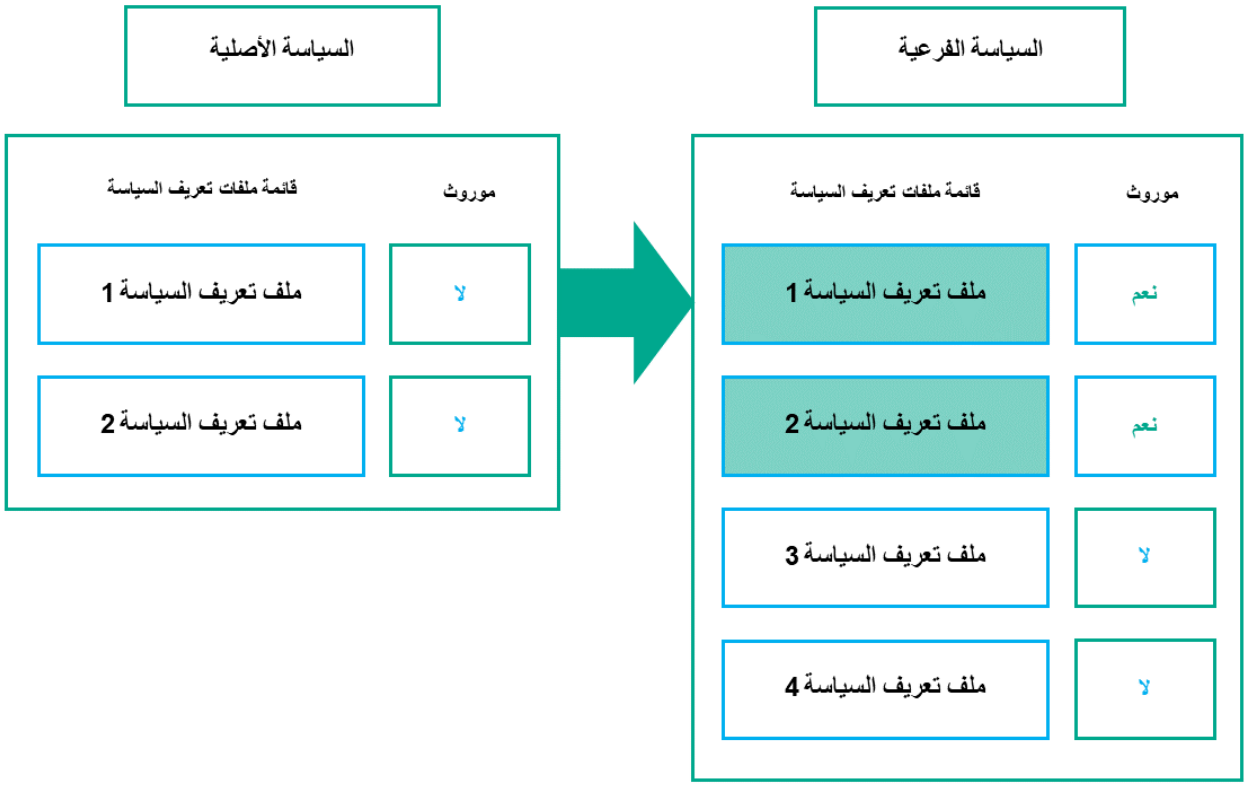


تكوين الجهاز المُدار يفي بشروط التنشيط لعدة ملفات تعريف سياسة

ملفات تعريف السياسة في التسلسل الهرمي للتوريث

ملفات تعريف السياسة من سياسات مستوى تسلسل هرمي مختلف تمتثل بالشروط التالية:

- سياسة المستوى الأقل ترث ملفات تعريف السياسة من سياسة المستوى الأعلى. ملف تعريف السياسة الموروث من سياسة مستوى أعلى يحصل على أولوية أعلى من مستوى ملف تعريف السياسة الأصلي.
- لا يمكنك تغيير أولوية ملف تعريف سياسة موروث (انظر الشكل أدناه).

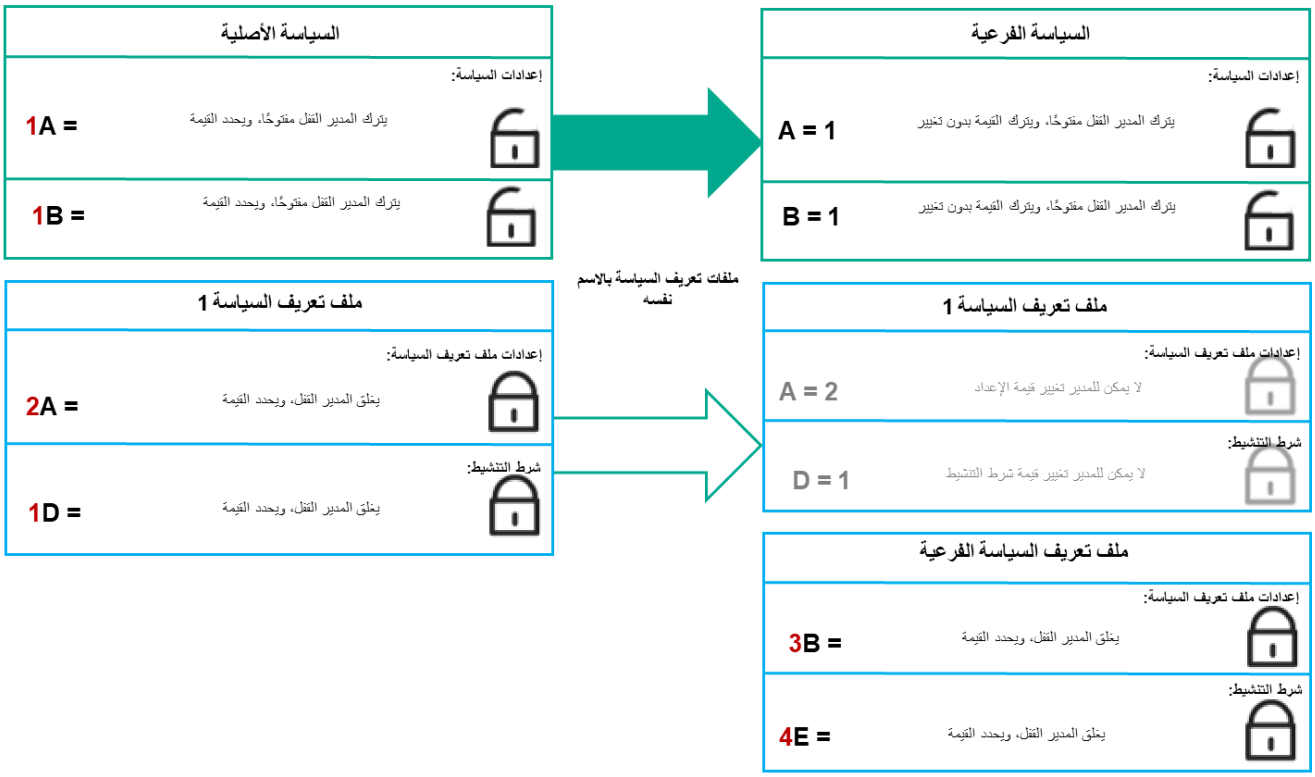


توريث ملفات تعريف السياسة

ملفات تعريف السياسة بالاسم نفسه

في حال وجود سياستين بالاسم نفسه في مستويين مختلفين في التسلسل الهرمي، تعمل هاتان السياساتان وفق القواعد التالية:

- الإعدادات المقفولة وشرط تنشيط ملف التعريف لملف تعريف سياسة مستوى أعلى تغيّر إعدادات وشرط تنشيط ملف التعريف لملف تعريف سياسة مستوى أقل (انظر الشكل أدناه).



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 تغير 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 فارغًا في حال عدم وجود سياسات. يمكنك عرض عواميد الجدول أو إخفائها أو تغيير ترتيبها أو عرض السطور التي تحتوي على قيمة تحددها أو استخدام البحث.

إنشاء سياسة

يمكنك إنشاء سياسات، ويمكنك كذلك تعديل السياسات الموجودة وحذفها.

لإنشاء سياسة:

1. انتقل إلى **الأجهزة** ← **السياسات وملفات التعريف**.

2. انقر على **إضافة**.
تفتح نافذة **تحديد تطبيق**.

3. حدد التطبيق الذي ترغب في إنشاء سياسة له.

4. انقر على **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 لاحقًا.

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
- دعم Kaspersky Endpoint Security for Linux

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.

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 افتراضيًا.

- **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 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

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 ومدّة تخزين الحدث الافتراضية على خادم الإدارة (بالأيام). النقر 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 تبويبي **البريد الإلكتروني**, **رسالة SMS** و**الملف التنفيذي المراد تشغيله**.

سجل المراجعة

تبويب **سجل المراجعة** يتيح لك عرض قائمة بمراجعات السياسة والتراجع عن تغييرات تمت إلى السياسة عند الضرورة.

تعديل سياسة.

لتعديل سياسة:

1. انتقل إلى **الأجهزة**← **السياسات وملفات التعريف**.

2. انقر على السياسة التي ترغب في تعديلها.
ستفتح نافذة إعدادات السياسة.

3. حدد الاعدادات العامة وإعدادات التطبيق الذي تقوم بإنشاء سياسة له. لمزيد من التفاصيل ، يُرجى الرجوع إلى ما يلي:

- تكوين خادم الإدارة
- إعدادات سياسة عميل الشبكة
- دعم Kaspersky Endpoint Security for Linux

لمعرفة تفاصيل عن إعدادات تطبيقات الأمان الأخرى، يمكنك الرجوع إلى وثائق ذلك التطبيق.

4. انقر على **حفظ**.

سيتم حفظ التغييرات التي تم إجراؤها على السياسة في خصائص السياسة، وسيتم عرضها في قسم **سجل المراجعة**.

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 بقفل 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 إذًا 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 افتراضيًا 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 على زر **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 على زر **نسخ**الموجود في الجزء السفلي من 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 حديثًا في المجموعة المستهدفة بالفعل، سيتم الإضافة إلى اسم السياسة المنقولة حديثًا بوضع المؤشر (<رقم التسلسل التالي>) في آخر الاسم، مثل (1).

نقل سياسة

يمكنك نقل السياسات من مجموعة إدارة إلى أخرى. إذا كنت مثلاً ترغب في حذف مجموعة لكنك لا تزال ترغب في استخدام سياساتها في مجموعة أخرى. قد ترغب في هذه الحالة في نقل السياسة من المجموعة القديمة إلى المجموعة الجديدة قبل حذف المجموعة القديمة.

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 زر **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 على زر **نقل**الموجود في الجزء السفلي من الشاشة.

6. انقر على **موافق** لتأكيد العملية.

إذا كانت سياسة غير موروثة 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 موروثة من المجموعة المصدر، سوف تبقى في المجموعة المصدر. سيتم نسخ ها 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 حديثًا في المجموعة المستهدفة بالفعل، سيتم الإضافة إلى اسم السياسة المنقولة حديثًا بوضع المؤشر (<رقم التسلسل التالي>) في آخر الاسم، مثل (1).

المزامنة المفروضة

على الرغم من قيام Kaspersky Security Center Linux بمزامنة الحالة والإعدادات والمهام والسياسات للأجهزة المُدارة تلقائيًا، أحيانًا يجب أن يعلم المدير علم اليقين في لحظة معينة إذا ما قد تمت المزامنة بالفعل على جهاز معين أم لا.

مزامنة جهاز واحد

لفرض المزامنة بين خادم الإدارة وجهاز مُدار:

1. اذهب إلى **الأجهزة** ← **الأجهزة المُدارة**.

2. انقر على اسم الجهاز الذي ترغب في مزامنته مع خادم الإدارة.
   ستفتح 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:
   - انتقل إلى **الأجهزة** ← **الأجهزة المُدارة** ← **المجموعات**، وبعدها حدد مجموعة الإدارة التي تحتوي على أجهزة لمزامنتها.
   - أجر تحديد جهاز لعرض قائمة الجهاز.
2. حدد خانات الاختيار الموجودة بجوار الأجهزة التي ترغب في مزامنتها مع خادم الإدارة.
3. 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. اذهب إلى **الأجهزة** ← **الأجهزة المُدارة**.
2. انقر على اسم الجهاز الذي ترغب في مزامنته مع خادم الإدارة.

   ستفتح نافذة خصائص مع قسم **عام** محدد.
3. حدد تبويب **التطبيقات**.
4. حدد التطبيق الذي ترغب في عرض تاريخ مزامنة السياسة له.

   ستفتح نافذة سياسة التطبيق مع تحديد قسم **عام** وعرض تاريخ ووقت توصيل السياسة.

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. 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. 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 على **حفظ**.
يتم حفظ الإعدادات وتطبيقها.

حذف سياسة

يمكنك حذف سياسة إذا كنت لم تعد بحاجة إليها. لا يمكنك حذف سياسة إلا إذا لم تكن موروثة في مجموعة الإدارة المحددة. إذا كانت سياسة موروثة، لا يمكنك حذفها إلا في مجموعة المستوى الأعلى التي تم إنشاؤها لها.

لحذف سياسة:

1. في القائمة الرئيسية، انتقل إلى **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 موروثة.

3. انقر على **موافق** لتأكيد العملية.

يتم خذف السياسة مع جميع ملفات تعريفها.

إدارة ملفات تعريف السياسة

يصف هذا القسم إدارة ملفات تعريف السياسة ويوفِّر معلومات عن عرض ملفات تعريف سياسة وتغيير أولوية ملف تعريف سياسة وإنشاء ملف تعريف سياسة 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

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 على **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.

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 تحددها.

5. انقر على **نسخ** .

يتم نسخ ملف تعريف السياسة إلى السياسة التي حددتها. يحصل ملف التعريف المنسوخ حديثًا على أقل أولوية. إذا نسخت ملف التعريف إلى السياسة نفسها، سيتم تمديد اسم ملف التعريف المنسوخ حديثًا بإضافة مؤشر (). على سبيل المثال: (1)، (2).

يمكنك لاحقًا تغيير إعدادات ملف التعريف، ويشمل ذلك اسمه وأولويته، لكن لن يتغير ملف تعريف السياسة الأصلي في هذه الحالة.

إنشاء قاعدة تفعيل ملف تعريف سياسة

لإنشاء قاعدة تفعيل ملف تعريف سياسة:

1. تقدم إلى قائمة ملفات تعريف السياسة التي تريدها.
ستظهر قائمة ملفات تعريف السياسة.

2. في تبويب **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 قسم **قواعد التفعيل**، وانقر على زر **إضافة**.
ستفتح نافذة بها قواعد تفعيل ملف تعريف السياسة.

4. حدد اسمًا للقاعدة.

5. حدد خانات الاختيار المجاورة للشروط التي يجب أن تؤثر على تفعيل ملف تعريف السياسة الذي تقوم بإنشائه:

- **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 الانترنت**: 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**

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**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف وتمكينها على الجهاز وفقًا لمالكه. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- الجهاز ينتمي للمالك المحدد (العلامة "=").
- الجهاز لا ينتمي للمالك المحدد (العلامة"#").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد مالك الجهاز عندما يتم تحديد هذا الخيار. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **تم تضمين مالك الجهاز في مجموعة الأمان الداخلية**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة عضوية المالك في مجموعة أمان داخلية خاصة بـ Kaspersky Security Center Linux. 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 Linux. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **قواعد مواصفات الأجهزة**

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**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة حجم ذاكرة الوصول العشوائي على ذلك الجهاز. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- حجم ذاكرة الوصول العشوائي للجهاز أصغر من القيمة المحددة (علامة "<").
- حجم ذاكرة الوصول العشوائي للجهاز أكبر من القيمة المحددة (علامة ">").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد حجم ذاكرة الوصول العشوائي على الجهاز. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **عدد المعالجات المنطقية**

مكّن هذا الخيار لتكوين قاعدة تفعيل ملف التعريف على الجهاز وتمكينها بواسطة عدد المعالجات المنطقية على ذلك الجهاز. في القائمة المنسدلة أسفل خانة الاختيار، يمكنك تحديد معيار لتفعيل ملف التعريف:

- عدد المعالجات المنطقية على الجهاز أقل من أو يساوي القيمة المحددة العلامة ("<").
- عدد المعالجات المنطقية على الجهاز أكبر من أو يساوي القيمة المحددة (العلامة ">").

إذا تم تمكين هذا الخيار، فسيتم تفعيل ملف التعريف على الجهاز وفقًا للمعيار الذي تم تكوينه. يمكنك تحديد عدد المعالجات المنطقية على الجهاز. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق معيار تفعيل ملف التعريف. يتم تعطيل هذا الخيار افتراضيًا.

- **قواعد تعيين الدور**

بالنسبة لهذا الخيار، حدد في الخطوة التالية:

- **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.

- **قواعد استخدام العلامة**

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:

- **قائمة العلامات**

في قائمة العلامات، حدد قاعدة لتضمين الجهاز في ملف تعريف السياسة عن طريق تحديد خانات الاختيار المقابلة للعلامات ذات الصلة.

يمكنك إضافة علامات جديدة إلى القائمة عن طريق إدخالها في الحقل الموجود أعلى القائمة والنقر فوق الزر **إضافة**.

يتضمن الملف التعريفي للسياسة أجهزة بها أوصاف تحتوي جميع العلامات المحددة. إذا تم إلغاء خانات الاختيار، لن يتم تطبيق المعيار. بشكل افتراضي، خانات الاختيار هذه غير محددة.

- **التطبيق على الأجهزة بدون العلامات المحددة**

مكّن هذا الخيار إذا كان يتعين عليك عكس تحديد علاماتك.

في حال تمكين هذا الخيار، سيتضمن ملف تعريف السياسة أجهزة بها أوصاف لا تحتوي على أي من العلامات المحددة. إذا تم تعطيل هذا الخيار، فلن يتم تطبيق المعيار.

يتم تعطيل هذا الخيار افتراضيًا.

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.
ستظهر 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.

يتم حذف ملف تعريف السياسة. إذا ورث السياسة مجموعة مستوى أقل، يبقى ملف التعريف في تلك المجموعة لكنه يصبح الملف الشخصي لسياسة تلك المجموعة. يتم هذا للتخلص من التغيير الكبير في إعدادات التطبيقات المُدارة المثبتة على الأجهزة في مجموعات المستوى الأدنى.

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 حالة تخصيص دور لمستخدم، فسيحصل هذا المستخدم على إعدادات الأمان الضرورية لتأدية المهام الوظيفية.

يمكن ربط دور المستخدم بمستخدمي الأجهزة في مجموعة إدارة محددة.

نطاقات دور المستخدم

نطاق دور المستخدم هو مجموعة من المستخدمين ومجموعات الإدارة. لا تنطبق الإعدادات المرتبطة بدور مستخدم إلا على الأجهزة التي تنتمي إلى المستخدمين الذين يملكون هذا الدور، وفقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

فائدة استخدام الأدوار

فائدة استخدام الأدوار هي أنك لن تضطر إلى تحديد إعدادات الأمان لكل جهاز من الأجهزة المُدارة أو لكل مستخدم من المستخدمين على حدة. عدد المستخدمين والأجهزة في الشركة قد يكون كبيرًا، لكن عدد المهام الوظيفية المختلفة التي تتطلب إعدادات أمان مختلفة أقل بدرجة كبيرة.

الاختلافات عن استخدام ملفات تعريف السياسة

ملفات تعريف السياسة من خصائص السياسة التي تم إنشاؤها لكل تطبيق من تطبيقات Kaspersky على حدة. يرتبط الدور بالعديد من ملفات تعريف السياسة التي تم إنشاؤها لتطبيقات مختلفة. وبالتالي الدور هو وسيلة لتوحيد الإعدادات لكل نوع مستخدم معين في مكان واحد.

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

يوفر Kaspersky Security Center Linux تسهيلات للوصول إلى ميزات Kaspersky Security Center Linux أو تطبيقات Kaspersky المُدارة.

يمكنك تكوين حقوق الوصول إلى ميزات التطبيق لمستخدمي Kaspersky Security Center Linux بإحدى الطرق التالية:

- عن طريق تكوين الحقوق لكل مستخدم أو مجموعة من المستخدمين بشكل فردي.
- عن طريق إنشاء أدوار المستخدم القياسية مع مجموعة محددة مسبقًا من الحقوق وتعيين هذه الأدوار للمستخدمين اعتمادًا على مدى نطاق واجباتهم.

يهدف تطبيق أدوار المستخدم إلى تبسيط وتقصير الإجراءات الروتينية لتكوين حقوق وصول المستخدمين إلى ميزات التطبيق. يتم تكوين حقوق الوصول ضمن دور ما وفقًا للمهام القياسية ونطاق واجبات المستخدمين.

يمكن تعيين أسماء لأدوار المستخدمين وفقًا لأغراض كل منها. يمكنك إنشاء عدد غير محدود من الأدوار في التطبيق.

يمكنك استخدام أدوار المستخدم المحددة مسبقًا مع مجموعة الحقوق المكونة بالفعل، أو إنشاء أدوار جديدةوتكوين الحقوق المطلوبة بنفسك.

حقوق الوصول إلى ميزات التطبيق

يوضح الجدول أدناه ميزات Kaspersky Security Center Linux 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**	• إضافة جهاز إلى مجموعة الإدارة: **قم بالتعديل**	لا شيء	لا شيء	لا شيء

		• 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**			
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	• **قراءة** • **تعديل** • **تنفيذ** • **إجراء عمليات على تحديدات الجهاز**	• 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**	• "تنزيل التحديثات إلى مستودع خادم الإدارة" • "تسليم التقارير" • "توزيع حزم التثبيت" • "تثبيت التطبيق عن بُعد على خوادم الإدارة الثانوية"	• "تقرير حالة الحماية" • "تقرير التهديدات" • "تقرير حول الأجهزة الأكثر إصابة" • "تقرير حول حالة قواعد بيانات مكافحة الفيروسات" • "تقرير الأخطاء" • "الإبلاغ عن هجمات الشبكة" • "تقرير موجز عن تطبيقات الدفاع المحيطي المثبتة" • "تقرير موجز عن التطبيقات المثبتة" • "تقرير حول مستخدمي الأجهزة المصابة" • "تقرير حول الحوادث" • "تقرير حول الأحداث"	لا شيء

				• "تقرير حول نشاط نقاط التوزيع" • "تقرير حول خوادم الإدارة الثانوية" • "تقرير حول أحداث التحكم في الجهاز" • "تقرير حول التطبيقات المحظورة" • "تقرير حول التحكم في الويب" • "تقرير حول أذونات المستخدم الفعالة" • "تقرير حول الحقوق"	
الميزات العامة: الكائنات المحذوفة	• **قراءة** • **تعديل**	• اعرض الكائنات المحذوفة في سلة المحذوفات: **اقرأ** • حذف كائنات من سلة المحذوفات: **قم بالتعديل**	لا شيء	لا شيء	لا شيء
الميزات العامة: معالجة الحدث	• **حذف الأحداث** • **تحرير إعدادات إشعار الحدث** • **تحرير إعدادات تسجيل الدخول إلى الأحداث** • **تعديل**	• تغيير إعدادات تسجيل الأحداث: قم **بتحرير إعدادات تسجيل الدخول إلى الأحداث** • تغيير إعدادات إشعار الأحداث: قم **بتحرير إعدادات إشعار الحدث** • حذف الأحداث: **احذف الأحداث**	لا شيء	لا شيء	الإعدادات: • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة في قاعدة البيانات • فترة زمنية لتخزين الأحداث من الأجهزة المحذوفة
الميزات العامة: العمليات على خادم الإدارة	• **قراءة** • **تعديل**	• حدد منافذ خادم الإدارة لاتصال عميل الشبكة: **قم بالتعديل**	• "النسخ الاحتياطي لبيانات	لا شيء	لا شيء

	• **تنفيذ** • **تعديل كائن ACL** • **إجراء عمليات على تحديدات الجهاز**	• 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 وحدة التحكم: **قم بالتعديل** • حدد منافذ خادم الإدارة لاتصال الهاتف المحمول: **قم بالتعديل** • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة 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**	خادم الإدارة" • "صيانة قاعدة البيانات"		
الميزات العامة: **نشر برامج Kaspersky**	• **إدارة تصحيحات Kaspersky** • **قراءة** • **تعديل** • **تنفيذ** • **إجراء عمليات على تحديدات الجهاز**	اقبل تثبيت التصحيح أو ارفضه: **إدارة تصحيحات Kaspersky**	لا شيء	• "تقرير حول استخدام مفتاح الترخيص بواسطة خادم الإدارة الافتراضي" • "تقرير حول إصدارات برامج Kaspersky" • "تقرير التطبيقات غير المتوافقة" • "تقرير حول إصدارات تحديثات وحدة	حزمة التثبيت: "Kaspersky"

				برامج "Kaspersky • "تقرير نشر الحماية"	
الميزات العامة: إدارة المفاتيح	• **تصدير إلى ملف** • **تعديل**	• تصدير ملف مفتاح: **تصدير ملف مفتاح** • تعديل إعدادات مفتاح ترخيص خادم الإدارة: **قم بالتعديل**	لا شيء	لا شيء	لا شيء
الميزات العامة: إدارة التقارير الإجبارية	• **قراءة** • **تعديل**	• إنشاء التقارير بغض النظر عن قوائم ACL الخاصة بهم: **اكتب** • تنفيذ التقارير بغض النظر عن قوائم ACL الخاصة بهم: **اقرأ**	لا شيء	لا شيء	لا شيء
الميزات العامة: التسلسل الهرمي لخوادم الإدارة	**تهيئة التسلسل الهرمي لخوادم الإدارة**	• تسجيل خوادم الإدارة الثانوية أو تحديثها أو حذفها: **تكوين التسلسل الهرمي لخوادم الإدارة**	لا شيء	لا شيء	لا شيء
الميزات العامة: أذونات المستخدم	**تعديل كائن ACL**	• 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**	لا شيء	لا شيء	لا شيء
الميزات العامة: خوادم الإدارة الافتراضية	• **إدارة خوادم الإدارة الافتراضية** • **قراءة**	• الحصول على قائمة خوادم الإدارة الافتراضية: **اقرأ** • الحصول على معلومات حول خادم الإدارة الافتراضي: **اقرأ**	لا شيء	لا شيء	لا شيء

	• **تعديل** • **تنفيذ** • **إجراء عمليات على تحديدات الجهاز**	• 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**			

أدوار المستخدم المحددة مسبقًا

توفر أدوار المستخدم المعينة لمستخدمي Kaspersky Security Center Linux مجموعات من حقوق الوصول إلى ميزات التطبيق.

يمكنك استخدام أدوار المستخدم المحددة مسبقًا مع مجموعة الحقوق المكونة بالفعل، أو إنشاء أدوار جديدة وتكوين الحقوق المطلوبة بنفسك. يمكن ربط بعض أدوار المستخدم المحددة مسبقًا والمتوفرة في Kaspersky Security Center Linux بمناصب وظيفية محددة، على سبيل المثال، **المدقق** ، **موظف الأمن**، **المشرف**. تم تكوين حقوق الوصول لهذه الأدوار مسبقًا وفقًا للمهام القياسية ونطاق واجبات الوظائف المرتبطة. يوضح الجدول أدناه كيف يمكن ربط الأدوار يمكن ربط الأدوار بمناصب وظيفية محددة.

أمثلة على أدوار المناصب الوظيفية المحددة

الدور	التعليق
مدقق الحسابات	يسمح بتنفيذ جميع العمليات مع جميع أنواع التقارير، وجميع عمليات العرض بما يشمل عرض الكائنات المحذوفة (يمنح أذونات **قراءة** و**تعديل** 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 أمان تكنولوجيا المعلومات في مؤسستك.
مسؤول الأمن	يسمح بتنفيذ جميع عمليات العرض ويسمح بإدارة التقارير ويمنح أذونات محدودة في **إدارة النظام**: نطاق **الاتصال**. يمكنك تعيين هذا الدور لموظف أمن مسؤول عن أمان تكنولوجيا المعلومات في مؤسستك.

يوضح الجدول أدناه حقوق الوصول المعينة لكل دور مستخدم محدد مسبقًا.

ميزات المجالات الوظيفية **إدارة الأجهزة المحمولة: الإدارة العامة** و**إدارة النظام** غير متوفرين في Kaspersky Security Center Linux. يتمتع المستخدم الذي يتمتع بأدوار **مشغل/ مسؤول إدارة الثغرات الأمنية والتصحيحات** و**مشغل/مسؤول إدارة الأجهزة المحمولة** بالوصول فقط للحقوق من **الميزات العامة** : المجال الوظيفي **الأساسي** .

حقوق الوصول لأدوار المستخدم المحددة مسبقًا

الدور	الوصف
مسؤول خادم الإدارة	يسمح بجميع العمليات في المجالات الوظيفية التالية، في **الميزات العامة**: • **الوظائف الأساسية** • **معالجة الحدث** • **التسلسل الهرمي لخوادم الإدارة** • **خوادم الإدارة الافتراضية**
مشغّل خادم الإدارة	يمنح حقوق **القراءة** و**التنفيذ** في جميع المجالات الوظيفية التالية في **الميزات العامة**:

	• **الوظائف الأساسية** • **خوادم الإدارة الافتراضية**
مدقق الحسابات	يسمح بجميع العمليات في المجالات الوظيفية التالية، في **الميزات العامة**: • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **الكائنات المحذوفة** • **إدارة التقارير المفروضة** يمكنك تعيين هذا الدور لشخص يقوم بإجراء تدقيق لمؤسستك.
مسؤول التثبيت	يسمح بجميع العمليات في المجالات الوظيفية التالية، في **الميزات العامة**: • **الوظائف الأساسية** • **نشر برنامج Kaspersky** • **إدارة مفتاح الترخيص** منح حقوق **القراءة والتنفيذ** في **الميزات العامة: المجالات الوظيفية لخوادم الإدارة الافتراضية**.
مشغّل التثبيت	يمنح حقوق **القراءة والتنفيذ** في جميع المجالات الوظيفية التالية في **الميزات العامة**: • **الوظائف الأساسية** • **نشر برنامج Kaspersky** (يمنح أيضًا **تصحيحات إدارة Kaspersky** مباشرةً في هذه المنطقة) • **خوادم الإدارة الافتراضية**
مسؤول Kaspersky Endpoint Security	يسمح بجميع العمليات في المجالات الوظيفية التالية: • **الميزات العامة: الوظائف الأساسية** • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات
مشغّل Kaspersky Endpoint Security	يمنح حقوق **القراءة والتنفيذ** في جميع المجالات الوظيفية التالية: • **الميزات العامة: الوظائف الأساسية** • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات
المسؤول الرئيسي	يسمح بجميع العمليات في المجالات الوظيفية، باستثناء المجالات التالية، في **الميزات العامة**: • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **إدارة التقارير المفروضة**
المشغل الرئيسي	يمنح حقوق **القراءة والتنفيذ** (إن أمكن) في جميع المجالات الوظيفية التالية: • **الميزات العامة**: • **الوظائف الأساسية** • **الكائنات المحذوفة** • **العمليات على خادم الإدارة**

	• **نشر برنامج Kaspersky Lab** • **خوادم الإدارة الافتراضية** • منطقة Kaspersky Endpoint Security، بما في ذلك جميع الميزات
إدارة جهاز المحمول	يسمح بجميع العمليات في **الميزات العامة: مجال وظيفي أساسي** .
مسؤول الأمن	يسمح بجميع العمليات في المجالات الوظيفية التالية، في **الميزات العامة**: • **الوصول إلى الكائنات بغض النظر عن قوائم التحكم في الوصول (ACLs) الخاصة بهم** • **إدارة التقارير المفروضة** يمنح **قراءة** و**تعديل** و**تنفيذ** و**حفظ الملفات من الأجهزة على محطة عمل المسؤول** و**تنفيذ العمليات على** حقوق تحديدات الأجهزة في نطاق **إدارة النظام:المجالات الوظيفية للاتصال**. يمكنك تعيين هذا الدور لموظف أمن مسؤول عن أمان تكنولوجيا المعلومات في مؤسستك.
مستخدم Self Service Portal	يسمح بجميع العمليات في **إدارة جهاز المحمول: المجالات الوظيفية لـ Self Service Portal**. هذه الميزة غير مدعومة في Kaspersky Security Center 11 والإصدار الأحدث.
المشرف	يمنح حق **القراءة** في **الميزات العامة**: **الوصول إلى الكائنات، بغض النظر عن قوائم التحكم في الوصول ACLs** و**الميزات العامة**: المجالات الوظيفية **لإدارة التقارير المفروضة**. يمكنك تعيين هذا الدور لموظف أمن ومديرين آخرين مسؤولين عن أمان تكنولوجيا المعلومات في مؤسستك.

إضافة حساب خاص بمستخدم داخلي

لإضافة حساب مستخدم داخلي جديد إلى Kaspersky Security Center Linux:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **المستخدمون**.
2. انقر على **إضافة**.
3. في نافذة **كيان جديد** التي تفتح، حدد الإعدادات الخاصة بحساب المستخدم الجديد:
   - احتفظ بالخيار الافتراضي **المستخدم**.
   - **الاسم** .
   - **كلمة المرور**لتوصيل المستخدم بـ Kaspersky Security Center Linux
     يجب أن تتوافق كلمة المرور مع القواعد التالية:
     - يجب أن تتضمن كلمة المرور من 8 إلى 16 حرفًا.
     - يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
       - الأحرف الكبيرة (A-Z)
       - الأحرف الصغيرة (a-z)
       - الأعداد (0-9)

- رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- يجب أن لا تحتوي كلمة المرور على أي مسافات بيضاء، أو حروف Unicode، أو تركيب يتكون من "." و"@"، عند وضع "." قبل "@".

لرؤية الحروف التي أدخلتها، انقر مع الاستمرار على زر **إظهار**.

عدد محاولات إدخال كلمة المرور محدود. افتراضيًا، يكون الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به هو 10. يمكنك تغيير عدد المحاولات المسموح به لإدخال كلمة مرور، كما هو موضح في "تغيير عدد محاولات إدخال كلمة المرور المسموح به".

إذا أدخل المستخدم كلمة مرور غير صالحة لعدد المرات المحدد، فسيتم منع الوصول إلى حساب المستخدم لمدة ساعة واحدة. يمكنك إلغاء قفل حساب المستخدم فقط عن طريق تغيير كلمة المرور.

- **الاسم بالكامل**
- **الوصف**
- **عنوان البريد الكتروني**
- **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 **المستخدمون والأدوار** ← **المستخدمون**.
2. انقر على **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 Linux:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **المستخدمون**.

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 الكتروني**
- **الهاتف الرئيسي**
- **كلمة المرور**لتوصيل المستخدم بـ Kaspersky Security Center Linux
  يجب أن تتوافق كلمة المرور مع القواعد التالية:
  - يجب أن تتضمن كلمة المرور من 8 إلى 16 حرفًا.
  - يجب أن تحتوي كلمة المرور على ثلاثة أحرف على الأقل من المجموعات المدرجة أدناه:
    - الأحرف الكبيرة (A-Z)
    - الأحرف الصغيرة (a-z)
    - الأعداد (0-9)
    - رموز خاصة (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - يجب أن لا تحتوي كلمة المرور على أي مسافات بيضاء، أو حروف Unicode، أو تركيب يتكون من "." و"@"، عند وضع "." قبل "@".

لرؤية كلمة المرور التي تم إدخالها، انقر مع الاستمرار فوق الزر **إظهار**.

عدد محاولات إدخال كلمة المرور محدود. افتراضيًا، يكون الحد الأقصى لعدد محاولات إدخال كلمة المرور المسموح به هو 10. يمكنك تغيير عدد المحاولات المسموح 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 التوصيل 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 خانات 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 جهاز.
3. في نافذة إعدادات المستخدم التي تفتح، حدد علامة تبويب **الأجهزة**.
4. انقر على **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** ← **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 يتم فتحها، 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 على **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 مسبقًا.
- 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 مسبقًا.
- 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، وفقط إذا كانت هذه الأجهزة تنتمي إلى مجموعات مرتبطة بهذا الدور، بما في ذلك المجموعات الفرعية.

لإضافة مستخدمين ومجموعات أمان ومجموعات إدارة إلى نطاق دور المستخدم، يمكنك استخدام إحدى الطرق التالية:

الطريقة الأولى:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **المستخدمون**.

2. حدد خانات 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** (×) 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 **المستخدمون والأدوار** ← **الأدوار**.

2. حدد خانة الاختيار الموجودة بجوار اسم الدور الذي ترغب في حذفه.

3. انقر على **حذف**.

4. في النافذة التي يتم فتحها، 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 نشطًا لمستخدم له الدور المحدد.

على سبيل المثال: تمنع السياسة تشغيل أي برنامج تحديد الموقع GPS على جميع الأجهزة في مجموعة إدارة. يلزم وجود برنامج تحديد الموقع GPS على جهاز واحد في مجموعة الإدارة "المستخدمين"، وهو الجهاز المملوك لمستخدم يعمل بوظيفة "ساعٍ". يمكنك في هذه الحالة تعيين دور "ساعي" إلى مالكه، وبعدها إنشاء ملف تعريف سياسة يسمح بتشغيل برامج تحديد الموقع GPS فقط على الأجهزة التي تم تخصيص دور "ساعي" إلى مالكيها. يتم الاحتفاظ بجميع إعدادات السياسة الأخرى. لن يتم السماح إلا للمستخدمين بدور "ساعي" أن يقوموا بتشغيل برنامج تحديد الموقع GPS. في حال تخصيص دور "ساعي" لأحد العاملين في وقتٍ لاحق، يمكن للعامل الجديد كذلك تشغيل أي برنامج تحديد الموقع على جهاز المؤسسة لديك. سيستمر حظر تشغيل برنامج تحديد الموقع GPS على الأجهزة الأخرى في مجموعة الإدارة نفسها.

لربط دور بملف تعريف سياسة:

1. في القائمة الرئيسية، انتقل إلى **المستخدمون والأدوار** ← **الأدوار**.
2. انقر على اسم الدور التي ترغب في رابطه 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 اسمًا 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 تلقائيًا بأي جهاز مخصص لمالكه دور.

إدارة مراجعات الكائن

يحتوي هذا القسم على معلومات حول إدارة مراجعات الكائنات. يتيح لك Kaspersky Security Center Linux تتبع تعديل الكائن. في كل مرة تحفظ فيها التغييرات التي أُجريت على الكائن، يتم إنشاء مراجعة. لكل مراجعة رقم.

تشتمل كائنات التطبيق التي تدعم إدارة المراجعة على:

- خودم الإدارة
- السياسات
- المهام
- مجموعات الإدارة

- حسابات المستخدمين
- حزم التثبيت

يمكنك تنفيذ الإجراءات التالية على مراجعات الكائنات:

- المقارنة بين مراجعة محددة والمراجعة الحالية
- المقارنة بين المراجعات المحددة
- مقارنة كائن بمراجعة محددة لكائن آخر من نفس النوع
- عرض المراجعة المحددة
- التراجع عن التغييرات التي أُجريت على كائن في مراجعة محددة
- حفظ المراجعات في ملف بتنسيق txt.

في نافذة خصائص أي كائن يدعم إدارة المراجعة، يعرض القسم **سجل المراجعة** قائمة مراجعات الكائنات تتضمن التفاصيل التالية:

- رقم مراجعة الكائن
- تاريخ ووقت تعديل الكائن
- اسم المستخدم الذي قام بتعديل الكائن
- الإجراء الذي تم تنفيذه على الكائن
- وصف المراجعة ذات الصلة بالتغيير الذي أُتم إجراؤه على إعدادات الكائن

  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 أُجريت على كائن في مراجعة محددة
- حفظ المراجعات في ملف بتنسيق txt.

في نافذة خصائص أي كائن يدعم إدارة المراجعة، يعرض القسم **سجل المراجعة** قائمة مراجعات الكائنات تتضمن التفاصيل التالية:

- رقم مراجعة الكائن
- تاريخ ووقت تعديل الكائن

- اسم المستخدم الذي قام بتعديل الكائن
- الإجراء الذي تم تنفيذه على الكائن
- وصف المراجعة ذات الصلة بالتغيير الذي أُتم إجراؤه على إعدادات الكائن

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.

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 يومًا). لا يمكنك تغيير مدّة التخزين إلا في حالة حصولك على إذن **التعديل** في نطاق حقوق **الكائنات المحذوفة**.

استخدام الأداة المساعدة klscflag لإغلاق المنفذ 13291

يتم استخدام المنفذ 13291 على خادم الإدارة لتلقي الاتصالات من وحدات تحكم الإدارة. على أجهزة الكمبيوتر التي لا تعمل بنظام Windows، لا يتم فتح هذا المنفذ افتراضيًا. إذا كنت تريد استخدام وحدة تحكم الإدارة المستندة إلى MMC أو الأداة المساعدة klakaut، فيمكنك فتح هذا المنفذ باستخدام الأداة المساعدة klscflag. تعمل هذه الأداة على تغيير قيمة المعلمة KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

لفتح 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 true - $
                                        ";"\svt BOOL_T -ss "|ss_type = \"SS_SETTINGS
```

2. أعد تشغيل خدمة خادم الإدارة Kaspersky Security Center عن طريق تنفيذ الأمر التالي:

```
sudo systemctl restart kladminserver_srv $
```

إن المنفذ 13291 مفتوح.

للتحقق مما إذا كان المنفذ 13291 قد تم فتحه 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)true---+
```

تعني القيمة الصحيحة أن المنفذ مفتوح. خلاف ذلك، يتم عرض القيمة الخاطئة.

تحديث قواعد بيانات Kaspersky وتطبيقاته

يصف هذا القسم الخطوات الواجب عليك اتخاذها لتحديث ما يلي بانتظام:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج
- تطبيقات Kaspersky المثبّتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

السيناريو: تحديث منتظم لقواعد بيانات Kaspersky وتطبيقاتها

يوفر هذا القسم سيناريو للتحديث المنتظم لقواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. بعد أن تكمل تكوين سيناريو حماية الشبكة، يجب أن تحافظ على موثوقية نظام الحماية للتأكد أن خوادم الإدارة والأجهزة المُدارة تبقى محمية من مختلف التهديدات، مثل الفيروسات وهجمات الشبكة وهجمات التصيد الاحتيالي.

تبقى حماية الشبكة محدثة بالتحديثات المنتظمة لما يلي:

- قواعد بيانات Kaspersky والوحدات النمطية للبرامج
- تطبيقات Kaspersky المثبّتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

عند إكمالك لهذا السيناريو، يمكنك التأكد مما يلي:

- شبكتك محمية بأحدث برامج Kaspersky، وهذه تشمل مكونات Kaspersky Security Center Linux 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 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 تشغِّل "المعالج"، قم بإنشاء المهمة الآن.

المهمة مطلوبة لتنزيل التحديثات من خوادم تحديث Kaspersky إلى مستودع خادم الإدارة وكذلك لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج لـ Kaspersky Security Center. بعد تنزيل التحديثات، يمكن نشرها على الأجهزة المُدارة.

إذا كانت شبكتك قد خصصت نقاط التوزيع، يتم تنزيل التحديثات تلقائيًا من مستودع خادم الإدارة إلى مستودعات نقاط التوزيع. في هذه الحالة، تقوم الأجهزة المُدارة المضمّنة في نطاق نقطة التوزيع بتنزيل التحديثات من مستودع نقطة التوزيع بدلاً من مستودع خادم الإدارة.

تعليمات المساعدة: 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 الكيفية: 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.

5. **تحسين عملية التحديث باستخدام ملفات مختلفة (اختياري)**

يمكنك تحسين حركة المرور بين خادم الإدارة والأجهزة المُدارة باستخدام ملفات مختلفة . عند تفعيل هذه الميزة، يقوم خادم الإدارة أو نقطة التوزيع بتنزيل ملفات diff بدلاً من كامل ملفات قواعد بيانات Kaspersky أو الوحدات النمطية للبرامج. يصف ملف diff الاختلافات بين نسختين من ملف قاعدة البيانات أو الوحدة النمطية للبرامج. وبالتالي يشغل ملف diff مساحة أقل من ملف كامل. يتسبب هذا في انخفاض حركة المرور بين خادم الإدارة أو نقاط التوزيع والأجهزة المُدارة. لاستخدام هذه الميزة، قم بتفعيل خيار **تنزيل ملفات تفاضلية** في خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة و/أو مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع.

تعليمات المساعدة: استخدام ملفات diff في تحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج

6. **تكوين التثبيت التلقائي لتحديثات تطبيقات الأمان.**

قم بإنشاء مهام التحديث للتطبيقات المُدارة من أجل توفير تحديثات في الوقت المناسب للوحدات النمطية للبرامج وقواعد بيانات Kaspersky، بما في ذلك قواعد بيانات مكافحة الفيروسات. لضمان التحديث في الوقت المناسب، ننصحك بتحديد خيار **موعد تنزيل التحديثات الجديدة إلى المستودع** عند تكوين جدول المهمة.

إذا كانت شبكتك تتضمن أجهزة IPv6 فقط وتريد تحديث تطبيقات الأمان المثبتة على هذه الأجهزة بانتظام، فتأكد من تثبيت إصدار خادم الإدارة 13.2 وإصدار عميل الشبكة 13.2 على الأجهزة المُدارة.

إذا تطلب التحديث مراجعة وقبول شروط اتفاقية ترخيص المستخدم النهائي، أنت بحاجة أولاً إلى قبول الشروط. يمكن بعد ذلك نشر التحديث على الأجهزة المُدارة.

النتائج

عند إكمال السيناريو، يتم تكوين Kaspersky Security Center Linux لتحديث قواعد بيانات Kaspersky بعد تنزيل التحديثات إلى مستودع خادم الإدارة. 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 المثبّتة، بما في ذلك مكونات Kaspersky Security Center وتطبيقات الأمان

Kaspersky Security Center لا يمكنه تحديث تطبيقات Kaspersky تلقائيًا. لتحديث التطبيقات، قم بتنزيل أحداث إصدارات التطبيقات من موقع Kaspersky الإلكتروني ثم ثبتها يدويًا:

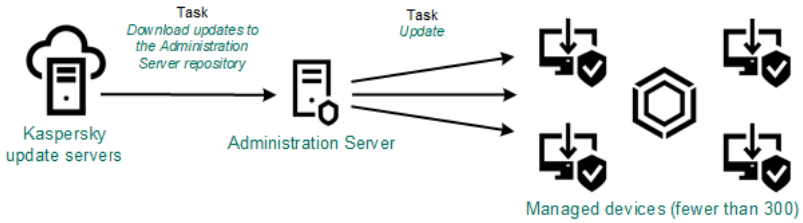
- خادم إدارة Kaspersky Security Center و Kaspersky Security Center 14 Web Console
- عميل الشبكة و Kaspersky Endpoint Security for Linux ومكون الإدارة الإضافي للويب

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 Linux على الأجهزة المُدارة
- من خلال مجلد محلي أو شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة

في هذا المخطط، يقوم Kaspersky Security Center بتنزيل التحديثات من خلال مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. وفي الشبكات الصغيرة التي تحتوي على أقل من 300 جهاز مُدار في مقطع شبكة واحد أو أقل من 10 أجهزة مُدارة في كل مقطع للشبكة، يتم توزيع التحديثات إلى الأجهزة المُدارة مباشرة من مستودع خادم الإدارة (انظر الشكل أدناه).



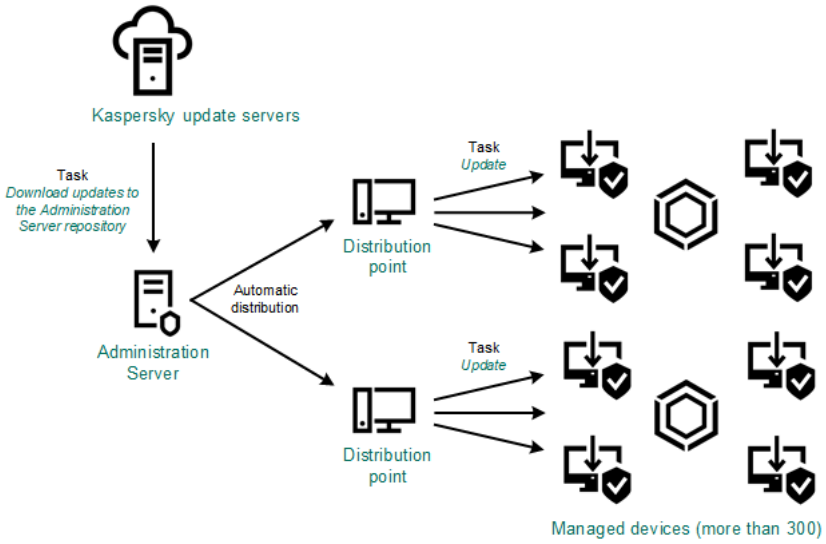
التحديث باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة دون نقاط توزيع

كمصدر للتحديثات، لا يمكنك استخدام خوادم تحديث Kaspersky فحسب، بل يمكنك أيضًا استخدام مجلد محلي أو مجلد شبكة.

يتصل خادم الإدارة افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة لاستخدام بروتوكول HTTP بدلاً من HTTPS.

إذا كانت شبكتك تحتوي على 300 جهاز مُدار أو أكثر في مقطع شبكة واحد أو إذا كانت شبكتك تتكون من مقاطع شبكات متعددة تحتوي على أكثر من 9 أجهزة مُدارة في كل مقطع شبكة، فنوصيك باستخدام نقاط التوزيع لنشر التحديثات إلى الأجهزة المُدارة (انظر الشكل أدناه). وتقلل نقاط التوزيع من التحميل الموجود على خادم الإدارة ويعمل على تحسين حركة المرور بين خادم الإدارة والأجهزة المُدارة. يمكنك حساب عدد نقاط التوزيع لمطلوبة لشبكتك وتكوينها.

وفي هذا المخطط، يتم تنزيل التحديثات تلقائيًا من مستودع خادم الإدارة إلى مستودعات نقاط التوزيع. تقوم الأجهزة المُدارة المضمّنة في نطاق نقطة التوزيع بتنزيل التحديثات من مستودع نقطة التوزيع بدلاً من مستودع خادم الإدارة.



التحديث باستخدام مهمة تنزيل التحديثات إلى مستودع خادم الإدارة مع نقاط توزيع

عند اكتمال مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يتم تنزيل تحديثات قواعد بيانات Kaspersky والوحدات النمطية للبرامج لتطبيق Kaspersky Endpoint Security for Linux إلى مستوده خادم الإدارة. يتم تثبيت هذه التحديثات من خلال مهمة تحديث لـ Kaspersky Endpoint Security for Linux.

لا تتوفر تنزيل التحديثات إلى مستودع مهمة خادم الإدارة على خوادم الإدارة الافتراضية. مستودع خادم الإدارة الافتراضي يعرض التحديثات المنزّلة على خادم الإدارة الرئيسي.

ويمكنك تكوين التحديثات للتحقق من التشغيل والأخطاء بمجموعة من الأجهزة الاختبارية. وفي حالة نجاح عملية التحقق، يتم توزيع التحديثات إلى الأجهزة المُدارة الأخرى.

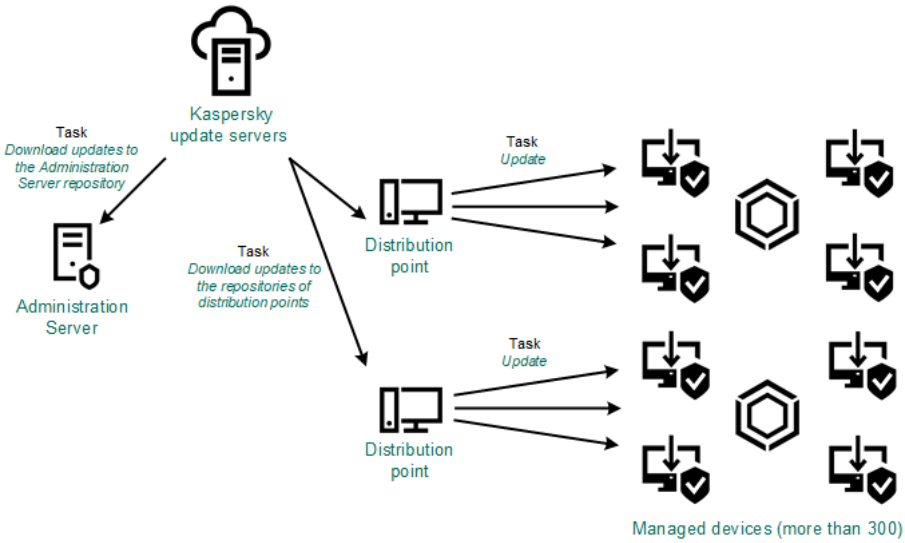
يتطلب كل تطبيق من تطبيقات Kaspersky تحديثات من خادم الإدارة. قام خادم الإدارة بتجميع تلك الطلبات وتنزيل التحديثات التي تم طلبها من قبل التطبيق فقط. يضمن هذا عدم تنزيل نفس التحديثات عدة مرات وعدم تنزيل التحديثات غير الضرورية أبدًا. عند تشغيل مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، يرسل خادم الإدارة المعلومات التالية إلى خوادم تحديث Kaspersky تلقائيًا لضمان تنزيل إصدارات ذات صلة بقواعد بيانات Kaspersky والوحدات النمطية للبرامج:

- معرف التطبيق وإصداره
- معرف إعداد التطبيق
- معرف المفتاح المفعل
- معرف تشغيل تنزيل التحديثات إلى مستودع مهمة خادم الإدارة

لا تحتوي أيٌ من المعلومات المنقولة على تفاصيل شخصية أو بيانات سرية أخرى. يحمي AO Kaspersky Lab المعلومات وفقًا للمتطلبات التي ينص عليها القانون.

باستخدام المهمتين: المهمة تنزيل التحديثات إلى مستودع خادم الإدارة والمهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع

يمكنك تنزيل التحديثات إلى مستودعات نقاط التوزيع مباشرة من خوادم تحديث Kaspersky بدلاً من مستودع خادم الإدارة، ثم توزيع التحديثات على الأجهزة المُدارة (انظر الشكل أدناه). ومن الأفضل التنزيل إلى مستودعات نقاط التوزيع إذا كانت تكلفة حركة المرور بين خادم الإدارة ونقاط التوزيع أكثر من حركة المرور بين نقاط التوزيع وخوادم تحديث Kaspersky أو إذا لم يتمتع خادم الإدارة بإمكانية الوصول إلى الإنترنت.



تحديث باستخدام المهمة تنزيل التحديثات إلى مستودع خادم الإدارة والمهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيع

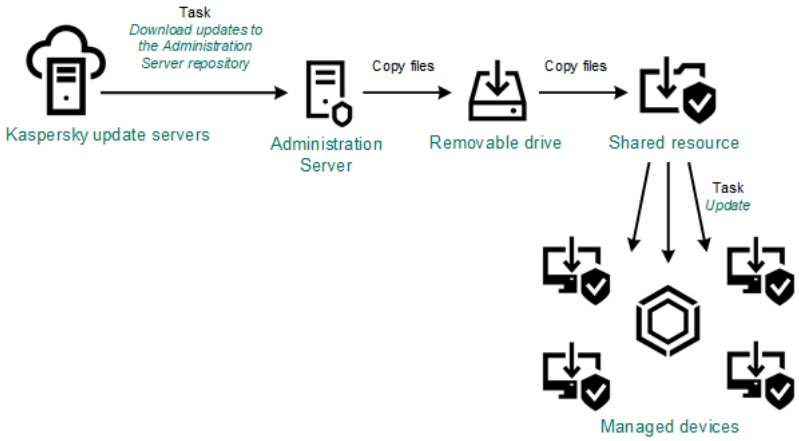
يتصل خادم الإدارة ونقاط التوزيع افتراضيًا بخوادم تحديث Kaspersky وتنزيل التحديثات باستخدام بروتوكول HTTPS. يمكنك تكوين خادم الإدارة و/أو نقاط التوزيع لاستخدام بروتوكول HTTP بدلاً من HTTPS.

لتنفيذ هذا المخطط، قم بإنشاء مهمة تنزيل التحديثات إلى المستودعات الخاصة بنقاط التوزيعبالإضافة إلى مهمة تنزيل التحديثات إلى مستودع خادم الإدارة. وبعد ذلك، ستقوم نقاط التوزيع بتنزيل التحديثات من خوادم تحديث Kaspersky وليس من مستودع خادم الإدارة.

كما يلزم توفير مهمة تنزيل التحديثات إلى مستودع خادم الإدارة في هذا المخطط، نظرًا لاستخدام هذه المهمة في تنزيل قواعد بيانات Kaspersky والوحدات النمطية للبرامج في Kaspersky Security Center.

يدويًا من خلال مجلد محلي أو مجلد مشترك أو خادم FTP

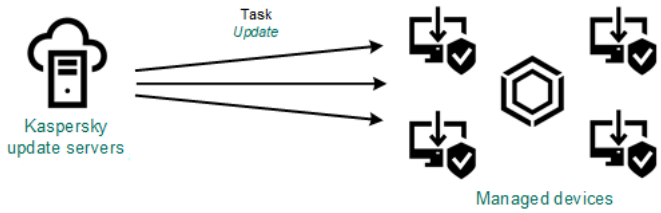
إذا لم تتمتع الأجهزة العميلة باتصال بخادم الإدارة، يمكنك استخدام مجلد محلي أو مورد مشترك كمصدر لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج والتطبيقات. وفي هذا المخطط، تحتاج إلى نسخ التحديثات اللازمة من مستودع خادم الإدارة إلى محرك الأقراص القابل للإزالة ونسخ التحديثات إلى المجلد المحلي أو المورد المشترك المحدد كمصدر تحديث في إعدادات Kaspersky Endpoint Security for Linux (انظر الشكل أدناه).



التحديث من خلال مجلد محلي أو مجلد مشترك أو خادم FTP

مباشرة من خوادم تحديث Kaspersky إلى Kaspersky Endpoint Security for Linux على الأجهزة المُدارة

على الأجهزة المُدارة، يمكنك تكوين Kaspersky Endpoint Security for Linux لتلقي التحديثات مباشرة من خوادم تحديث Kaspersky (انظر الشكل أدناه).



تحديث تطبيقات الأمن مباشرة من خوادم تحديث Kaspersky

في هذا المخطط، تطبيق الأمن لا يستخدم المستودع المتوفر من Kaspersky Security Center. ولتلقي التحديثات مباشرة من خوادم تحديث Kaspersky، حدد خوادم تحديث Kaspersky كمصدر تحديث في تطبيق الأمان. للحصول على وصف كامل لهذه الإعدادات، يُرجى الرجوع إلى وثائق Kaspersky Endpoint Security for Linux.

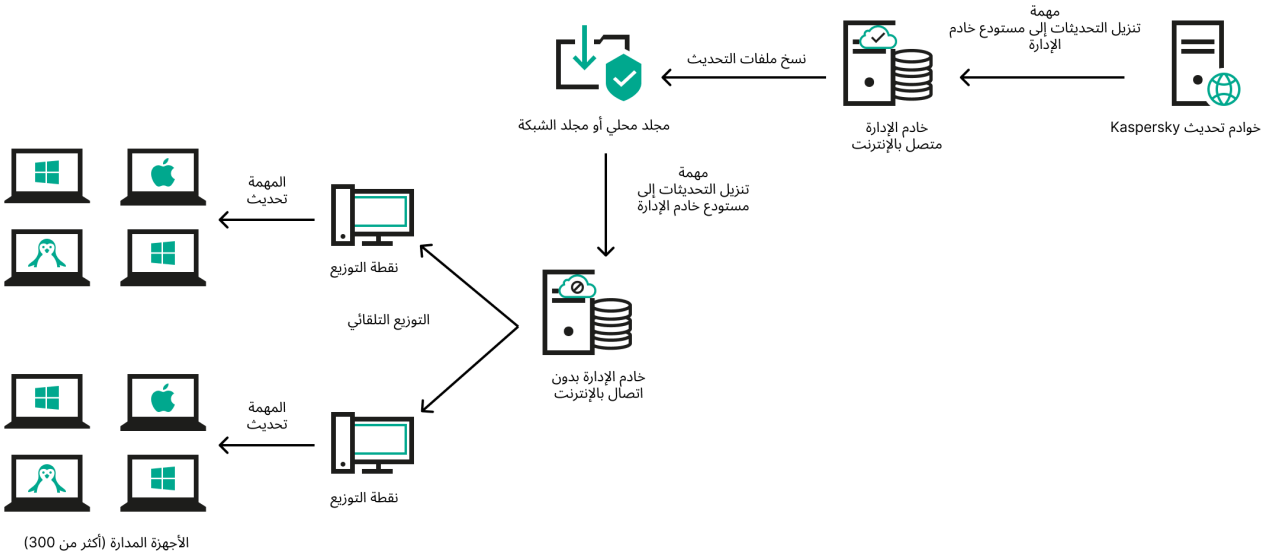
من خلال مجلد محلي أو شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت، فيمكنك تكوين مهمة تنزيل التحديثات إلى مستودع خادم الإدارة لتنزيل التحديثات من مجلد محلي أو مجلد شبكة. في هذه الحالة، يجب عليك نسخ ملفات التحديث المطلوبة إلى المجلد المحدد من وقت لآخر. على سبيل المثال، يمكنك نسخ ملفات التحديث المطلوبة من أحد المصادر التالية:

- خادم الإدارة الذي لديه اتصال بالإنترنت (انظر الشكل أدناه)

  نظرًا لأن خادم الإدارة يقوم بتنزيل التحديثات التي تطلبها تطبيقات الأمان فقط، فيجب أن تتطابق مجموعات تطبيقات الأمان التي تتم إدارتها بواسطة خوادم الإدارة – تلك التي تحتوي على اتصال بالإنترنت وتلك التي لا تحتوي على ذلك –.

  إذا كان خادم الإدارة الذي تستخدمه لتنزيل التحديثات يحتوي على الإصدار 13.2 أو إصدار أقدم، فافتح خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، ثم قم بتمكين خيار **تنزيل التحديثات باستخدام النظام القديم**.



التحديث من خلال مجلد محلي أو مجلد شبكة إذا لم يكن لدى خادم الإدارة اتصال بالإنترنت

- Kaspersky Update Utility

  نظرًا لأن هذه الأداة تستخدم النظام القديم لتنزيل التحديثات، افتح خصائص مهمة تنزيل التحديثات إلى مستودع خادم الإدارة، ثم قم بتمكين خيار تنزيل التحديثات باستخدام النظام القديم.

إنشاء مهمة تنزيل التحديثات إلى مستودع خادم الإدارة

تتيح لك مهمة تنزيل تحديثات تنزيل التحديثات إلى مستودع خادم الإدارة تنزيل تحديثات قواعد البيانات ووحدات البرامج لتطبيقات أمان Kaspersky من خوادم تحديث Kaspersky إلى مستودع خادم الإدارة.

ينشئ معالج البدء السريع من Kaspersky Security Center تلقائيًا تنزيل التحديثات إلى مستودع خادم الإدارة الإدارة لخادم الإدارة. في قائمة المهام ، يمكن أن يكون هناك تنزيل التحديثات إلى مستودع خادم الإدارة. يمكنك إنشاء هذه المهمة مرة أخرى إذا تمت إزالتها من قائمة المهام لخادم الإدارة.

بعد اكتمال مهمة تنزيل التحديثات إلى مستودع خادم الإدارة وتنزيل التحديثات، يمكن نشرها على الأجهزة المدارة.

قبل توزيع التحديثات على الأجهزة المدارة، يمكنك تشغيل المهمة التحقق من التحديث. يمكنك ذلك من التأكد من أن خادم الإدارة يثبت التحديثات التي تم تنزيلها بشكل صحيح ولا 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. انتقل إلى **الأجهزة** ← **المهام**.
2. انقر على **إضافة**.

   يبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.
3. بالنسبة لتطبيق Kaspersky Security Center، حدد نوع مهمة **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. في صفحة **إنهاء عملية إنشاء المهمة**، يمكنك تمكين الخيار **فتح تفاصيل المهمة عند اكتمال الإنشاء** لفتح نافذة خصائص المهمة وتعديل إعدادات المهمة الافتراضية. بخلاف ذلك، يمكنك تكوين إعدادات المهمة لاحقًا في أي وقت.
6. انقر على زر **إنهاء**.

   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**

  كمصدر للتحديثات، يمكنك استخدام خوادم تحديث Kaspersky أو مجلد محلي أو مجلد شبكة أو خادم إدارة أساسي.

- **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.

- **نسخ التحديثات التي تم تنزيلها إلى مجلدات إضافية**

  بعد تلقي خادم الإدارة للتحديثات، يقوم بنسخها إلى المجلدات المحددة. استخدم هذا الخيار في حال رغبت في إدارة توزيع التحديثات يدويًا على الشبكة الخاصة بك.

  على سبيل المثال، قد ترغب في استخدام هذا الخيار في الموقف التالي: تتكون شبكة المؤسسة الخاصة بك من العديد من الشبكات الفرعية المستقلة، ولا تمتلك الأجهزة على كل شبكة فرعية إمكانية الوصول إلى الشبكات الفرعية الأخرى. ومع ذلك فإن جميع الأجهزة في جميع الشبكات الفرعية تمتلك إمكانية الوصول إلى مشاركة الشبكة العامة. في هذه الحالة، قم بتعيين خادم الإدارة في واحدة من الشبكات الفرعية لتنزيل التحديثات من خوادم تحديث Kaspersky، وقم بتمكين هذا الخيار ثم حدد مشاركة الشبكة هذه. من تنزيل التحديثات إلي مستودع المهام لخوادم إدارة أخرى، قم بتحديد نفس مشاركة الشبكة كمصدر تحديث.

  يتم تعطيل هذا الخيار افتراضيًا.

- **تنزيل ملفات تفاضلية**

يقوم هذا الخيار بتمكين ميزة تنزيل ملفات diff.

يتم تعطيل هذا الخيار افتراضيًا.

- **تنزيل التحديثات باستخدام النظام القديم**

بدءًا من الإصدار 14، يقوم Kaspersky Security Center بتنزيل تحديثات قواعد البيانات ووحدات البرامج باستخدام النظام الجديد. لكي يقوم التطبيق بتنزيل التحديثات باستخدام النظام الجديد، يجب أن يحتوي مصدر التحديث على ملفات تحديث ببيانات تعريف متوافقة مع النظام الجديد. إذا كان مصدر التحديث يحتوي على ملفات تحديث ببيانات أولية متوافقة مع النظام القديم فقط، فقم بتمكين الخيار **تنزيل التحديثات باستخدام النظام القديم**. خلاف ذلك، ستفشل مهمة تنزيل التحديث.

على سبيل المثال، يجب تمكين هذا الخيار عند تحديد مجلد محلي أو مجلد شبكة كمصدر تحديث، ويتم تنزيل ملفات التحديث الموجودة في هذا المجلد بواسطة أحد التطبيقات التالية:

- Kaspersky Update Utility

تقوم هذه الأداة بتنزيل التحديثات باستخدام النظام القديم.

- Kaspersky Security Center 13.2 أو إصدار سابق

على سبيل المثال، خادم الإدارة 1 ليس به اتصال بالإنترنت. في هذه الحالة، يمكنك تنزيل التحديثات باستخدام خادم الإدارة 2 الذي يحتوي على اتصال بالإنترنت، ثم وضع التحديثات على مجلد محلي أو مجلد شبكة لاستخدامه كمصدر تحديث لخادم الإدارة 1. إذا كان خادم الإدارة 2 يحتوي على الإصدار 13.2 أو إصدار أقدم، فقم بتمكين الخيار **تنزيل التحديثات باستخدام النظام القديم** في مهمة خادم الإدارة 1.

يتم تعطيل هذا الخيار افتراضيًا.

- **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.

9. 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** (يتم تحديده بصورة افتراضية)

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**

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)**

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. إنه ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center Linux.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 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.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل 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.

- **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.

- إعدادات المهمة الإضافية:

- **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** و**مرة** و**فورًا**، 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 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.

- **أوقف المهمة إذا كانت تعمل لمدة أطول من (دقيقة)**

بعد انتهاء الفترة الزمنية المحددة، يتم إيقاف المهمة تلقائيًا، سواء أكانت مكتملة أم لا.

قم بتمكين هذا الخيار إذا كنت تريد مقاطعة (أو إيقاف) المهام التي تستغرق وقتًا طويلاً للتنفيذ.

يتم تعطيل هذا الخيار افتراضيًا. وقت تنفيذ المهمة الافتراضي هو 120 دقيقة.

10. 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 العميلة وخوادم الإدارة الثانوية من المجلد المشترك لخادم الإدارة.

عرض التحديثات المُنزّلة

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 المنزّلة:

في القائمة الرئيسية ، انتقل إلى **العمليات** ← **تطبيقات KASPERSKY** ← **تحديثات قواعد بيانات KASPERSKY ووحدات البرامج النمطية**.

ستظهر قائمة بالتحديثات المتاحة.

التحقق من التحديثات المُنزّلة

قبل تثبيت التحديثات على الأجهزة المدارة، يمكنك أولاً التحقق من صحة التحديث الخاصة بقابلية التشغيل والأخطاء من خلال مهمة التحقق من صحة التحديث. يتم تنفيذ مهمة التحقق من صحة التحديث تلقائيًا كجزء من مهمة 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. أيضًا لن يتم بدء الهام ذات نوع الجدول **عند تنزيل تحديثات جديدة إلى المستودع** بعد. يتم إجراء هذه العمليات في البداية التالية لمهمة تنزيل التحديثات إلى مستودع خادم الإدارة إذا اكتمل فحص التحديثات الجديدة بنجاح.

تعتبر مجموعة التحديثات غير صالحة في حالة الوفاء بأحد الشروط التالية على جهاز اختبار واحد على الأقل:

- حدث خطأ في مهمة تحديث.
- تغيير حالة الحماية في الوقت الحقيقي لتطبيق الأمن بعد تطبيق التحديثات.
- تم اكتشاف كائن مصاب أثناء تشغيل مهمة الفحص عند الطلب.
- حدث خطأ في وقت تشغيل تطبيق Kaspersky.

إذا لم يكن أي من الشروط المدرجة في القائمة صحيحًا لأي جهاز اختبار، فتعتبر مجموعة التحديثات صالحة وتعتبر مهمة التحقق من صحة التحديث مكتملة بنجاح.

قبل أن تبدأ في إنشاء مهمة التحقق من صحة التحديث، نفذ المتطلبات الأساسية:

1. إنشاء مجموعة الإدارة مع العديد من أجهزة الاختبار. ستحتاج إلى هذه المجموعة للتحقق من التحديثات.

   نُوصى باستخدام الأجهزة التي تتمتع بحماية موثوقة وتكوين التطبيق الشائع عبر الشبكة. يزيد هذا النهج من جودة واحتمالية اكتشاف الفيروسات أثناء عمليات الفحص، ويقلل من مخاطر الإيجابيات الكاذبة. إذا تم اكتشاف الفيروسات على أجهزة الاختبار، تعتبر مهمة التحقق من صحة التحديث غير ناجحة.

2. إنشاء مهام التحديث وفحص الفيروسات لتطبيق مدعوم من Kaspersky Security Center، على سبيل المثال Kaspersky Endpoint Security for Linux. عند إنشا مهام التحديث وفحص الفيروسات، حدد مجموعة الإدارة مع أجهزة الاختبار.

   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 Linux يتحقق من التحديثات التي تم تنزيلها قبل توزيعها إلى الأجهزة العميلة:

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 افتراضيًا.

   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

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. اتبع خطوات المعالج.
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 لاحقًا في أي وقت.
7. انقر على زر **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 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 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 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 افتراضيًا.

- **تنزيل التحديثات باستخدام النظام القديم**

بدءًا من الإصدار 14، يقوم Kaspersky Security Center بتنزيل تحديثات قواعد البيانات ووحدات البرامج باستخدام النظام الجديد. لكي يقوم التطبيق بتنزيل التحديثات باستخدام النظام الجديد، يجب أن يحتوي مصدر التحديث على ملفات تحديث ببيانات تعريف متوافقة مع النظام الجديد. إذا كان مصدر التحديث يحتوي على ملفات تحديث ببيانات أولية متوافقة مع النظام القديم فقط، فقم بتمكين الخيار **تنزيل التحديثات باستخدام النظام القديم**. خلاف ذلك، ستفشل مهمة تنزيل التحديث.

على سبيل المثال، يجب تمكين هذا الخيار عند تحديد مجلد محلي أو مجلد شبكة كمصدر تحديث، ويتم تنزيل ملفات التحديث الموجودة في هذا المجلد بواسطة أحد التطبيقات التالية:

- Kaspersky Update Utility

تقوم هذه الأداة بتنزيل التحديثات باستخدام النظام القديم.

- Kaspersky Security Center 13.2 أو إصدار سابق

على سبيل المثال، تم تكوين نقطة توزيع لأخذ التحديثات من مجلد محلي أو مجلد شبكة. في هذه الحالة، يمكنك تنزيل التحديثات باستخدام خادم إدارة متصل بالإنترنت، ثم وضع التحديثات للمجلد المحلي في نقطة التوزيع. إذا كان خادم الإدارة يحتوي على الإصدار 13.2 أو إصدار أقدم ، فقم بتمكين الخيار **تنزيل التحديثات باستخدام النظام القديم** في مهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع.

يتم تعطيل هذا الخيار افتراضيًا.

10. أنشئ جدولاً لبدء المهمة. إن لزم الأمر، قم بتحديد الإعدادات التالية:

- **البدء المُجدول**:

حدد الجدول الذي تعمل المهمة وفقًا له، وقم بتكوين الجدول المحدد.

- **يدويًا** (يتم تحديده بصورة افتراضية)

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**

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)**

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. إنه ضروري للتوافق مع الإصدارات السابقة من Kaspersky Security Center Linux.

بشكل افتراضي، يبدأ تشغيل المهمة كل يوم، في الوقت الحالي للنظام.

- **أسبوعيًا**

تعمل المهمة كل أسبوع في اليوم المحدد وفي الوقت المحدد.

- **حسب أيام الأسبوع**

تعمل المهمة بشكل منتظم، في الأيام المحددة من الأسبوع وفي الوقت المحدد.

بشكلٍ افتراضي، تعمل المهمة كل يوم جمعة الساعة 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.

- **كل شهر في أيام معينة من الأسابيع المحددة**

تعمل المهمة بشكل 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.

- **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 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**

تبدأ المهمة الحالية بعد اكتمال مهمة أخرى. يمكنك تحديد كيفية وجوب اكتمال المهمة السابقة (بنجاح أو مع خطأ) لتنشيط بدء تشغيل المهمة الحالية.

- **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** و**مرة** و**فورًا**، 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 المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

يتم حساب وقت البدء الموزع تلقائيًا عند إنشاء مهمة، استنادًا إلى عدد الأجهزة العميلة التي تم تعيين المهمة إليها. لاحقًا، تبدأ المهمة دائمًا في وقت البدء المحسوب. ومع ذلك، تتغير القيمة المحسوبة لوقت بداية المهمة، فقط عند تحرير إعدادات المهمة أو بدء تشغيل المهمة يدويًا.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

- **استخدام التأخير العشوائي لبدء المهمة ضمن فاصل زمني (بالدقائق)**

إذا تم تمكين هذا الخيار، يتم بدء تشغيل المهمة على أجهزة العملاء بشكل عشوائي خلال الفاصل الزمني المحدد. بداية المهمة الموزعة تساعد على تجنب عدد كبير من الطلبات المتزامنة من قبل الأجهزة العميلة إلى خادم الإدارة عند تشغيل مهمة مجدولة.

إذا تم تعطيل هذا الخيار، فستبدأ المهمة على الأجهزة العميلة وفقًا للجدول.

يتم تعطيل هذا الخيار افتراضيًا. الفاصل الزمني الافتراضي هو ساعة واحدة.

11. انقر على زر **حفظ**.

سيتم إنشاء المهمة وتكوينها.

بالإضافة إلى الإعدادات التي تقوم بتحديدها في أثناء إنشاء مهمة، يمكنك تغيير خصائص أخرى للمهمة التي تم إنشاؤها.

عند تنفيذ مهمة 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.

إضافة مصادر التحديثات الخاصة بتحديثات التنزيل إلى مهمة مستودع خادم الإدارة

عند إنشاء أو استخدام المهمة لتنزيل التحديثات إلى مستودع خادم الإدارة، يمكنك اختيار مصادر التحديثات التالية:

- خوادم تحديث Kaspersky
- خادم الإدارة الرئيسي

  ينطبق هذا المصدر على المهام التي يتم إنشاؤها لخادم الإدارة الثانوي أو الافتراضي.
- مجلد محلي أو مجلد الشبكة

تُستخدم خوادم تحديث Kaspersky افتراضيًا، ولكن يمكنك أيضًا تنزيل التحديثات من مجلد محلي أو مجلد شبكة. قد ترغب في استخدام المجلد إذا لم يتوفر وصول إلى الإنترنت لشبكتك. في هذه الحالة، يمكنك تنزيل التحديثات يدويًا من خوادم تحديث Kaspersky ووضع الملفات التي تم تنزيلها في المجلد المطلوب.

يمكنك تحديد مسار واحد فقط لمجلد محلي أو مجلد شبكة. كمجلد محلي، يمكنك استخدام مجلد واحد فقط على خادم الإدارة؛ كمجلد شبكة، كما يمكنك استخدام خادم FTP أو HTTP فقط.

إذا أضفت خوادم تحديث Kaspersky والمجلد المحلي أو مجلد الشبكة ، فسيتم تنزيل التحديثات أولاً من المجلد. في حالة حدوث خطأ أثناء التنزيل، سيتم استخدام خوادم تحديث Kaspersky.

في حالة وجود مجلد مشترك يحتوي على تحديثات محميًا بكلمة مرور، قم بتمكين خيار **تحديد حساب للوصول إلى المجلد المشترك لمصدر التحديث (إن وجد)** وأدخل بيانات اعتماد الحساب المطلوبة للوصول.

لإضافة مصادر التحديثات:

1. انتقل إلى **الأجهزة** ← **المهام**.
2. انقر على **تنزيل التحديثات إلى مستودع خادم الإدارة**.
3. انتقل إلى علامة تبويب **إعدادات التطبيق** .
4. في سطر **مصادر التحديثات**، انقر على زر **تكوين** .
5. في النافذة التي تفتح، انقر على زر **إضافة**.
6. في قائمة مصادر التحديث، أضف المصادر الضرورية. إذا قمت بتحديد خيار **المجلد المحلي أو مجلد الشبكة**، فحدد مسارًا للمجلد.
7. انقر على**موافق**، ثم أغلق نافذة خصائص مصدر التحديث.
8. في نافذة مصدر التحديث، انقر على **موافق**.
9. انقر على زر **حفظ** في نافذة المهمة.

يتم الآن تنزيل التحديثات إلى مستودع خادم الإدارة من المصادر المحددة.

حول استخدام ملفات diff لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج

عندما يقوم Kaspersky Security Center Linux بتنزيل التحديثات من خوادم تحديث Kaspersky، فإنه يعمل على تحسين حركة المرور باستخدام ملفات مختلفة. 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.

لا تستخدم نقاط التوزيع الإرسال المتعدد لـ IP من أجل التوزيع التلقائي لملفات diff.

تمكين ميزة تنزيل ملفات diff: سيناريو

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 مكّن الميزة في إعدادات نهج عميل الشبكة لنقطة التوزيع التي تتلقى تحديثات من خادم الإدارة.

   ثم قم بتمكين الميزة لنقطة التوزيع التي تستقبل التحديثات من خادم الإدارة.

   يتم تمكين الميزة في إعدادات سياسة عميل الشبكة و—إذا تم تعيين نقاط التوزيع يدويًا، وإذا كنت تريد تجاوز إعدادات السياسة—في قسم **نقاط التوزيع** في خصائص خادم الإدارة.

للتحقق من أنه تم تمكين ميزة تنزيل ملفات diff بنجاح، يمكنك قياس حركة المرور الداخلية قبل وبعد تنفيذ السيناريو.

تنزيل التحديثات عن طريق نقاط التوزيع

يتيح Kaspersky Security Center Linux لنقاط التوزيع تلقي التحديثات من خادم الإدارة، أو خوادم Kaspersky، أو من مجلد شبكة أو مجلد محلي.

لتكوين تنزيل التحديث لنقطة توزيع:

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. انقر على اسم نقطة التوزيع التي سيتم من خلالها تسليم التحديثات إلى الأجهزة العميلة في المجموعة.

4. في النافذة خصائص نقطة التوزيع، حدد القسم **مصدر التحديثات**.

5. تحديد مصدر تحديث 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 تنزيل التحديثات إلى مستودعات نقاط التوزيع:
  - إذا كانت هذه المهمة موجودة بالفعل على الجهاز، فحدد المهمة من القائمة.
  - في حالة عدم وجود مثل هذه المهمة حتى الآن على الجهاز، انقر فوق الرابط **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.

ستتلقى نقطة التوزيع التحديثات من المصدر المحدد.

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.

عندما تحتاج إلى تحديث قواعد البيانات والوحدات النمطية للبرامج على جهاز (أو مجموعة أجهزة) ليست متصلة بخادم الإدارة (الرئيسي أو التابع) أو نقطة توزيع أو الإنترنت، يجب عليك استخدام مصادر تحديثات بديلة، مثل خادم FTP أو مجلد محلي. عليك في هذه الحالة تسليم ملفات التحديثات المطلوبة باستخدام جهاز تخزين كبير المساحة، مثل محرك أقراص فلاش أو محرك قرص ثابت خارجي.

يمكنك نسخ التحديثات المطلوبة من:

- خادم الإدارة.

  للتأكد من احتواء مستودع خادم الإدارة على التحديثات المطلوبة لتطبيق الأمان المثبت على الجهاز غير المتصل، يجب أن يكون على الأقل أحد الأجهزة المتصلة المُدارة مثبت عليه نفس تطبيق الأمان. يجب تكوين هذا التطبيق لاستقبال تحديثات من مستودع خادم الإدارة من خلال مهمة 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 مباشرةً من خوادم تحديث Kaspersky.

يوجد أدناه مثال على تكوين تحديثات قواعد بيانات والوحدات النمطية للبرامج عن طريق نسخها من مستودع خادم الإدارة.

لتحديث قواعد بيانات Kaspersky والوحدات النمطية للبرامج على الأجهزة غير المتصلة بالإنترنت:

1. قم بتوصيل محرك الأقراص القابلة للإزالة بالجهاز المثبت عليه خادم الإدارة.

2. انسخ ملفات التحديثات إلى محرك الأقراص القابل للإزالة.

بشكلٍ 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. على الأجهزة غير المتصلة بالإنترنت، قم بتكوين Kaspersky Endpoint Security for Linux لاستقبال التحديثات من مجلد محلي أو مصدر مشترك، مثل خادم FTP أو مجلد مشترك.

4. انسخ ملفات التحديثات من محرك الأقراص القابل للإزالة إلى المجلد المحلي أو المصدر المشترك الذي ترغب في استخدمه كمصدر تحديث.

5. على الجهاز غير المتصل بالإنترنت الذي يتطلب تثبيت التحديث، ابدأ مهمة تحديث Kaspersky Endpoint Security for Linux.

بعد اكتمال مهمة التحديث، تكون قواعد بيانات Kaspersky والوحدات النمطية للبرامج محدثة على الجهاز.

تعديل نقاط التوزيع وبوابات الاتصال

تُجري بنية مجموعات الإدارة في Kaspersky Security Center Linux الوظائف التالية:

- تعيين نطاق السياسات.

توجد طريقة بديلة لتطبيق مجموعات الإعدادات ذات الصلة على الأجهزة، عن طريق استخدام ملفات تعريف السياسة.

- تعيين نطاق المهام الجماعية

يوجد نهج لتحديد نطاق المهام الجماعية غير المستندة إلى التسلسل الهرمي لمجموعات الإدارة: استخدام المهام لتحديدات الأجهزة والمهام لأجهزة محددة.

- تعيين حقوق الوصول إلى الأجهزة وخوادم الإدارة الافتراضية وخوادم الإدارة الثانوية.

- تعيين نقاط التوزيع

عند بناء بنية مجموعات الإدارة، يجب عليك الأخذ في الاعتبار مخطط شبكة المؤسسة للتعيين الأمثل لنقاط التوزيع. يتيح التوزيع المثالي لنقاط التوزيع توفير الحركة على شبكة المؤسسة.

بناءً على المخطط المؤسسي ومخطط الشبكة، يمكن تطبيق التكوينات القياسية التالية على بنية مجموعات الإدارة:

- مكتب واحد

- مكاتب صغيرة متعددة بعيدة

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

التكوين القياسي لنقاط التوزيع: مكتب واحد

في التكوين القياسي "مكتب واحد"، تكون كل الأجهزة داخل شبكة المؤسسة ويمكنها "رؤية" بعضها البعض. قد تتكون شبكة المؤسسة من عدد قليل من أجزاء منفصلة (الشبكات أو قطاعات الشبكة) التي ترتبط من خلال قنوات ضيقة.

يمكن أن تتوفر الطرق التالية لبناء بنية مجموعات الإدارة:

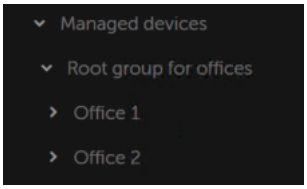
- بناء بنية مجموعات الإدارة مع الأخذ في الاعتبار مخطط الشبكة. قد لا تعكس بنية مجموعات الإدارة مخطط الشبكة بالدقة المطلقة. قد يكون التطابق بين الأجزاء المنفصلة للشبكة ومجموعات الإدارة المحددة كافيًا. يمكنك استخدام التعيين التلقائي لنقاط التوزيع أو تعيينها يدويًا.

- بناء بنية مجموعات الإدارة دون أخذ مخطط الشبكة في الاعتبار. في هذه الحالة، يجب عليك تعطيل التعيين التلقائي لنقاط التوزيع ثم تعيين جهاز واحد أو عدة أجهزة للعمل كنقاط توزيع لمجموعة إدارة الجذر في كل جزء من الأجزاء المنفصلة للشبكة، على سبيل المثال، لمجموعة **الأجهزة المُدارة**. ستكون جميع نقاط التوزيع عند نفس المستوى وستتميز بنفس النطاق لتغطي جميع الأجهزة في شبكة المؤسسة. في هذه الحالة، سيتصل كل من وكيل الشبكة بنقطة التوزيع التي تحتوي على أقصر مسار. يمكن تتبع المسار إلى نقطة توزيع عن طريق الأداة المساعدة tracert.

التكوين القياسي لنقاط التوزيع: مكاتب صغيرة متعددة بعيدة

يقدم هذا التكوين القياسي عدد من المكاتب الصغيرة البعيدة، والتي قد تتصل بالمكتب الرئيسي عبر الإنترنت. كل مكتب بعيد موجود وراء NAT، بمعنى أن الاتصال من مكتب بعيد إلى مكتب آخر غير ممكن لأن الأجهزة معزولة عن بعضها.

يجب أن ينعكس هذا التكوين في بنية مجموعات الإدارة: يجب إنشاء مجموعة إدارة منفصلة لكل مكتب بعيد (المجموعات **المكتب 1** و**المكتب 2** في الشكل الموجود أدناه).



يتم تضمين المكاتب البعيدة في بنية مجموعة الإدارة

يجب تعيين نقطة توزيع واحدة أو عدة نقاط توزيع لكل مجموعة إدارة مقابلة لمكتب ما. يجب أن تكون نقاط التوزيع أجهزة موجودة في المكتب البعيد تحتوي على مساحة قرص خالية كافية. ستتمكن الأجهزة التي تم نشرها في المجموعة **المكتب 1** على سبيل المثال، من الوصول إلى نقاط التوزيع المعينة لمجموعة الإدارة **المكتب 1**.

إذا كان بعض المستخدمين يتنقلون فعليًا بين المكاتب مع أجهزة الكمبيوتر المحمولة الخاصة بهم، فيجب عليك تحديد جهازين أو أكثر (بالإضافة إلى نقاط التوزيع الحاليين) في كل مكتب بعيد وتعيينهم للعمل كنقاط توزيع لمجموعة إدارة من المستوى الأعلى (**المجموعة الجذر للمكاتب** في الشكل الموجود أعلاه).

مثال: جهاز كمبيوتر محمول تم نشره في مجموعة الإدارة **المكتب 1** ثم انتقل فعليًا إلى مكتب مقابل لمجموعة الإدارة **المكتب 2**. بعد انتقال جهاز الكمبيوتر المحمول، يحاول عميل الشبكة الوصول إلى نقاط التوزيع المعينة إلى المجموعة **المكتب 1**، إلا إن هذه النقاط تكون غير متاحة. آنذاك، يحاول عميل الشبكة الوصول إلى نقاط التوزيع التي تم تعيينها إلى **المجموعة الجذر للمكاتب**. ولأن المكاتب البعيدة معزولة عن بعضها، فإن محاولات الوصول إلى نقاط التوزيع المعينة إلى مجموعة الإدارة **المجموعة الجذر للمكاتب** لن تكون ناجحة إلا عند محاولة عميل الشبكة الوصول إلى نقاط التوزيع في مجموعة **المكتب 2**. بمعنى أن جهاز الكمبيوتر المحمول سيظل في مجموعة الإدارة المقابلة للمكتب الأولي، ولكن جهاز الكمبيوتر المحمول سيستخدم نقطة التوزيع الخاصة بالمكتب الذي يوجد فيه فعليًا في الوقت الحالي.

حساب عدد نقاط التوزيع وتكوينهم

كلما زاد عدد الأجهزة العميلة التي تحتوي عليها الشبكة، زاد عدد نقاط التوزيع المطلوبة بالنسبة لها. لا نوصي بتعطيل التعيين التلقائي لنقاط التوزيع. عند تمكين التعيين التلقائي لنقاط التوزيع، يقوم خادم الإدارة بتعيين نقاط التوزيع إذا كان عدد الأجهزة العميلة كبيرًا إلى حد ما ويقوم بتحديد تكوينهم.

استخدام نقاط التوزيع المعينة بشكل حصري

إذا كنت تخطط لاستخدام أجهزة محددة كنقاط توزيع (أي الخوادم المخصصة حصريًا)، فيمكنك إلغاء الاشتراك من استخدام التعيين التلقائي لنقاط التوزيع. وفي هذه الحالة، تأكد من أن الأجهزة التي تنوي تعيينها كنقاط توزيع تحتوي على حجم كافٍ من مساحة القرص الفارغة ولا يتم إيقاف تشغيلها بانتظام وتم تعطيل وضع السكون بها.

عدد نقاط التوزيع التي تم تعيينها حصريًا في شبكة تحتوي على مقطع شبكة واحد بناءً على عدد الأجهزة المتصلة بالشبكة

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

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

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

استخدام الأجهزة العميلة القياسية (محطات العمل) كنقاط توزيع

إذا كنت تخطط لاستخدام أجهزة عميلة قياسية (أي محطات العمل) كنقاط توزيع، فنوصيك بتعيين نقاط التوزيع كما هو موضح في الجداول أدناه لتجنب التحميل الزائد على قنوات الاتصال وخادم الإدارة:

عدد محطات العمل التي تعمل كنقاط توزيع في شبكة تحتوي على مقطع شبكة واحد بناءً على عدد الأجهزة المتصلة بالشبكة

عدد الأجهزة العميلة في مقطع الشبكة	عدد نقاط التوزيع
أقل من 300	0 (لا تقم بتعيين نقاط توزيع)
أكثر من 300	(1 + N/300)، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل

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

عدد الأجهزة العملية لكل مقطع شبكة	عدد نقاط التوزيع
أقل من 10	0 (لا تقم بتعيين نقاط توزيع)
10–30	1
31–300	2
أكثر من 300	(1 + N/300)، حيث N هو عدد الأجهزة المتصلة بالشبكة؛ يجب أن يوجد 3 نقاط توزيع على الأقل

في حالة إيقاف تشغيل نقطة توزيع (أو عدم توفرها لسبب آخر)، يمكن للأجهزة المُدارة الموجودة في نطاقها الوصول إلى خادم الإدارة للحصول على تحديثات.

تعيين نقاط التوزيع تلقائيًا

نوصي بقيامك بتعيين نقاط التوزيع تلقائيًا. في هذه الحالة، سيحدد Kaspersky Security Center Linux 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 Linux تعيين أجهزة للعمل كنقاط توزيع.

نوصي بقيامك بتعيين نقاط التوزيع تلقائيًا. في هذه الحالة، سيحدد Kaspersky Security Center Linux بنفسه الأجهزة التي سيتم تعيين نقاط التوزيع لها. ولكن، إذا كان يتعين عليك إلغاء الاشتراك في تعيين نقاط التوزيع تلقائيًا لأي سبب (على سبيل المثال، إذا كنت ترغب في استخدام خوادم معيّنة حصريًا) فيمكنك تعيين نقاط التوزيع يدويًا بعد قيامك بحساب عددهم وتكوينهم.

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

لتعيين جهاز للعمل كنقطة توزيع يدويًا:

1. في 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 على زر **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 **موافق**.
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 القسم **عام** على إعدادات تفاعل نقطة التوزيع مع الأجهزة العميلة.

- **رقم 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 Linux تلقائيًا بتعيين عنوان IP متعدد الإرسال فريد ضمن النطاق المحدد.

- **رقم منفذ الإرسال المتعدد IP**

رقم منفذ الإرسال المتعدد لعنوان IP.

رقم المنفذ هو 15001 بشكل افتراضي. في حالة تحديد الجهاز المثبت عليه خادم الإدارة كنقطة التوزيع، فسيتم بشكل افتراضي استخدام المنفذ 13001 لاتصال SSL.

- **نشر التحديثات**

يتم توزيع التحديثات على الأجهزة المدارة من المصادر التالية:

- نقطة التوزيع هذه، إذا تم تمكين هذا الخيار.
- نقاط التوزيع الأخرى أو خادم الإدارة أو خوادم تحديث Kaspersky، إذا تم تعطيل هذا الخيار.

إذا كنت تستخدم نقاط التوزيع لنشر التحديثات، فيمكنك حفظ حركة المرور لأنك تقلل عدد التنزيلات. يمكنك أيضًا تخفيف الحمل على خادم الإدارة ونقل الحمل بين نقاط التوزيع. يمكنك حساب عدد نقاط التوزيع لشبكتك لتحسين حركة البيانات والتحميل.

إذا قمت بتعطيل هذا الخيار، فقد يزيد عدد تنزيلات التحديث وتحميلها على خادم الإدارة. يتم تمكين هذا الخيار افتراضيًا.

- **نشر حزم التثبيت**

يتم توزيع حزم التثبيت على الأجهزة المُدارة من المصادر التالية:

- نقطة التوزيع هذه، إذا تم تمكين هذا الخيار.
- نقاط التوزيع الأخرى أو خادم الإدارة أو خوادم تحديث Kaspersky، إذا تم تعطيل هذا الخيار.

إذا كنت تستخدم نقاط التوزيع لنشر حزم التثبيت، فيمكنك توفير حركة البيانات لأنك تقلل عدد التنزيلات. يمكنك أيضًا تخفيف الحمل على خادم الإدارة ونقل الحمل بين نقاط التوزيع. يمكنك حساب عدد نقاط التوزيع لشبكتك لتحسين حركة البيانات والتحميل.

إذا قمت بتعطيل هذا الخيار، فقد يزيد عدد تنزيلات حزمة التثبيت وتحميلها على خادم الإدارة. يتم تمكين هذا الخيار افتراضيًا.

- في قسم **النطاق**، حدد مجموعات الإدارة التي ستقوم نقطة التوزيع بتوزيع التحديثات عليها.
- 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 تنزيل التحديثات إلى مستودعات نقاط التوزيع:
  - إذا كانت هذه المهمة موجودة بالفعل على الجهاز، فحدد المهمة من القائمة.
  - في حالة عدم وجود مثل هذه المهمة حتى الآن على الجهاز، انقر فوق الرابط **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.

- قم بتكوين استقصاء نطاقات IP بنقطة التوزيع.

- **نطاقات IP**

يمكنك تمكين اكتشاف الجهاز لنطاقات IPv4 وشبكات IPv6.

إذا مكنت خيار **تمكين استقصاء النطاق** ، فيمكنك إضافة نطاقات ممسوحة ضوئيًا وتعيين الجدول الزمني لها. يمكنك إضافة نطاقات IP لقائمة النطاقات التي تم فحصها.

إذا مكنت خيار **تمكين الاستقصاء باستخدام تقنية شبكة لا تتطلب تكوينًا** فستقوم نقطة التوزيع تلقائيًا باستقصاء شبكة IPv6 باستخدام شبكات التكوين الصفري (وكما يشار إليها باسم شبكة لا تتطلب تكوينًا). 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. انتقل إلى **الأجهزة** ← **المجموعات** .
2. في بنية مجموعة الإدارة، حدد مجموعة الإدارة التي ترغب في عرض نقاط التوزيع بها.
3. انقر على علامة تبويب **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.

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 **عدم قطع الاتصال بخادم الإدارة** على الأجهزة المدارة أو إرسال الحزم إلى منفذ UDP الخاص بعميل 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**، مكّن 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**.

يتم تمكين خادم الإرسال على نقطة التوزيع المحددة.

إدارة تطبيقات الجهات الخارجية على أجهزة العميل

يصف هذا القسم مزايا Kaspersky Security Center Linux المتعلقة بإدارة تطبيقات الأطراف الخارجية المثبتة 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.

مكون التحكم في التطبيقات متوفر لتطبيق Kaspersky Endpoint Security 11.2 for Linux والإصدارات الأحدث.

المتطلبات الأساسية

- يتم نشر Kaspersky Security Center Linux في مؤسستك.
- تم إنشاء سياسة Kaspersky Endpoint Security for Linux ونشطة.

المراحل

يسير سيناريو استخدام التحكم في التطبيقات في مراحل:

1. **تشكيل قائمة الملفات التنفيذية على أجهزة العميل وعرضها**

   تساعدك هذه المرحلة في معرفة الملفات التنفيذية الموجودة على الأجهزة المُدارة. اعرض قائمة الملفات التنفيذية وقارنها بقوائم الملفات التنفيذية المسموح بها والمحظورة. يمكن أن تكون القيود المفروضة على استخدام الملفات التنفيذية متعلقة بسياسات أمان المعلومات في مؤسستك. يمكنك تخطي هذه المرحلة إذا كنت تعرف تمامًا الملفات التنفيذية المثبتة على الأجهزة المُدارة.

   تعليمات المساعدة: الحصول على قائمة بالملفات القابلة للتنفيذ المخزنة على أجهزة العميل وعرضها

2. **إنشاء فئات التطبيقات للتطبيقات المستخدمة في مؤسستك**

   قم بتحليل قوائم الملفات 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.

   تعليمات المساعدة: إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا

3. **تكوين التحكم في التطبيق في سياسة Kaspersky Endpoint Security for Linux**

   تكوين مكون التحكم في التطبيقات في سياسة Kaspersky Endpoint Security for Linuxباستخدام فئات التطبيق التي قد أنشأتها في المرحلة السابقة.

4. **التحقق من تكوين التحكم في التطبيقات**

   تأكد من أنك قد قمت بما يلي:

   - إنشاء فئات التطبيقات.
   - قم بتكوين التحكم في التطبيقات باستخدام فئات التطبيقات.

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 لتطبيق Kaspersky Endpoint Security for Linux.

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 لتطبيق Kaspersky Endpoint Security 11.2 for Linux والإصدارات الأحدث.

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. في Kaspersky Security Center Linux، لا يمكنك إنشاء إلا فئات بمحتوى مضاف يدويًا. أنت تضع الشروط، مثل بيانات تعريف الملف وكود التجزئة للملف وشهادة الملف وفئة KL ومسار الملف كي تشمل الملفات التنفيذية في الفئة.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى التعليمات عبر الإنترنت لتطبيق Kaspersky Endpoint Security for Linux.

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.

ميزة جرد الملفات التنفيذية متوفرة لتطبيق Kaspersky Endpoint Security 11.2 for Linux والإصدارات الأحدث.

لإنشاء مهمة مخزون للملفات التنفيذية على الأجهزة العميلة:

1. انتقل إلى **الأجهزة** ← **المهام**.

   يتم عرض قائمة المهام.

2. انقر على زر **إضافة**.

   سيبدأ معالج المهمة الجديدة. اتبع خطوات المعالج.

3. في صفحة **مهمة جديدة** من القائمة المنسدلة **التطبيق**، حدد Kaspersky Endpoint Security for Linux.

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 التيتم إنشاؤها في قائمة المهام.

لمعرفة وصف تفصيلي لمهمة الجرد، يُرجى الرجوع إلى التعليمات عبر الإنترنت لتطبيق Kaspersky Endpoint Security.

بعد إجراء مهمة **المخزون**، يتم تشكيل قائمة الملفات التنفيذية المخزنة على الأجهزة المُدارة، ويمكنك عرض القائمة.

أثناء الجرد، يتم اكتشاف الملفات التنفيذية بالامتدادات التالية: MZ وCOM وPE وNE وSYS وCMD, BAT وPS1 وJS وVBS وREG وMSI وCPL وDLL وJAR وHTML.

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.

إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا

يمكنك تحديد مجموعة من المعايير كقالب للملفات التنفيذية التي ترغب في السماح ببدئها أو حظرها في مؤسستك. على أساس الملفات التنفيذية التي تستوفي المعايير، يمكنك إنشاء فئة تطبيق واستخدامها في تكوين مكون التحكم في التطبيقات.

لإنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا:

1. في **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. اتبع خطوات المعالج.
3. في صفحة **تحديد طريقة إنشاء الفئة** من المعالج، حدد خيار **فئة ذات محتوى مضاف يدويًا. تتم إضافة بيانات الملفات التنفيذية يدويًا إلى الفئة**.
4. في صفحة **الشروط**في المعالج، انقر على زر **إضافة** لإضافة معيار شرط لإدراج الملفات في فئة الإنشاء.
5. في صفحة **معيار الشرط**، حدد نوع قاعدة لإنشاء فئة من القائمة:

- **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.

- **تحديد المسار إلى تطبيق (يدعم الأقنعة)**

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 Linux 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 for Linux حوسبة SHA-256.

  حدد أيًا من خيارات حساب قيمة التجزئة بواسطة Kaspersky Security Center Linux للملفات الموجودة في الفئة:

  - إذا كانت جميع مثيلات تطبيقات الأمان المثبتة على شبكتك هي Kaspersky Endpoint Security for Linux، فحدد خانة الاختيار **SHA-256** .
  - حدد خانة اختيار **تجزئة MD5** فقط إذا كنت تستخدم Kaspersky Endpoint Security for Windows. لا يدعم Kaspersky Endpoint Security for Linux وظيفة تجزئة MD5.

  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. ستتم إضافة الملفات التنفيذية التي تحتوي على نفس بيانات التعريف إلى فئة التطبيق.

  الشهادة

  إذا تم تحديد هذا الخيار، فيمكنك تحديد الشهادات من وحدة التخزين. ستتم إضافة الملفات التنفيذية التي تم توقيعها وفقًا للشهادات المحددة إلى فئة المستخدم.

- **من المجلد المؤرشف**

في حال تحديد هذا الخيار، يمكنك تحديد ملف في مجلد مضغوط، ثم تحديد الشرط الذي ترغب في استخدامه لإضافة الأوصاف إلى فئة المستخدم. المجلد المؤرشف غير مفكوك الضغط، والشروط التي تحددها تُطبق إلى الملفات في المجلد. كشرط، يمكنك تحديد أي من المعايير التالية:

- **تجزئة الملف**

  أنت تحدد وظيفة التجزئة (MD5 أو SHA-256) التي ترغب في استخدامها في حساب قيم التجزئة. تتم إضافة التطبيقات التي لها نفس قيمة تجزئة الملفات الموجودة في المجلد المؤرشف إلى فئة تطبيقات المستخدم.

  حدد وظيفة تجزئة MD5 فقط إذا كنت تستخدم Kaspersky Endpoint Security for Windows. لا يدعم Kaspersky Endpoint Security for Linux وظيفة تجزئة MD5.

- **بيانات وصفية**

  أنت تحدد البيانات الوصفية التي ترغب في استخدامها كمعايير. ستتم إضافة الملفات التنفيذية التي تحتوي على نفس البيانات الوصفية إلى فئة تطبيقات المستخدم.

- **الشهادة**

  أنت تحدد خصائص الشهادة (موضوع الشهادة أو بصمة الإصبع أو الجهة المصدرة) التي ترغب في استخدامها كمعايير. سيتم إضافة الملفات التنفيذية التي تم توقيعها مع الشهادات التي لها نفس الخصائص إلى فئة 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.

لمعرفة معلومات تفصيلية عن التحكم في التطبيقات، يمكنك الرجوع إلى التعليمات عبر الإنترنت لتطبيق Kaspersky Endpoint Security for Linux.

عرض قائمة فئات التطبيق

يمكنك عرض قائمة فئات التطبيقات التي تم إنشاؤها وإعدادات كل فئة تطبيق.

لعرض قائمة فئات التطبيقات،

في علامة التبويب **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.

إضافة الملفات التنفيذية المتعلقة بالأحداث إلى فئة التطبيق

بعد أن تقوم بتكوين التحكم في التطبيقات في سياسات Kaspersky Endpoint Security for Linux، 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. 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**

       حدد هذا الخيار إذا كنت ترغب في إنشاء فئة تطبيق جديدة بناءً على الملفات التنفيذية ذات الصلة بالحدث.
       يتم تحديد هذا الخيار افتراضيًا.
       إذا كنت قد حددت هذا الخيار، حدد اسم فئة جديدة.

     - **إضافة إلى فئة تطبيق حالي**

       حدد هذا الخيار إذا كنت ترغب في إضافة ملفات تنفيذية متعلقة بالحدث إلى فئة تطبيق موجودة.
       لا يتم تحديد هذا الخيار افتراضيًا.
       إذا كنت قد حددت هذا الخيار، حدد فئة التطبيق المضاف إليها المحتوى يدويًا الت ترغب في إضافة ملفات تنفيذية إليها.

   - في قسم **نوع القاعدة**، حدد أحد الخيارات التالية:
     - **قواعد الإضافة إلى التضمينات**
     - **قواعد الإضافة إلى الاستثناءات**

- في قسم **المعلمة المستخدمة كشرط**، حدد أحد الخيارات التالية:

- **تفاصيل الشهادة (أو تجزئات SHA-256 للملفات التي لا تحتوي على 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)**

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)**

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 المتوقف، لإصدار Kaspersky Endpoint Security 10 Service Pack 1 فقط)**

حدد هذا الخيار فقط إذا كنت تستخدم Kaspersky Endpoint Security for Windows. لا يدعم Kaspersky Endpoint Security for Linux وظيفة تجزئة MD5.

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.

5. انقر فوق **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 لتطبيق Kaspersky Endpoint Security for Linux.

المراقبة وإعداد التقارير

يوضح هذا القسم إمكانيات المراقبة وإعداد التقارير في Kaspersky Security Center Linux. تمنحك هذه الإمكانيات نظرة عامة على البنية الأساسية الخاصة بك وحالات الحماية والإحصائيات.

بعد نشر Kaspersky Security Center Linux أو أثناء العملية، يمكنك تكوين مزايا المراقبة وإعداد التقارير لتتناسب مع احتياجاتك بشكل أفضل.

السيناريو: المراقبة وإعداد التقارير

يعرض هذا القسم سيناريو لتكوين ميزة المراقبة وإعداد التقارير في Kaspersky Security Center Linux.

المتطلبات الأساسية

بعد أن تنشر Kaspersky Security Center Linux في شبكة مؤسسة، يمكنك بدء مراقبته وإنشاء تقارير عن عمله.

المراقبة وإعداد التقارير في شبكة مؤسسة تسير في مراحل:

1. **تكوين تبديل حالات الجهاز**

   تعرَّف على إعدادات حالات الجهاز اعتمادًا على الظروف. يمكنك عن طريق تغيير هذه الإعدادات تغيير عدد الأحداث ذات مستويات الأهمية حرج أو تحذيري. عند تكوين تبديل حالات الجهاز، تأكد مما يلي:

   - الإعدادات الجديدة لا تخالف سياسات أمان المعلومات لمؤسستك.
   - أنت تقدر على التفاعل مع أحداث الأمان المهمة في شبكة مؤسستك في الوقت المناسب.

2. **تكوين إخطارات الأحداث التي تحدث على أجهزة العميل:**

   تعليمات للمساعدة:

   قم بتكوين الإخطار (عن طريق البريد الإلكتروني أو الرسائل النصية القصيرة أو عن طريق تشغيل ملف تنفيذي) للأحداث على أجهزة العميل.

3. **اتخاذ الإجراءات الموصى بها للإخطارات الحرجة والتحذيرية**

   تعليمات للمساعدة:

   اتخاذ الإجراءات الموصى بها لشبكة مؤسستك

4. **مراجعة حالة الأمان لشبكة مؤسستك**

   تعليمات للمساعدة:

   - راجع عنصر الواجهة حالة الحماية
   - قم بإنشاء ومراجعة تقرير عن حالة الحماية
   - قم بإنشاء ومراجعة تقرير الأخطاء

5. **تحديد مواقع أجهزة العميل غير المحمية**

   تعليمات للمساعدة:

- مراجعة عنصر واجهة المستخدمأجهزة جديدة
- قم بإنشاء ومراجعة تقرير نشر الحماية

6 **التحقق من حماية أجهزة العميل**

تعليمات للمساعدة:

- إنشاء التقارير ومراجعتها من فئتي حالة الحماية وإحصائيات التهديد
- بدء تحديد الحدث حرج ومراجعته

7 **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:

- وضع حد للعدد الأقصى من الأحداث

8 **مراجعة معلومات الترخيص**

تعليمات للمساعدة:

- أضف عنصر الواجهة استخدام المفتاح إلى جزء المعلومات وراجعه.
- 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 14 Web Console الأنواع التالية من المراقبة وإعداد التقارير في شبكة مؤسستك:

- لوحة القيادة
- تقارير
- مجموعات الأحداث المحددة
- الإشعارات

لوحة القيادة

يتيح لك جزء المعلومات مراقبة اتجاهات الأمان في شبكة مؤسستك من خلال تزويدك بعرض رسومي للمعلومات.

تقارير

تسمح لك ميزة التقارير بالحصول على معلومات رقمية تفصيلية حول أمان شبكة مؤسستك وحفظ هذه المعلومات إلى أحد الملفات وإرسالها بالبريد الإلكتروني وطباعتها.

مجموعات الأحداث المحددة

توفر تحديدات الأحداث عرضًا على الشاشة يتضمن مجموعات الأحداث المُسمَّاة المحددة من قاعدة بيانات خادم الإدارة. يتم تجميع مجموعات الأحداث هذه وفقًا للفئات التالية:

- حسب مستوى الأهمية—**أحداث حرجة**، و**حالات الخلل الوظيفي**، و**تحذيرات**، و**معلومات عن الأحداث**
- حسب الوقت—**الأحداث الأخيرة**
- حسب النوع—**طلبات المستخدم** و**أحداث التدقيق**

يمكنك إنشاء أقسام الأحداث المحددة من قبل المستخدم بناءً على الإعدادات المتوفرة بغرض تكوينها في واجهة Kaspersky Security Center 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**
- **جارٍ التحديث**
- **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 لاحقًا إضافة عنصر الواجهة هذا إلى جزء المعلومات مرة أخرى.

تحريك عنصر واجهة مستخدم على لوحة القيادة

لنقل عنصر واجهة إلى جزء المعلومات:

1. في القائمة الرئيسية، انتقل إلى **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 رسمًا بيانيًا، يمكنك تغيير تمثيلها إلى مخطط شريطي أو مخطط خطي. يمكنك لبعض عناصر الواجهة تغيير حجمها: صغير أو متوسط أو كبير.

لتغير تمثيل عنصر الواجهة:

1. في القائمة الرئيسية، انتقل إلى **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** و**تعيين 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: أذونات المستخدم**.

جارٍ تكوين وضع لوحة المعلومات فقط

قبل بدء تكوين وضع لوحة المعلومات فقط، تأكد من استيفاء المتطلبات الأساسية التالية:

- لديك حق **تعديل قوائم التحكم في الوصول للكائن** مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**. إذا لم يكن لديك هذا الحق، فستكون علامة التبويب الخاصة بتكوين الوضع مخفية.
- يكون للمستخدم حق **القراءة** في المجال الوظيفي **الميزات العامة: الوظائف الأساسية**.

في حالة ترتيب تسلسل هرمي لخوادم الإدارة في شبكتك، لتكوين وضع لوحة المعلومات فقط، انتقل إلى الخادم حيث يتوفر حساب المستخدم في 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 أبقيت الخيار معطلاً، فستُعرض القائمة الرئيسية للمستخدم، حتى يتمكن من تنفيذ إجراءات مختلفة في Kaspersky Security Center، بما في ذلك تغيير إعدادات الأمان والتطبيقات المصغرة.

7. انقر فوق الزر **حفظ** عند الانتهاء من تكوين وضع لوحة المعلومات فقط. وبعد ذلك ستُعرض فقط لوحة المعلومات المعدة مسبقًا للمستخدم.

8. إذا أراد المستخدم عرض إحصائيات تطبيقات Kaspersky المدعومة ويحتاج إلى حقوق الوصول للقيام بذلك، عليك تكوين حقوق الوصول للمستخدم. بعد ذلك، تُعرض بيانات تطبيقات Kaspersky للمستخدم في التطبيقات المصغرة هذه.

يمكن الآن للمستخدم تسجيل الدخول إلى Kaspersky Security Center ضمن الحساب المخصص ومراقبة إحصائيات حماية الشبكة في وضع لوحة المعلومات فقط.

تقارير

يصف هذا القسم كيفية استخدام التقارير وإدارة قوالب التقارير المخصصة واستخدام قوالب التقارير لإنشاء تقارير جديدة وإنشاء مهام تسليم التقارير.

استخدام التقارير

تسمح لك ميزة التقارير بالحصول على معلومات رقمية تفصيلية حول أمان شبكة مؤسستك وحفظ هذه المعلومات إلى أحد الملفات وإرسالها بالبريد الإلكتروني وطباعتها.

تتوفر التقارير في Kaspersky Security Center 14 Web Console في قسم **المراقبة والإبلاغ** عن طريق النقر على **التقارير**.

بشكل افتراضي، التقارير تشمل معلومات لآخر 30 يومًا.

Kaspersky Security Center Linux به مجموعة افتراضية من التقارير للفئات التالية:

- **حالة الحماية**
- **النشر**
- **جارٍ التحديث**
- **إحصائيات التهديد**

- **غير ذلك**

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 على **إضافة**.
   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** .

ستفتح 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**

إذا تم تمكين هذا الخيار، فإن عدد الإدخالات المعروضة في الجدول مع بيانات التقرير التفصيلية لا يزيد عن القيمة المحددة.

يتم أولاً فرز إدخالات التقرير وفقًا للقواعد المحددة في القسم **الحقول** ← **حقول التفاصيل** في خصائص قالب التقرير، وبعد ذلك يتم الاحتفاظ فقط بالإدخالات الأولى الناتجة. يعرض عنوان الجدول المزود ببيانات تقرير مفصلة العدد المعروض من الإدخالات وإجمالي عدد الإدخالات المتاح الذي يطابق إعدادات قالب التقرير الآخر.

إذا تم تعطيل هذا الخيار، فإن الجدول المزود ببيانات التقرير التفصيلية يعرض جميع الإدخالات المتوفرة. لا نوصيك بتعطيل هذا الخيار. إن تقليل عدد إدخالات التقرير المعروضة يقلل من الحمل على نظام إدارة قواعد البيانات (DBMS) ويقلل الوقت اللازم لإنشاء وتصدير التقرير. تحتوي بعض التقارير على عدد كبير جدًا من الإدخالات. إذا كانت هذه هي الحالة، فقد تجد صعوبة في قراءتها وتحليلها جميعًا. وقد تنفذ مساحة الذاكرة في جهازك أيضًا أثناء إنشاء مثل هذا التقرير، وبالتالي لن تتمكن من عرض التقرير.

يتم تمكين هذا الخيار افتراضيًا. القيمة الافتراضية هي 1000.

- **مجموعة**

انقر على زر **إعدادات** لتغيير مجموعة أجهزة العميل التي تم إنشاء التقرير من أجلها. قد لا يكون هذا الزر متاحًا لبعض أنواع التقارير. الإعدادات الفعلية تعتمد على الإعدادات المحددة أثناء إنشاء قالب القرير.

- **الفاصل الزمني**

انقر على زر **إعدادات** لتعديل فترة التقرير. قد لا يكون هذا الزر متاحًا لبعض أنواع التقارير. القيم المتاحة هي كما يلي:

- بين تاريخين محددين

- من التاريخ المحدد إلى تاريخ إنشاء التقرير

- من تاريخ إنشاء التقرير، ناقص العدد المحدد من الأيام، إلى تاريخ إنشاء التقرير

- **تضمين بيانات من خوادم الإدارة الثانوية والافتراضية**

إذا تم تمكين هذا الخيار، فإن التقرير يقوم بتضمين معلومات من خوادم الإدارة الثانوية والظاهرية التابعة الخاضعة لخادم الإدارة الذي يتم إنشاء قالب التقرير له.

قم بتعطيل هذا الخيار إذا كنت ترغب في عرض البيانات فقط من خادم الإدارة الحالي.

يتم تمكين هذا الخيار افتراضيًا.

- **أعلى إلى مستوى التداخل**

يتضمن التقرير بيانات من خوادم الإدارة الثانوية والظاهرية الموجودة ضمن خادم الإدارة الحالي على مستوى تداخل أقل من أو يساوي القيمة المحددة.

القيمة الافتراضية هي 1. قد ترغب في تغيير هذه القيمة إذا كان عليك استعادة المعلومات من خوادم الإدارة الثانوية الموجودة في المستويات الأدنى في الشجرة.

- **فاصل انتظار البيانات (بالدقائق)**

قبل إنشاء التقرير، ينتظر خادم الإدارة الذي يتم إنشاء قالب التقرير له البيانات من خوادم الإدارة الثانوية خلال العدد المحدد من الدقائق. إذا لم يتم تلقي أي بيانات من خادم الإدارة الثانوي في نهاية هذه الفترة، فسيتم تشغيل التقرير على أي حال. بدلاً من البيانات الفعلية، 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 (ثوانٍ).

- **بيانات ذاكرة التخزين المؤقت من خوادم الإدارة الثانوية**

تقوم خوادم الإدارة الثانوية بنقل البيانات إلى خادم الإدارة الذي يتم من أجله إنشاء قالب التقرير بانتظام. وهناك يتم تخزين البيانات المنقولة في ذاكرة التخزين المؤقت.

إذا لم يتمكن خادم الإدارة الحالي من تلقي البيانات من خادم الإدارة الثانوي أثناء إنشاء التقرير، فسيعرض التقرير البيانات المأخوذة من ذاكرة التخزين المؤقت. يتم أيضًا عرض التاريخ الذي تم فيه نقل البيانات إلى ذاكرة التخزين المؤقت.

يتيح لك تمكين هذا الخيار عرض المعلومات من خوادم الإدارة الثانوية حتى إذا تعذر استرجاع البيانات الحديثة. ومع ذلك، يمكن أن تكون البيانات المعروضة قديمة.

يتم تعطيل هذا الخيار افتراضيًا.

- **تكرار تحديث التخزين المؤقت (بالساعات)**

تقوم خوادم الإدارة الثانوية بنقل البيانات إلى خادم الإدارة الذي يتم من أجله إنشاء قالب التقرير على فترات منتظمة. يمكنك تحديد هذه الفترة بالساعات. إذا حددت 0 ساعات، لا يتم نقل البيانات إلا عند إنشاء التقرير.

القيمة الافتراضية هي 0.

- **نقل معلومات تفصيلية من خوادم الإدارة الثانوية**

في التقرير الذي يتم إنشاؤه، يشتمل الجدول المزود ببيانات التقرير التفصيلية على بيانات من خوادم الإدارة الثانوية لخادم الإدارة الذي يتم من أجله إنشاء قالب التقرير.

يؤدي تمكين هذا الخيار إلى إبطاء إنشاء التقرير وزيادة حركة المرور بين خوادم الإدارة. ومع ذلك، يمكنك عرض جميع البيانات في تقرير واحد.

بدلاً من تمكين هذا الخيار، قد تحتاج إلى تحليل بيانات التقرير التفصيلية للكشف عن خادم إدارة تابع معيب، ثم إنشاء نفس التقرير فقط لخادم الإدارة المعيب هذا.

يتم تعطيل هذا الخيار افتراضيًا.

- 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 **تحرير** في تحديد إذا ما كانت المعلومات في التقرير يجب أن تبقى مرتبة ومفلترة لكل من الحقول.

في قسم **عوامل تصفية حقول التفاصيل**، يمكنك أيضًا 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). أيضًا لن يحتوي التقرير المحول 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** (×) 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.

لتصدير تقرير إلى ملف:

1. انتقل إلى **المراقبة والإبلاغ** ← **التقارير**.

2. حدد خانة الاختيار الموجودة بجوار التقرير الذي ترغب في تصديره إلى ملف.

3. انقر على زر **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.

أداة wkhtmltopdf مطلوبة لتحويل تقرير إلى PDF. عند تحديد خيار صيغة PDF، يتحقق خادم الإدارة من تثبيت أداة wkhtmltopdf على الجهاز. إذا لم يتم تثبيت الأداة، فسيعرض التطبيق رسالة حول ضرورة تثبيت الأداة على جهاز خادم الإدارة. ثبّت الأداة يدويًا، ثم انتقل إلى الخطوة التالية.

6. انقر على زر **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 تمثيلًا.
- 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. انتقل إلى **المراقبة والإبلاغ** ← **التقارير**.

2. [اختياري] حدد خانات الاختيار الموجودة بجوار قوالب التقارير التي ترغب في إنشاء مهمة تسليم تقرير لها.

3. انقر فوق الزر **مهمة تسليم تقرير جديد** .

4. يبدأ معالج المهمة الجديدة. 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.

   أداة wkhtmltopdf مطلوبة لتحويل تقرير إلى PDF. عند تحديد خيار صيغة PDF، يتحقق خادم الإدارة من تثبيت أداة wkhtmltopdf على الجهاز. إذا لم يتم تثبيت الأداة، فسيعرض التطبيق رسالة حول ضرورة تثبيت الأداة على جهاز خادم الإدارة. ثبّت الأداة يدويًا، ثم انتقل إلى الخطوة التالية.

   c. سواء كان سيتم إرسال التقارير عبر البريد الإلكتروني أو مع إعدادات الإخطار بالبريد الإلكتروني.

   d. سواء كان سيتم حفظ التقارير إلى مجلد، وسواء إذا ما كان سيتم استبدال تقارير محفوظة مسبقًا في هذا المجلد، وسواء إذا ما كان سيتم استخدام حساب معين للوصول إلى المجلد (لمجلد مشترك).

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 وغلق 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 خانات الاختيار الموجودة بجوار قوالب التقارير التي ترغب في حذفها.

3. انقر على زر **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 Linux، 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**، و**حالات الخلل الوظيفي**، و**تحذيرات**، و**معلومات عن الأحداث**
- حسب الوقت—**الأحداث الأخيرة**
- حسب النوع—**طلبات المستخدم** و**أحداث التدقيق**

يمكنك إنشاء أقسام الأحداث المحددة من قبل المستخدم بناءً على الإعدادات المتوفرة بغرض تكوينها في واجهة Kaspersky Security Center 14 Web Console.

تتوفر تحديدات الأحدث 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.

يحتوي Kaspersky Security Center Linux على 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).

لكلٍ من التحديثات المحددة مسبقًا والتي يحددها المستخدم، يمكنك وضع حدٍ لعدد الأحداث المعروضة أو عدد السجلات التي سيتم البحث عنها. يؤثر الخياران على الوقت الذي يستغرقه Kaspersky Security Center Linux 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 على **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 مسبقًا، لا يمكنك إلا تحرير خصائص علامات التبويب التالية: **عام** (باستثناء اسم التحديد) و**الوقت** و**حقوق 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.
   تفتح 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 خانات الاختيار الموجودة بجوار الأحداث المطلوبة.
3. انقر على زر **حذف**.

يتم حذف الأحداث المحددة ولا يمكن استردادها.

حذف تحديدات الحدث

لا يمكنك حذف إلا تحديدات الأحداث من تحديد المستخدم. لا يمكن حذف تحديدات الأحداث المحددة مسبقًا.

لحذف تحديد حدث أو عدة تحديدات:

1. في القائمة الرئيسية، انتقل إلى **المراقبة والإبلاغ** ← **تحديدات الأحداث**.

2. حدد خانات الاختيار الموجودة بجوار تحديدات الحدث التي ترغب في حذفها.

3. انقر على **حذف**.

4. في النافذة التي يتم فتحها، انقر على **موافق**.

يتم حذف تحديد الحدث.

تعيين مدة التخزين لحدث

يتيح لك Kaspersky Security Center Linux تلقي معلومات عن الأحداث التي تقع أثناء تشغيل خادم الإدارة وتطبيقات Kaspersky المثبتة على الأجهزة المُدارة. يتم حفظ المعلومات حول الأحداث في قاعدة بيانات خادم الإدارة. قد تحتاج إلى تخزين بعض الأحداث لفترة أطول أو أقصر من تلك التي حددتها القيم الافتراضية. يمكنك تغيير الإعدادات الافتراضية لمدّة التخزين لحدث.

إذا لم تكن مهتمًا بتخزين بعض الأحداث في قاعدة بيانات خادم الإدارة، يمكنك تعطيل الإعداد المسؤول عن ذلك في سياسة خادم الإدارة وسياسة تطبيق Kaspersky أو في خصائص خادم الإدارة (لأحداث خادم الإدارة فقط). سيقلل هذا من عدد أنواع الأحداث في قاعدة البيانات.

لكما زادت مدة تخزين حدث، زادت سرعة وصول قاعدة البيانات إلى أقصى سعة لها. رغم ذلك، 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 علامة تبويب **تكوين الحدث** .
   يتم عرض قائمة بأنواع الأحداث ذات الصلة بقسم **حرج**.

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 Linux، 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 Linux على مجموعة من أنواع الأحداث خاصة به. يسرد هذا القسم أنواع الأحداث التي تحدث في خادم إدارة Kaspersky Security Center Linux ووكيل الشبكة. 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 Linux 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 Linux 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: ضبط مدة التخزين لحدث

أحداث خادم الإدارة

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بخادم الإدارة.

الأحداث الحرجة لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center Linux التي لها 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	يقوم Kaspersky Security Center بالتحقق مما إذا تم تجاوز قيود الترخيص أم لا بمعدل مرة يوميًا. تحدث الأحداث من هذا النوع عند اكتشاف خادم الإدارة حدوث تجاوز لبعض قيود الترخيص بواسطة تطبيقات Kaspersky المثبتة على الأجهزة العميلة وكذلك في حال تجاوز عدد وحدات الترخيص المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد لنسبة 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص. حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا. • تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). يحدد Kaspersky Security Center Linux القواعد المُستخدمة لإنشاء أحداث عند تجاوز تقييد الترخيص.	180 يومًا
أصبح الجهاز غير مُدار	4111	KLSRV_HOST_OUT_CONTROL	تحدث الأحداث من هذا النوع في حالة وجود أي جهاز مُدار مرئيًا على الشبكة، ولكنه غير متصل بخادم الإدارة لفترة زمنية محددة. تعرف على ما يمنع التشغيل السليم لعميل الشبكة على الجهاز. تتضمن الأسباب المحتملة حدوث مشكلات في الشبكة وإزالة عميل الشبكة من الجهاز.	180 يومًا
حالة الجهاز حرج	4113	KLSRV_HOST_STATUS_CRITICAL	تحدث الأحداث من هذا النوع عندما يتم تعيين أي جهاز مُدار للحالة حرج. يمكنك تكوين الشروط التي يتم من خلالها تغيير حالة الجهاز إلى حرجة.	180 يومًا
تمت إضافة ملف المفتاح إلى قائمة الرفض	4124	KLSRV_LICENSE_BLACKLISTED	تقع الأحداث من هذا النوع عندما يضيف برنامج Kaspersky رمز التنشيط أو ملف المفتاح الذي تستخدمه في قائمة الرفض. تواصل مع الدعم الفني للحصول على المزيد من التفاصيل.	180 يومًا
ستنتهي فترة صلاحية الترخيص قريبًا	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	تحدث أحداث من هذا النوع عندما يقترب تاريخ انتهاء صلاحية الترخيص التجاري.	180 يومًا

			يقوم Kaspersky Security Center بالتحقق مما إذا تم تجاوز تاريخ انتهاء صلاحية الترخيص أم لا بمعدل مرة يوميًا. يتم نشر أحداث من هذا النوع قبل 30 يوم و15يوم و 5 أيام ويوم واحد من تاريخ انتهاء صلاحية الترخيص. لا يمكن تغيير هذا العدد من 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 Linux الوظائف الأساسية فقط. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تأكد من إضافة مفتاح ترخيص احتياطي إلى خادم الإدارة. • إذا كنت تستخدم اشتراكًا، فتأكد من تجديده. يتم تجديد الاشتراك غير المحدود تلقائيًا في حالة الدفع المسبق لموفر الخدمة في المواعيد المحددة.		
انتهت صلاحية الشهادة	4132	KLSRV_CERTIFICATE_EXPIRED	تحدث الأحداث من هذا النوع عند انتهاء صلاحية شهادة خادم الإدارة لإدارة الجهاز المحمول. تحتاج إلى تحديث الشهادة منتهية الصلاحية. يمكنك تكوين التحديثات التلقائية للشهادات بتحديد خانة الاختيار **إعادة إصدار الشهادة تلقائيًا إن أمكن** في إعدادات إصدار الشهادة.	180 يومًا

أحداث الخلل الوظيفي الخاصة بخادم الإدارة

يوضح الجدول أدناه أحداث خادم الإدارة Kaspersky Security Center Linux الذي يندرج 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 حال قيامك بإدارة مفاتيح الترخيص لتطبيقات تابعة لجهات خارجية في Kaspersky Security Center وكذلك إذا تجاوز عدد عمليات التثبيت الحد	180 يومًا

			الذي تم تعيينه بواسطة مفتاح الترخيص التابع لجهة خارجية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. قم بحذف التطبيق التابع لجهة خارجية من الأجهزة التي لا يستخدم عليها التطبيق. • قم باستخدام ترخيص تابع لجهة خارجية لعدد أجهزة أكثر. يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المُرخصة. تشتمل مجموعة التطبيقات المرخصة على التطبيقات التي تفي بالمعايير المحددة بواسطتك.		
فشل نسخ التحديثات إلى المجلد المحدد	4123	KLSRV_UPD_REPL_FAIL	تحدث الأحداث من هذا النوع عند القيام بنسخ تحديثات البرنامج إلى مجلد (مجلدات) إضافية مشتركة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا كان يحتوي حساب المستخدم المخصص للحصول على إمكانية الوصول إلى المجلد (المجلدات) على أذن كتابي أم لا. • تحقق مما إذا تم تغيير اسم المستخدم و / أو كلمة المرور الخاصة بالمجلد (المجلدات) أم لا. • تحقق من الاتصال بالإنترنت لأنه قد يكون السبب في حدوث هذا الحدث. اتبع التعليمات للقيام بتحديث قواعد البيانات والوحدات النمطية للبرامج.	180 يومًا
لا توجد مساحة فارغة على القرص	4107	KLSRV_DISK_FULL	تحدث الأحداث من هذا النوع عند نفاد مساحة القرص في الجهاز المثبت عليه خادم الإدارة. قم بتحرير مساحة القرص على الجهاز.	180 يومًا
المجلد المشترك غير متاح	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	تحدث الأحداث من هذا النوع في حال عدم توافر المجلد المشترك لخادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا تم تشغيل خادم الإدارة وتوافره (حيث يوجد المجلد المشترك) أم لا. • تحقق مما إذا تم تغيير اسم المستخدم و / أو كلمة المرور الخاصة بالمجلد أم لا. • تحقق من الاتصال بالشبكة.	180 يومًا

قاعدة بيانات خادم الإدارة غير متوفرة	4109	KLSRV_DATABASE_UNAVAILABLE	تحدث الأحداث من هذا النوع في حال أصبحت قاعدة بيانات خادم الإدارة غير متاحة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • تحقق مما إذا كان الخادم البعيد الذي يحتوي على خادم SQL المثبت متاحًا أم لا. • اعرض سجلات DBMS لمعرفة سبب عدم توافر قاعدة بيانات خادم الإدارة. على سبيل المثال، بسبب الصيانة الوقائية قد يكون الخادم البعيد الذي يحتوي على خادم SQL غير متاح.	180 يومًا
لا توجد مساحة فارغة في قاعدة بيانات خادم الإدارة	4110	KLSRV_DATABASE_FULL	تحدث الأحداث من هذا النوع في حالة عدم توافر مساحة فارغة في قاعدة بيانات خادم الإدارة. لا يقوم خادم الإدارة بإداء وظيفته عند وصول قاعدة البيانات الخاصة به إلى سعته وكذلك عند استحالة إجراء المزيد من التسجيلات في قاعدة البيانات. فيما يلي الأسباب التي أدت إلى هذا الحدث، وفقًا لـDBMS التي تستخدمها، والاستجابات المناسبة للحدث: • إنك تستخدم خادم SQL Server Express Edition DBMS: • في وثيقة SQL Server Express، قم بفحص حد حجم قاعدة البيانات للإصدار الذي تستخدمه. من المحتمل أنه قد تجاوزت قاعدة بيانات خادم الإدارة الخاصة بك حد حجم قاعدة البيانات. • يمكنك تقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. • في قاعدة بيانات خادم الإدارة، توجد أحداث تجاوز عددها الحد الأقصى أرسلها مكون التحكم في التطبيقات. يمكنك تغيير إعدادات سياسة Kaspersky Endpoint Security for Linux المتعلقة بتخزين حدث التحكم في التطبيقات في قاعدة بيانات خادم الإدارة. • إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition: • لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.	180 يومًا

			• 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 Linux 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. تحدث الأحداث من هذا النوع عند اكتشاف خادم الإدارة حدوث تجاوز لبعض قيود الترخيص بواسطة تطبيقات Kaspersky المثبتة على الأجهزة العميلة وكذلك في حال كان عدد وحدات الترخيص المستخدمة حاليًا والمغطاة بواسطة ترخيص منفرد يشكل من 100% إلى 110% من إجمالي عدد الوحدات المغطاة بواسطة الترخيص. حتى عند حدوث هذا الحدث، تكون الأجهزة العميلة محمية. يمكنك الاستجابة للحدث من خلال الطرق التالية: • استعراض قائمة الأجهزة المُدارة. حذف الأجهزة غير المُستخدمة حاليًا. • تقديم ترخيص لعدد أكبر من الأجهزة (إضافة رمز تنشيط صالح أو ملف المفتاح لخادم الإدارة). يحدد Kaspersky Security Center Linux القواعد المُستخدمة لإنشاء أحداث عند تجاوز تقييد الترخيص.	90 يومًا
ظل الجهاز غير نشط على الشبكة لوقت طويل	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	تحدث الأحداث من هذا النوع عندما يظهر الجهاز المُدار عدم النشاط لبعض الوقت. يحدث هذا غالبًا عند إيقاف تشغيل الجهاز المُدار. يمكنك الاستجابة للحدث من خلال الطرق التالية:	90 يومًا

			• إزالة الجهاز من قائمة الأجهزة المدارة تلقائيًا. حدد الفاصل الزمني الذي يتم بعده إنشاء الحدث **ظل الجهاز غير نشط على الشبكة لوقت طويل** باستخدام Kaspersky Security Center 14 Web Console . • حدد الفاصل الزمني الذي يتم بعده إزالة الجهاز تلقائيًا من المجموعة باستخدام Kaspersky Security Center 14 Web Console .	
تعارض في أسماء الجهاز	4102	KLSRV_EVENT_HOSTS_CONFLICT	تحدث الأحداث من هذا النوع عندما يعتبر خادم الإدارة جهازين مُدارين أو أكثر كجهاز واحد. يحدث هذا غالبًا عند استخدام محرك أقراص ثابت مستنسخ لنشر البرامج على الأجهزة المُدارة وبدون تحويل عميل الشبكة إلى وضع استنساخ القرص المخصص على جهاز مرجعي. لتجنب هذه المشكلة، قم بتبديل Network Agent إلى وضع استنساخ القرص على جهاز مرجعي قبل استنساخ محرك الأقراص الثابتة لهذا الجهاز.	90 يومًا
حالة الجهاز 'تحذير'	4114	KLSRV_HOST_STATUS_WARNING	تحدث الأحداث من هذا النوع عندما يتم تعيين الحالة تحذير للجهاز المُدار. يمكنك تكوين الشروط التي يتم من خلالها تغيير حالة الجهاز إلى تحذير.	90 يومًا
سيتم تجاوز حد عمليات التثبيت لإحدى مجموعات التطبيقات المرخصة قريبًا	4127	KLSRV_INVLICPROD_FILLED	تحدث الأحداث من هذا النوع عندما يصل عدد عمليات التثبيت لتطبيقات الطرف الثالث المضمنة في مجموعة التطبيقات المرخصة إلى 90٪ من الحد الأقصى للقيمة المسموح بها المحددة في خصائص مفتاح الترخيص. يمكنك الاستجابة للحدث من خلال الطرق التالية: • إذا لم يكن تطبيق الطرف الثالث قيد الاستخدام على بعض الأجهزة المدارة، فاحذف التطبيق من هذه الأجهزة. • إذا كنت تتوقع أن يتجاوز عدد عمليات التثبيت لتطبيق الطرف الثالث الحد الأقصى المسموح به في المستقبل القريب، ففكر في الحصول على ترخيص جهة خارجية لعدد أكبر من الأجهزة مقدمًا.	90 يومًا

			يمكنك إدارة مفاتيح الترخيص للتطبيقات التابعة لجهات خارجية باستخدام الوظائف الخاصة بمجموعات التطبيقات المُرخصة.	
تم طلب شهادة	4133	KLSRV_CERTIFICATE_REQUESTED	تحدث الأحداث من هذا النوع عندما تفشل إعادة إصدار شهادة إدارة الأجهزة المحمولة تلقائيًا. قد تكون الأسباب والردود المناسبة على الحدث فيما يلي: • تم بدء إعادة الإصدار التلقائي للشهادة التي تم تعطيل خيار **إعادة إصدار الشهادة تلقائيًا إن أمكن**. قد يكون هذا بسبب حدوث خطأ أثناء إنشاء الشهادة. قد يلزم إعادة إصدار الشهادة يدويًا. • إذا كنت تستخدم تكاملاً مع بنية تحتية للمفتاح العام، فقد يكون السبب هو عدم وجود سمة SAM-Account-Name للحساب المستخدم للتكامل مع PKI ولإصدار الشهادة. راجع خصائص الحساب.	90 يومًا
تمت إزالة الشهادة	4134	KLSRV_CERTIFICATE_REMOVED	تحدث الأحداث من هذا النوع عندما يزيل المسؤول أي نوع من الشهادات (عامة، بريد، VPN) لإدارة 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.	90 يومًا
انتهت صلاحية شهادة أسماء نقاط الوصول	4135	KLSRV_APN_CERTIFICATE_EXPIRED	تحدث الأحداث من هذا النوع عند انتهاء صلاحية شهادة APN. تحتاج إلى تجديد شهادة APN يدويًا وتثبيتها على خادم iOS MDM.	غير مخزنة
ستنتهي صلاحية شهادة أسماء نقاط الوصول قريبًا	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	تحدث الأحداث من هذا النوع عندما يتبقى أقل من 14 يومًا قبل انتهاء صلاحية شهادة APN. عند انتهاء صلاحية شهادة APN، تحتاج إلى تجديد شهادة APN يدويًا وتثبيتها على خادم iOS MDM. نوصيك بجدولة تجديد شهادة أسماء نقاط الوصول (APNs) قبل تاريخ انتهاء الصلاحية.	غير مخزنة
فشل إرسال رسالة FCM إلى الجهاز المحمول	4138	KLSRV_GCM_DEVICE_ERROR	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	90 يومًا

			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").		
حدث خطأ في HTTP أثناء إرسال رسالة FCM إلى خادم FCM	4139	KLSRV_GCM_HTTP_ERROR	تحدث الأحداث من هذا النوع عندما يتم تكوين إدارة الأجهزة المحمولة لاستخدام Google Firebase Cloud Messaging (FMC) لتوصيل الأجهزة المحمولة المدارة بنظام التشغيل Android ويعود خادم FMC إلى طلب خادم الإدارة برمز HTTP غير 200 (موافق). قد تكون الأسباب والردود المناسبة على الحدث فيما يلي: • مشكلات من جانب خادم FMC. اقرأ رمز HTTP في تفاصيل وصف الحدث واستجب وفقًا لذلك. لمزيد من المعلومات حول رموز HTTP المستلمة من خادم FMC والأخطاء ذات الصلة، يُرجى الرجوع إلى وثائق خدمة Google Firebase (انظر فصل "رموز استجابة خطأ الرسائل المتلقية للمعلومات"). • مشاكل من جانب الخادم الوكيل (إذا كنت تستخدم خادمًا وكيلاً). اقرأ كود HTTP في تفاصيل الحدث واستجب وفقًا لذلك.	90 يومًا
فشل إرسال رسالة FCM إلى خادم FCM	4140	KLSRV_GCM_GENERAL_ERROR	تحدث الأحداث من هذا النوع بسبب أخطاء غير متوقعة من جانب خادم الإدارة عند العمل مع بروتوكول Google Firebase Cloud Messaging HTTP. اقرأ تفاصيل الحدث في وصف الحدث واستجب وفقًا لذلك. إذا لم تتمكن من إيجاد حل لمشكلة ما بنفسك، فنوصيك بالاتصال بالدعم الفني لـ Kaspersky.	90 يومًا
توجد مساحة فارغة قليلة على القرص الصلب	4105	KLSRV_NO_SPACE_ON_VOLUMES	تحدث الأحداث من هذا النوع عند نفاد مساحة القرص في الجهاز المثبت عليه خادم الإدارة. قم بتحرير مساحة القرص على الجهاز.	90 يومًا
توجد مساحة	4106	KLSRV_NO_SPACE_IN_DATABASE	تحدث الأحداث من هذا النوع في حال	90 يومًا

فارغة قليلة في قاعدة بيانات خادم الإدارة			أصبحت مساحة قاعدة بيانات خادم الإدارة محدودة للغاية. إذا لم يتم إصلاح الوضع، فستصل قاعدة بيانات خادم الإدارة إلى سعتها ولن يقوم خادم الإدارة بأداء وظيفته قريبًا. فيما يلي الأسباب التي أدت إلى هذا الحدث، وفقًا لـ DBMS التي تستخدمها، والاستجابات المناسبة للحدث. إنك تستخدم خادم SQL Server Express Edition DBMS: • في وثيقة SQL Server Express، قم بفحص حد حجم قاعدة البيانات للإصدار الذي تستخدمه. من المحتمل أن قاعدة بيانات خادم الإدارة الخاصة بك على وشك الوصول إلى حد حجم قاعدة البيانات. • يمكنك تقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. • في قاعدة بيانات خادم الإدارة، توجد أحداث تجاوز عددها الحد الأقصى أرسلها مكون التحكم في التطبيقات. يمكنك تغيير إعدادات سياسة Kaspersky Endpoint Security for Linux المتعلقة بتخزين حدث التحكم في التطبيقات في قاعدة بيانات خادم الإدارة. إنك تستخدم DBMS المتوفر بخلاف خادم SQL Server Express Edition: • لا تقم بتقييد عدد الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة. استعرض المعلومات عند تحديد DBMS.	
تمت مقاطعة الاتصال بخادم الإدارة الثانوي	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي. اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الثانوي واستجب وفقًا لذلك.	90 يومًا
تم قطع الاتصال بخادم الإدارة الأساسي	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	تحدث أحداث من هذا النوع عند انقطاع الاتصال بخادم الإدارة الثانوي.	90 يومًا

			اقرأ سجل أحداث Kaspersky على الجهاز حيث تم تثبيت خادم الإدارة الرئيسي واستجب وفقًا لذلك.	
تم تسجيل تحديثات جديدة للوحدات النمطية لبرامج Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	تحدث أحداث من هذا النوع عندما يسجل خادم الإدارة تحديثات جديدة لبرنامج Kaspersky المثبت على الأجهزة المدارة التي تتطلب الموافقة ليتم تثبيتها. وافق على التحديثات أو ارفضها باستخدام Kaspersky Security Center Web Console.	90 يومًا
تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وبدأت عملية حذف الأحداث	4145	KLSRV_EVP_DB_TRUNCATING	تحدث الأحداث من هذا النوع عند بدء حذف الأحداث القديمة من قاعدة بيانات خادم الإدارة بعد الوصول إلى سعة قاعدة بيانات خادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • قم بتغيير الحد الأقصى لعدد الأحداث المخزّنة في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.	غير مخزنة
تم تجاوز الحد الأقصى لعدد الأحداث في قاعدة البيانات، وتم حذف الأحداث	4146	KLSRV_EVP_DB_TRUNCATED	تحدث الأحداث من هذا النوع عند حذف الأحداث القديمة من قاعدة بيانات خادم الإدارة بعد الوصول إلى سعة قاعدة بيانات خادم الإدارة. يمكنك الاستجابة للحدث من خلال الطرق التالية: • قم بتغيير الحد الأقصى المسموح به لعدد الأحداث المخزّنة في قاعدة بيانات خادم الإدارة. • يمكنك تقليل قائمة الأحداث المطلوب تخزينها في قاعدة بيانات خادم الإدارة.	غير مخزنة

الأحداث المعلوماتية لخادم الإدارة

يوضح الجدول أدناه أحداث خادم إدارة Kaspersky Security Center Linux التي تندرج ضمن مستوى خطورة **معلومات**.

الأحداث المعلوماتية لخادم الإدارة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم استنفاد أكثر من 90% من هذا المفتاح	4097	KLSRV_EV_LICENSE_CHECK_90	30 يومًا
تم اكتشاف جهاز جديد	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 يومًا
تمت إضافة جهاز إلى المجموعة تلقائيًا	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 يومًا

تمت إزالة الجهاز من المجموعة: غير نشط على الشبكة لمدة طويلة	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 يومًا
سيتم تجاوز حد عمليات التثبيت قريبًا (تم استهلاك أكثر من 95%) لأحدى مجموعات التطبيقات المرخصة	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 يومًا
تم العثور على ملفات ستُرسل إلى Kaspersky للتحليل	4131	KLSRV_APS_FILE_APPEARED	30 يومًا
تم تغيير معرف مثيل FCM على هذا الجهاز المحمول	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 يومًا
تم نسخ التحديثات بنجاح إلى المجلد المحدد	4122	KLSRV_UPD_REPL_OK	30 يومًا
تم إنشاء الاتصال بخادم الإدارة الثانوي	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 يومًا
تم إنشاء الاتصال بخادم الإدارة الأساسي	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 يومًا
تم تحديث قواعد البيانات	4144	KLSRV_UPD_BASES_UPDATED	30 يومًا
تدقيق: تم إنشاء اتصال بخادم الإدارة	4147	KLAUD_EV_SERVERCONNECT	30 يومًا
تدقيق: تم تعديل الكائن	4148	KLAUD_EV_OBJECTMODIFY	30 يومًا
تدقيق: تم تغيير حالة الكائن	4150	KLAUD_EV_TASK_STATE_CHANGED	30 يومًا
تدقيق: تم تعديل إعدادات المجموعة	4149	KLAUD_EV_ADMGROUP_CHANGED	30 يومًا
التدقيق: تم إنهاء الاتصال بخادم الإدارة	4151	KLAUD_EV_SERVERDISCONNECT	30 يومًا
التدقيق: تم تعديل خصائص الكائن	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 يومًا
التدقيق: تم تعديل أذونات المستخدم	4153	KLAUD_EV_OBJECTACLMODIFIED	30 يومًا

أحداث عميل الشبكة

يتضمن هذا القسم معلومات حول الأحداث المتعلقة بعميل الشبكة.

أحداث تحذير عميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center Linux التي تندرج ضمن مستوى خطورة **تحذير**.

أحداث تحذير عميل الشبكة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
وقع حادث	549	GNRL_EV_APP_INCIDENT_OCCURED	30 يومًا

الأحداث المعلوماتية لعميل الشبكة

يوضح الجدول أدناه أحداث عميل شبكة Kaspersky Security Center Linux التي تندرج ضمن مستوى خطورة **معلومات**.

الأحداث المعلوماتية لعميل الشبكة

اسم العرض لنوع الحدث	معرف نوع الحدث	نوع الحدث	مدة التخزين الافتراضية.
تم تثبيت التطبيق	7703	KLNAG_EV_INV_APP_INSTALLED	30 يومًا
تم إلغاء تثبيت التطبيق	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 يومًا
تم تثبيت التطبيق المراقب	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 يومًا
تم إلغاء تثبيت التطبيق المراقب	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 يومًا
تمت إضافة جهاز جديد	7708	KLNAG_EV_DEVICE_ARRIVAL	30 يومًا
تمت إزالة الجهاز	7709	KLNAG_EV_DEVICE_REMOVE	30 يومًا
تم اكتشاف جهاز جديد	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 يومًا
تم اعتماد الجهاز	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 يومًا

حظر الأحداث المتكررة

يوفر هذا القسم معلومات عن إدارة حظر الأحداث المتكررة وحول إزالة حظر الأحداث المتكررة.

حول حظر الأحداث المتكررة

التطبيق المُدا، على سبيل المثال، Kaspersky Endpoint Security for Linux، المثبت على جهاز مدار واحد أو عدة أجهزة مُدارة يمكنه إرسال الكثير من الأحداث من نفس النوع إلى خادم الإدارة. تلقي أحداث متكررة قد يؤدي إلى زيادة التحميل على قاعدة بيانات خادم الإدارة والكتابة فوق أحداث أخرى. يبدأ خادم الإدارة في حظر الأحداث الجماعية عندما يتجاوز مقدار كل الأحداث المستلمة الحد المحدد لقاعدة البيانات.

يحظر خادم الإدارة الأحداث المتكررة من الاستلام تلقائيًا. لا يمكنك حظر الأحداث المتكررة بنفسك، أو اختر الأحداث التي ترغب في حظرها.

إذا كنت ترغب في معرفة ما إذا تم حظر حدث أم لا، يمكنك عرض قائمة الإخطارات أو يمكنك معرفة ما إذا كان هذا الحدث موجودًا في قسم **حظر الأحداث المتكررة** في خصائص خادم الإدارة. في النافذة، يمكنك إجراء ما يلي:

- إذا كنت ترغب في منع الكتابة فوق قاعدة البيانات، يمكنك ذلك الاستمرار في حظر استلام مثل هذا النوع من الأحداث.
- إذا كنت ترغب، على سبيل المثال، في معرفة سبب إرسال الأحداث المتكررة إلى خادم الإدارة، يمكنك رفع الحظر عن الأحداث المتكررة والاستمرار في استقبال أحداث من هذا النوع على أي حال.
- إذا كنت ترغب في الاستمرار في تلقي الأحداث المتكررة حتى يتم حظرها مرة أخرى، يمكنك رفع الحظر عن الأحداث المتكررة.

إدارة حظر الأحداث المتكررة

يقوم خادم الإدارة بحظر التلقي التلقائي للأحداث المتكررة، ولكن يمكنك إلغاء الحظر والاستمرار في تلقي الأحداث المتكررة. يمكنك كذلك حظر تلقي الأحداث المتكررة التي قمت بإلغاء حظرها من قبل.

لإدارة منع الأحداث المتكررة:

1. في نافذة التطبيق الرئيسية، انقر فوق أيقونة **الإعدادات**( ) بجوار اسم خادم الإدارة المطلوب.
   تفتح نافذة خصائص خادم الإدارة.
2. في تبويب **عام**، حدد قسم **حظر الأحداث المتكررة**.
3. في قسم **حظر الأحداث المتكررة**:
   - إذا كنت ترغب في إلغاء حظر تلقي الأحداث المتكررة:
     a. حدد الأحداث المتكررة التي ترغب في إلغاء حظرها ثم انقر على زر **استثناء**.
     b. انقر على زر **حفظ**.
   - إذا كنت ترغب في حظر تلقي أحداث متكررة:
     a. حدد الأحداث المتكررة التي ترغب في حظرها ثم انقر على 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 تبويب **عام**، حدد قسم **حظر الأحداث المتكررة**.
3. في قسم **حظر الأحداث المتكررة**، حدد الحدث المتكرر الذي ترغب في إزالة الحظر عنه.
4. انقر على زر **إزالة من الحظر**.

بهذا تم حذف الحدث المتكرر من قائمة الأحداث الجماعية. سيستلم خادم الإدارة أحداثًا من هذا النوع.

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 المرفوضة في سجل أحداث Kaspersky. يتم وضع الأحداث الجديدة في قائمة الانتظار ثم حفظها في قاعدة البيانات بعد اكتمال عملية الحذف.

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 Linux 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 مسبقًا:

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 روابطًا 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 (🌐)، الحماية (🛡)، التحديثات (🔄)، إدارة الجهاز (🖥)، منع الاستغلال (🖥)، خادم الإدارة (🖥).
- مستوى أهمية الإشعار. يتم عرض إخطارات مستويات الأهمية التالية: **الإخطارات الحرجة** (🔴)، و**إخطارات التحذير** (⚠)، و**إخطارات المعلومات**. يتم تجميع الإخطارات في القائمة بمستويات الأهمية.

- **الإخطار**. يحتوي هذا على وصف الإخطار.
- **الإجراء** . يحتوي هذا على رابط لإجراء سريع ننصح باتخاذه. يمكنك على سبيل المثال بالنقر على هذا الرابط التقدم إلى المستودع وتثبيت تطبيقات الأمان على الأجهزة أو عرض قائمة بالأجهزة أو قائمة بالأحداث. بعد اتخاذ الإجراء الموصى به للإخطار، يتم تخصيص حالة تم مراجعته إلى هذا الإخطار.
- **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** (🏳).

إذا كان أيقونة **العلم** به نقطة حمراء، يوجد إخطارات لم يتم مراجعتها.

ستفتح نافذة تسرد الإخطارات. بشكل افتراضي، يكون تبويب **جميع الإخطارات** محددًا ويتم تجميع الإخطارات بمستوى الأهمية: حرج أو تحذير أو معلومات.

2. حدد تبويب**النظام**.

يتم عرض قائمة إخطارات مستويات الأهمية حرج (🔴) وتحذير (⚠). قائمة الإخطارات تشمل ما يلي:

- تحديد بالألوان. الإخطارات الحرجة تكون باللون الأحمر. الإخطارات التحذيرية تكون باللون الأصفر.
- الأيقونة التي تشير إلى موضوع الإخطار: النشر (📦)، الحماية (🛡)، التحديثات (🔄)، إدارة الجهاز (🖥)، منع الاستغلال (🛡)، خادم الإدارة (🖥).
- وصف الإخطار.
- أيقونة **العلم**. يكون أيقونة **العلم** باللون الرمادي إلى كان قد تم تخصيص حالة لم يتم مراجعته إلى الإخطارات. عندما تحدد أيقونة **العلم** الرمادي وتخسس حالة تم مراجعته إلى إخطار، يتغير لون الأيقونة إلى الأبيض.
- رابط الإجراء الموصى به. عندما تتخذ الإجراء الموصى به بعد النقر على الرابط، يتم تخصيص حالة تم مراجعته إلى الإخطار.
- عدد الأيام التي مرت منذ لحظة تسجيل الإخطار على خادم الإدارة.

3. حدد تبويب **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 آخر: **الإخطارات بمستوى الأهمية المحدد** مع مستوى الخطورة تحذير.

يتم تحديد قائمة الإخطارات في عنصر الواجهة بحجمها، وتشمل إخطارين. هذا الإخطاران يتعلقان بآخر الأحداث.

قائمة الإخطارات في عنصر الواجهة تشمل ما يلي:

- الأيقونة المتعلقة بموضوع الإخطار: النشر (📦)، الحماية (🛡)، التحديثات (🔄)، إدارة الجهاز (🖥)، منع الاستغلال (🛡)، خادم الإدارة (🖥).
- وصف الإخطار مع رابط إلى الإجراء الموصى به. عندما تتخذ إجراء الموصى به بعد النقر على الرابط، يتم تخصيص حالة تم مراجعته إلى الإخطار.

- عدد الأيام أو عدد الساعات التي مرت منذ لحظة تسجيل الإخطار على خادم الإدارة.
- رابط الإخطارات الأخرى. عند النقر على هذا الرابط، يتم نقلك إلى عرض الإخطارات في قسم **الإخطارات** لقسم **المراقبة والإبلاغ**.

حول حالات الجهاز

يخصص Kaspersky Security Center Linux حالة لكل جهاز مُدار. تعتمد الحالة الخاصة على ما إذا كانت الشروط التي حددها المستخدم قد استوفيت أم لا. في بعض الحالات، عند تعيين حالة لجهازٍ ما، يأخذ Kaspersky Security Center Linux في الاعتبار علامة رؤية الجهاز على الشبكة (انظر الجدول أدناه). إذا لم يعثر Kaspersky Security Center Linux على جهاز على الشبكة في غضون ساعتين، سيتم تعيين علامة رؤية الجهاز إلى غير مرئي.

الحالات كما يلي:

- حرج أو حرج/مرئي
- تحذير أو تحذير/مرئي
- موافق أو موافق/مرئي

يسرد الجدول أدناه الشروط الافتراضية التي يجب استيفائها لتعيين الحالة حرج أو تحذير إلى جهاز، مع جميع القيم المحتملة.

شروط تعيين الحالة إلى الجهاز

الشرط	وصف الشرط	القيم المتوفرة
تطبيق الأمان غير مثبت	عميل الشبكة مثبّت على الجهاز، إلا أن تطبيق الأمان غير مثبّت.	• زر التبديل قيد التشغيل. • زر التبديل متوقف.
تم اكتشاف العديد من الفيروسات	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.	أكثر من 0.
يختلف مستوى الحماية في الوقت الحقيقي عن المستوى الذي تم تعيينه من قِبل المسؤول	الجهاز مرئي على الشبكة، إلا أن مستوى الحماية في الوقت الحقيقي يختلف عن المستوى الذي حدده المسؤول (في الشرط) لحالة الجهاز.	• متوقف. • متوقف مؤقتًا. • قيد التشغيل.
لم يتم إجراء فحص الفيروسات منذ وقت طويل	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.	أكثر من يوم واحد.
قواعد البيانات قديمة	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لم يتم تحديث قواعد بيانات مكافحة الفيروسات على هذا الجهاز خلال الفاصل الزمني المحدد. لا ينطبق الشرط إلا على الأجهزة التي تمت إضافتها إلى قاعدة بيانات خادم الإدارة قبل يوم واحد أو أكثر.	أكثر من يوم واحد.
لم يتم الاتصال منذ فترة طويلة	يتم تثبيت عميل الشبكة على الجهاز، ولكن لم يتم اتصال الجهاز بخادم الإدارة خلال الفاصل الزمني المحدد نظرًا لإيقاف تشغيل الجهاز.	أكثر من يوم واحد.

تم اكتشاف تهديدات نشطة	يتجاوز عدد الكائنات التي لم تتم معالجتها في المجلد **تهديدات نشطة** القيمة المحددة.	أكثر من 0 عناصر.
إعادة التشغيل مطلوبة	الجهاز مرئي على الشبكة، إلا إن أحد التطبيقات يتطلب إعادة تشغيل الجهاز لمدة أطول من الفاصل الزمني المحدد ولأحد الأسباب المحددة.	أكثر من 0 دقائق.
تم تثبيت تطبيقات غير متوافقة	الجهاز مرئي على الشبكة، إلا إن مخزون البرنامج المنفَّذ عبر عميل الشبكة قد اكتشف تطبيقات غير متوافقة مثبتة على الجهاز.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
انتهت صلاحية الترخيص	الجهاز مرئي على الشبكة، إلا إن الترخيص قد انتهى.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
ستنتهي فترة صلاحية الترخيص قريبًا	الجهاز مرئي على الشبكة، إلا أن الترخيص سينتهي على الجهاز خلال فترة أقل من عدد الأيام المحدد.	أكثر من 0 أيام.
تم اكتشاف حوادث لم تتم معالجتها	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.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
حالة الجهاز المحددة بواسطة التطبيق	تم تحديد حالة الجهاز بواسطة التطبيق المدار.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.
نفدت مساحة قرص الجهاز	مساحة القرص الشاغرة على الجهاز أقل من القيمة المحددة أو أنه يتعذر مزامنة الجهاز مع خادم الإدارة. يتم تغيير الحالة حرج أو تحذير إلى الحالة جيد عند مزامنة الجهاز بنجاح مع خادم الإدارة وتكون المساحة الفارغة على الجهاز أكبر من أو تساوي القيمة المحددة.	أكثر من 0 ميجابايت
أصبح الجهاز غير مُدار	أثناء اكتشاف الأجهزة، تم التعرف على الجهاز بأنه مرئي على الشبكة، لكن فشلت أكثر من ثلاث محاولات للمزامنة مع خادم الإدارة.	• زر التبديل متوقف. • زر التبديل

		قيد التشغيل.
تم تعطيل الحماية	الجهاز مرئي على الشبكة، إلا إنه قد تم تعطيل تطبيق الأمان على الجهاز لمدة أطول من الفاصل الزمني المحدد.	أكثر من 0 دقائق.
تطبيق الأمان ليس قيد التشغيل	الجهاز مرئي على الشبكة وتم تثبيت تطبيق أمان على الجهاز، إلا أنه لا يعمل.	• زر التبديل متوقف. • زر التبديل قيد التشغيل.

يتيح لك Kaspersky Security Center Linux إعداد 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 Linux من الإصدار السابق، فإن قيم شرط **قواعد البيانات قديمة** لتخصيص الحالة تتغير إلى حرجة أو تحذير لا تتغير.

عندما يقوم Kaspersky Security Center Linux 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 لجهازٍ 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 عى 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 الأيمن، 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 عى تحذير .

تكوين تسليم الإخطار

يمكنك تكوين إخطار عن الأحداث التي تقع في Kaspersky Security Center Linux. اعتمادًا على طريقة الإخطار المختارة، تتوفر أنواع الإخطارات التالية:

- البريد الإلكتروني: عند وقوع حدثٍ ما، يرسل Kaspersky Security Center Linux إخطارًا إلى لعناوين البريد الإلكتروني المحددة.
- الرسائل النصية القصيرة: عند وقوع حدثٍ ما، يرسل Kaspersky Security Center Linux 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 Linux:

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 **SMTP خوادم**، حدد عناوين خادم البريد، مع الفصل بينهم بفواصل منقوطة. يمكنك استخدام القيم التالية:

- عنوان IPv4 أو IPv6

- 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 إعلامات البريد الإلكتروني.

في حال تمكين خيار **استخدام مصادقة ESMTP**، يمكنك تحديد إعدادات مصادقة ESMTP في **اسم المستخدم** و**كلمة 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 دوما 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 لاتصال TLS.

إذا قمت بتحديد قيمة **استخدم TLS دوما 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 Linux مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center Linux 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.

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.

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 **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 معلمات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال. يمكنك تحرير نص الرسالة عن طريق إضافة بعض المعلمات البديلة الأخرى مع تفاصيل ذات صلة أكثر بالحدث.

إذا كان نص الإخطار يحتوي على علامة النسبة المئوية (%)، فيجب عليك كتابته مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل CPU 100%%".

النقر على رابط **تكوين حد الإخطارات الرقمي** يتيح لك تحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مُدار الفاصل الزمني المحدد.

- رسالة SMS

تبويب **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 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** و **كلمة 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 دوما 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 لاتصال TLS.

إذا قمت بتحديد قيمة **استخدم TLS دوما 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 ملف شهادة خادم SMTP بالنقر فوق رابط **تحديد الشهادات** : يمكنك استلام ملف بقائمة الشهادات من جهات إصدار موثوقة ورفع الملف إلى خادم الإدارة. يتحقق Kaspersky Security Center Linux مما إذا كانت شهادة خادم SMTP موقعة أيضًا من جانب جهة إصدار موثوقة. لا يمكن لـ Kaspersky Security Center Linux 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 فارغًا، سيتم استخدام عنوان المستلم افتراضيًا. 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 نصًا يحتوي على معلومات حول الحدث الذي يرسله التطبيق عند وقوع حدث. يمكن أن يشمل هذا النص معلمات بديلة، مثل اسم الحدث واسم الجهاز واسم المجال.

إذا كان نص الإخطار يحتوي على علامة النسبة المئوية (%)، فيجب عليك كتابته مرتين متتاليتين للسماح بإرسال الرسالة. على سبيل المثال، "تحميل %%CPU 100".

انقر فوق زر **إرسال رسالة اختبار** للتحقق مما إذا كنت قد قمت بتكوين الإشعارات بشكل صحيح: يرسل التطبيق إشعارا تجريبيًا إلى المستلم الذي حددته.

انقر فوق رابط **تكوين حد الإخطارات الرقمي** لتحديد الحد الأقصى لعدد الإشعارات التي يمكن للتطبيق إرسالها خلال الفترة الزمنية المحددة.

- **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 النائبة التي تحدد تفاصيل الحدث التي سيتم إرسالها في رسالة الإشعار. يجب أن يكون المجلد والملف اللذين تحددهما موجودين على خادم الإدارة.

النقر على رابط **تكوين حد الإخطارات الرقمي** يتيح لك تحديد الحد الأقصى لعدد الإخطارات التي يمكن للتطبيق إرسالها على مُدار الفاصل الزمني المحدد.

3. حدد إعدادات الإخطار في التبويب.

4. انقر فوق الزر **موافق** لإغلاق النافذة خصائص خادم الإدارة.

يتم تطبيق إعدادات تسليم الإخطار المحفوظة على جميع الأحداث التي تقع في Kaspersky Security Center Linux.

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 الاختبار

للتحقق من إرسال إشعارات الحدث أم لا، يستخدم التطبيق إشعار الاختبار لاكتشاف فيروس EICAR في الأجهزة العميلة.

للتحقق من إرسال إخطارات الأحداث:

1. أوقف مهمة حماية نظام الملفات في الوقت الحقيقي على الجهاز العميل وانسخ اختبار الفيروس EICAR إلى ذلك الجهاز العميل. الآن قم بإعادة تمكين الحماية في الوقت الحقيقي لملف النظام.

2. قم بتشغيل مهمة الفحص للأجهزة العميلة في إحدى مجموعات الإدارة أو للأجهزة المحددة، بما في ذلك الجهاز الذي يحتوي على "الفيروس" EICAR.

إذا تم تكوين مهمة الفحص بشكل صحيح، فسوف يتم اكتشاف اختبار "الفيروس". إذا تم تكوين الإخطارات بشكل صحيح، فيتم إخطارك بأنه قد تم اكتشاف أحد الفيروسات.

لفتح سجل اختبار الكشف عن الفيروسات:

1. في القائمة الرئيسية، انتقل إلى **المراقبة والإبلاغ** ← **تحديدات الأحداث**.

2. انقر فوق اسم اختيار **الأحداث الأخيرة**.

في النافذة التي تفتح، يتم عرض الإشعار بشأن اختبار الفيروس.

لا يحتوي اختبار الفيروس EICAR على أي 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 Linux إخطار المسؤول بشأن الأحداث على الأجهزة العميلة عبر تشغيل الملف التنفيذي. يجب أن يحتوي الملف التنفيذي على ملف تنفيذي آخر مع العناصر النائبة للحدث ليتم ترحيله إلى المسؤول.

العناصر النائبة لوصف حدث

عنصر 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
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	اسم المهمة
%KL_PRODUCT%	عميل شبكة Kaspersky Security Center Linux
%KL_VERSION%	رقم إصدار عميل الشبكة
%HOST_IP%	عنوان IP
%HOST_CONN_IP%	عنوان IP للاتصال

مثال:
يتم إرسال إشعارات الحدث بواسطة ملف تنفيذي (مثل script1.bat) الذي يوجد بداخله ملف تنفيذي آخر (مثل script2.bat) مع تشغيل العنصر النائب %COMPUTER%. عند وقوع حدث ما، سيتم تشغيل الملف script1.bat على جهاز المسؤول والذي بدوره يشغّل الملف script2.bat مع العنصر النائب %COMPUTER%. يتلقى المسؤول اسم الجهاز حيث وقع الحدث.

إعلامات Kaspersky

يصف هذا القسم كيفية استخدام إعلانات Kaspersky وتكوينها وتعطيلها.

حول أخبار Kaspersky

قسم أخبار Kaspersky (**المراقبة والإبلاغ** ← **أخبار Kaspersky**) يبقيك على اطلاع من خلال توفير المعلومات المتعلقة بإصدار Kaspersky Security Center لديك والتطبيقات المدارة المثبتة على الأجهزة المدارة. يقوم Kaspersky Security Center بتحديث المعلومات الواردة في القسم بشكل دوري عن طريق إزالة الأخبار القديمة وإضافة معلومات جديدة.

يعرض Kaspersky Security Center إعلانات Kaspersky التي تتعلق بخادم الإدارة المتصل حاليًا وتطبيقات Kaspersky المثبتة على الأجهزة المدارة لخادم الإدارة هذا. يتم عرض الإعلانات بشكل فردي لأي نوع من خوادم الإدارة سواء كام—أساسي أم ثانوي أم افتراضي.

يجب أن يكون خادم الإدارة متصلاً بالإنترنت لتلقي أخبار Kaspersky.

تهدف الإعلانات إلى الحفاظ على تحديث تطبيقات Kaspersky المثبتة في شبكتك وتشغيلها 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 إعلانات Kaspersky 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.

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. إذا كنت لا ترغب في تلقي الإعلانات، يمكنك تعطيل هذه الميزة.

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**)يبقيك على اطلاع من خلال توفير المعلومات المتعلقة بإصدار Kaspersky Security Center لديك والتطبيقات المدارة المثبتة على الأجهزة المدارة. إذا كنت لا ترغب في تلقي أخبار Kaspersky، يمكنك تعطيل هذه الميزة.

لتعطيل إعلانات Kaspersky:

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 **أخبار Kaspersky**.
3. قم بتبديل زر التبديل إلى وضع **تعطيل الأخبار المتعلقة بالأمان**.
4. انقر على زر **حفظ**.

بهذا تم تعطيل أخبار Kaspersky.

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 Linux بتكوين تصدير الأحداث إلى أنظمة SIEM بإحدى الطرق التالية: التصدير إلى أي نظام SIEM يستخدم تنسيق Syslog أو تصدير الأحداث إلى أنظمة SIEM مباشرةً من قاعدة بيانات Kaspersky Security Center. عند إكمال هذا السيناريو، يرسل خادم الإدارة الأحداث إلى نظام SIEM تلقائيًا.

المتطلبات الأساسية

قبل أن تبدأ في تصدير تكوين الأحداث في Kaspersky Security Center Linux:

- 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 Linux**

  تعليمات للمساعدة: تكوين تصدير الحدث في نظام SIEM

- **تحديد الأحداث التي تريد تصديرها إلى نظام SIEM**

  تمييز الأحداث التي تريد تصديرها إلى نظام SIEM: أولاً، ضع علامة على الأحداث العامة التي تحدث في جميع تطبيقات Kaspersky المُدارة. بعد ذلك، يمكنك تحديد الأحداث لتطبيقات محددة مُدارة من Kaspersky.

- **تكوين تصدير الأحداث إلى نظام SIEM**

  يمكنك التأكد من ذلك باستخدام إحدى الطرق التالية:

  - استخدم TCP/IP أو UDP أو TLS من خلال بروتوكولات TCP.
  - استخدم 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 Linux، يجب عليك تحديد بعض إعدادات نظام SIEM. يوصى بأن تتحقق من هذه الإعدادات مسبقًا للتحضير لإعداد Kaspersky Security Center Linux.

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 Linux وخادم نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center Linux وفي إعدادات المستلم لنظام SIEM الخاص بك.

- **البروتوكول**

  البروتوكول المستخدم لنقل الرسائل من Kaspersky Security Center Linux إلى نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center Linux وفي إعدادات المستلم لنظام SIEM الخاص بك.

حول الأحداث في Kaspersky Security Center Linux

يتيح لك Kaspersky Security Center Linux 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.

الأحداث حسب النوع

يتوفر في Kaspersky Security Center Linux الأنواع التالية من الأحداث:

- الأحداث العامة. تحدث هذه الأحداث في جميع تطبيقات Kaspersky المدارة. مثال على حدث عام هو انتشار الفيروسات. لقد حددت الأحداث العامة بناء الجملة والدلالات بدقة. يتم استخدام الأحداث العامة على سبيل المثال، في التقارير ولوحات المعلومات.
- أحداث خاصة بتطبيقات Kaspersky المدارة. يحتوي كل تطبيق من تطبيقات Kaspersky المدارة على مجموعة من الأحداث الخاصة به.

الأحداث حسب المصدر

يمكنك عرض القائمة الكاملة للأحداث التي يمكن إنشاؤها بواسطة تطبيق ما في علامة التبويب **تكوين الحدث** في سياسة التطبيق. بالنسبة لخادم الإدارة، يمكنك أيضًا عرض قائمة الأحداث في خصائص خادم الإدارة.

يمكن إنشاء الأحداث من خلال التطبيقات التالية:

- مكونات Kaspersky Security Center Linux:

- خادم الإدارة
- عميل الشبكة
- تطبيقات Kaspersky المُدارة

للحصول على تفاصيل حول الأحداث التي تم إنشاؤها بواسطة تطبيقات Kaspersky المُدارة، يُرجى الرجوع إلى وثائق التطبيق المقابل.

الأحداث حسب مستوى الأهمية

يحتوي كل حدث على مستوى الأهمية الخاص به. بناء على شروط الحدوث، يمكن تعيين مستويات أهمية مختلفة لأي حدث. توجد أربعة مستويات للأهمية للأحداث:

- حدث حرج هو حدث يشير إلى تكرار مشكلة حرجة قد تؤدي إلى فقدان البيانات أو خلل في التشغيل أو خطأ حرج.
- خلل وظيفي هو حدث يشير إلى تكرار مشكلة خطيرة أو خطأ أو خلل حدث أثناء تشغيل التطبيق أو عند تنفيذ الإجراء.
- تحذير هو حدث ليس خطيرًا بالضرورة، غير أنه يشير إلى مشكلة محتملة في المستقبل. يتم تعيين معظم الأحداث كتحذيرات إذا كان من الممكن استعادة التطبيق بدون فقدان البيانات أو الإمكانيات الوظيفية بعد حدوث هذه الأحداث.
- حدث معلومات هو حدث يحدث لأغراض الإخبار عن إكمال التشغيل بنجاح، أو التشغيل الصحيح للتطبيق، أو إكمال الإجراء.

لكل حدث مدّة تخزين محددة، يمكنك خلالها عرضه في Kaspersky Security Center Linux أو تعديله. لا يتم حفظ بعض البيانات في قاعدة بيانات خادم الإدارة بشكل افتراضي لأن مدّة التخزين المحددة هي صفر. يمكن تصدير الأحداث التي سيتم تخزينها في قاعدة بيانات خادم الإدارة فقط لمدة يوم واحد على الأقل إلى الأنظمة الخارجية.

حول تصدير الحدث

يمكن استخدام تصدير الحدث في الأنظمة المركزية التي تتعامل مع مشكلات الأمان على المستوى التنظيمي والتقني، والتي توفر خدمات مراقبة الأمان، وتجمع المعلومات من الحلول المختلفة. وهذه هي أنظمة SIEM التي توفر التحليل الفوري لتحذيرات الأمان والأحداث التي تنشئها أجهزة الشبكة والتطبيقات، أو مراكز تشغيل الأمان (SOC).

يمكن لهذه الأنظمة استلام البيانات من العديد من المصادر، بما فيها الشبكات والأمان والخوادم وقواعد البيانات والتطبيقات. توفر أنظمة SIEM أيضًا وظيفة تجميع البيانات التي تم رصدها لمساعدتك في تجنب فقدان الأحداث الحرجة. إضافة إلى ذلك، تُجري الأنظمة تحليلاً تلقائيًا للأحداث والتحذيرات المترابطة لإخطار المسؤولين بمشاكل الأمان العاجلة. يمكن تنفيذ التحذير من خلال لوحة معلومات ويمكن إرسالها من خلال قنوات لجهات خارجية مثل البريد الإلكتروني.

تشتمل عملية تصدير الأحداث من Kaspersky Security Center Linux إلى أنظمة SIEM الخارجية على طرفين: Kaspersky Security Center Linux ومستلم الحدث – نظام SIEM. لتصدير حدث بنجاح، يجب عليك تكوين هذا الحدث في نظام SIEM وفي وحدة تحكم إدارة Kaspersky Security Center Linux. لا يهم ما الطرف الذي تقوم بتكوينه أولاً. يمكنك تكوين نقل الأحداث في Kaspersky Security Center Linux ثم تكوين مستلم الأحداث بواسطة نظام SIEM أو العكس.

تنسيق Syslog لتصدير الحدث

يمكنك إرسال الأحداث بتنسيق Syslog إلى أي نظام SIEM. باستخدام بروتوكول Syslog، يمكنك ترحيل أي من الأحداث التي تحدث في خادم الإدارة وفي تطبيقات Kaspersky المثبتة على الأجهزة المدارة. عند تصدير الأحداث عبر تنسيق Syslog، يمكنك تحديد أنواع الأحداث التي سيتم ترحيلها بالضبط إلى نظام SIEM.

استلام الأحداث بواسطة نظام SIEM

يجب أن يستلم نظام SIEM الأحداث المحللة بشكل صحيح والمستلمة من Kaspersky Security Center Linux. 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 Linux إلى أنظمة SIEM الخارجية على طرفين: Kaspersky Security Center Linux ومستلم الحدث – نظام SIEM. يجب عليك تكوين عملية تصدير الأحداث في نظام SIEM الخاص بك وفي Kaspersky Security Center Linux.

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 Linux، يجب عليك إعداد المستلم في نظام SIEM الخاص بك. بوجه عام، يجب تحديد الإعدادات التالية في نظام SIEM.

- **بروتوكول التصدير**

  بروتوكول نقل الرسائل، إما UDP أو TCP أو TLS، عبر TCP. يجب أن يكون هذا البروتوكول مطابقًا لما حددته في Kaspersky Security Center Linux.

- **المنفذ**

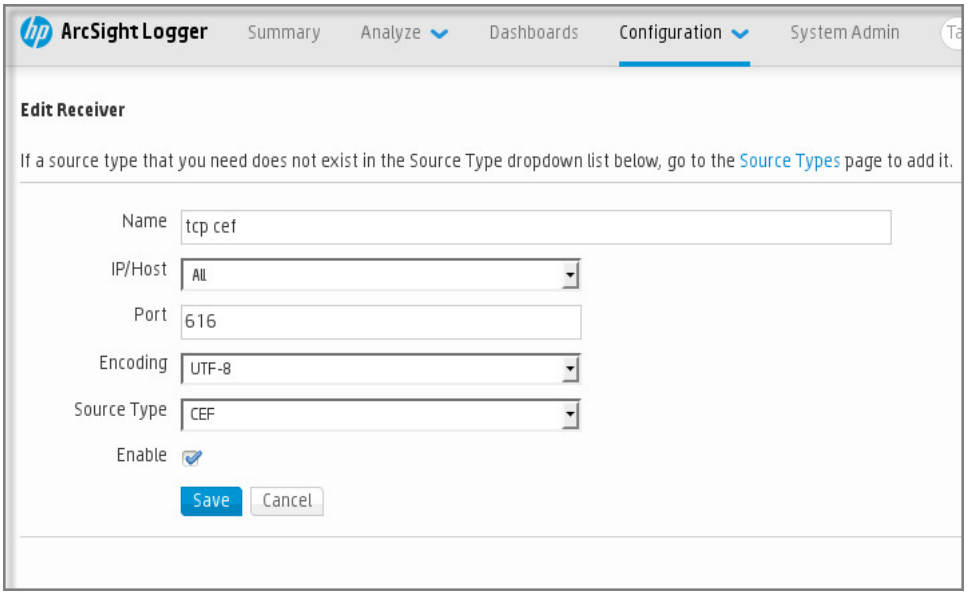
  حدد رقم المنفذ للاتصال بـ Kaspersky Security Center Linux. يجب أن يكون هذا المنفذ هو نفس المنفذ الذي تحدده في Kaspersky Security Center Linux أثناء التكوين باستخدام نظام SIEM.

- **تنسيق البيانات**

  حدد تنسيق Syslog.

بناءً على نظام SIEM الذي تستخدمه، قد يتعين عليك تحديد بعض الإعدادات الإضافية للمستلم.

يوضح الشكل أدناه شاشة إعداد جهاز الاستقبال في ArcSight.



إعداد المستلم في ArcSight

محلل الرسالة

يتم تمرير الأحداث التي تم تصديرها إلى أنظمة SIEM كرسائل. يجب تحليل هذه الرسائل على النحو الصحيح حتى يتسنى استخدام معلومات الأحداث بواسطة نظام SIEM. تمثل محللات الرسالة جزءًا من نظام SIEM، إذ تُستخدم لتجزئة محتويات الرسالة في الحقول ذات الصلة، مثل معرف الحدث والخطورة والوصف والمعلمات وما إلى ذلك. يتيح هذا الإجراء لنظام SIEM معالجة الأحداث المستلمة من Kaspersky Security Center Linux حتى يمكن تخزينها في قاعدة بيانات نظام SIEM.

يحتوي كل نظام من أنظمة SIEM على مجموعة من محللات الرسالة القياسية. يوفر Kaspersky أيضًا محللات الرسالة لبعض أنظمة SIEM، على سبيل المثال، QRadar وArcSight. يمكنك تنزيل هذه الرسائل من مواقع ويب أنظمة SIEM المطابقة. عند تكوين المستلم، يمكنك استخدام أحد محللات 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 خانات 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 أيضًا 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 مسبقًا في سياسة التطبيق، فلن تتمكن من إعادة تعريف الأحداث المحددة لجهاز مُدار.

لتحديد الأحداث التي تريد تصديرها لجهاز مُدار:

1. في القائمة الرئيسية، انتقل إلى **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 خانات الاختيار الموجودة بجوار الأحداث التي ترغب في تصديرها إلى SIEM.

7. انقر على الزر **وضع علامة على التصدير إلى نظام SIEM باستخدام Syslog**.

ويمكنك أيضا 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 فصاعدًا، يرسل خادم الإدارة الأحداث المحددة إلى نظام SIEM إذا تم تكوين التصدير إلى نظام SIEM.

وضع علامة على الأحداث العامة للتصدير بتنسيق Syslog

يمكنك وضع علامة على الأحداث العامة التي سيصدرها خادم الإدارة إلى أنظمة SIEM باستخدام تنسيق Syslog.

وضع علامة على الأحداث العامة للتصدير إلى نظام SIEM:

1. قم بأحد الإجراءات التالية:

- 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 أيضا 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 فصاعدًا، يرسل خادم الإدارة الأحداث المحددة إلى نظام SIEM إذا تم تكوين التصدير إلى نظام SIEM.

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 Linux إلى الأنظمة الخارجية.

في Kaspersky Security Center Linux، 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 Linux ليرسل الأحداث إلى نظام SIEM. يبدأ Kaspersky Security Center Linux 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 Linux لتصدير الأحداث إلى نظام SIEM

لتصدير الأحداث إلى نظام SIEM، يجب عليك تكوين عملية التصدير في Kaspersky Security Center Linux.

لتكوين التصدير إلى أنظمة SIEM في Kaspersky Security Center 14 Web Console:

1. في القائمة المنسدلة **إعدادات وحدة التحكم**، حدد **التكامل**.

   ستفتح 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 Linux وخادم نظام SIEM الخاص بك. حدد هذه القيمة في إعدادات Kaspersky Security Center Linux وفي إعدادات المستلم لنظام SIEM الخاص بك.

- **البروتوكول**

حدد البروتوكول الذي سيُستخدم 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 CenterLinu Linux. يتحقق Kaspersky Security Center Linux مما إذا كانت شهادة خادم نظام SIEM موقعة أيضًا من قِبل جهة إصدار موثوقة 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 Linux 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 أيٍ من أسماء الموضوعات المحددة مع اسم موضوع شهادة نظام SIEM، فسيتحقق Kaspersky Security Center Linux 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 Linux الشهادة الموقعة ذاتيًا التي تم إنشاؤها، ويمكنك تمرير الجزء العام من الشهادة أو بصمة SHA1 إلى نظام SIEM.

6. إذا أردت، يمكنك تصدير الأحداث المؤرشفة من قاعدة بيانات خادم الإدارة وتعيين تاريخ البدء الذي تريد بدء تصدير الأحداث المؤرشفة منه:

a. انقر فوق رابط**تعيين تاريخ بدء التصدير** الرابط.

b. في القسم الذي يتم فتحه، حدد تاريخ البدء في حقل **تاريخ بدء التصدير من**.

c. انقر على زر **موافق**.

7. قم بتبديل الخيار إلى وضع**تصدير الأحداث إلى قاعدة بيانات نظام SIEM تلقائيًا مُمكّن**.

8. انقر على زر **حفظ**.

يتم تكوين التصدير إلى نظام SIEM. من الآن فصاعدًا، إذا قمت بتكوين استلام الأحداث في نظام SIEM، يقوم خادم الإدارة بتصدير الأحداث المميزة إلى نظام SIEM. إذا قمت بتعيين تاريخ بدء التصدير، يقوم خادم الإدارة أيضًا بتصدير الأحداث المميزة والمخزنة في قاعدة بيانات خادم الإدارة من التاريخ المحدد.

تصدير الأحداث مباشرة من قاعدة البيانات

يمكنك استعادة الأحداث مباشرة من قاعدة بيانات Kaspersky Security Center Linux دون استخدام واجهة Kaspersky Security Center Linux. 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 Linux. يمكنك العثور على وصف آراء الجمهور هذه في مستند klakdb.chm.

يشتمل الرأي العام v_akpub_ev_event على مجموعة حقول تمثل معلمات الحدث في قاعدة البيانات. في مستند klakdb.chm يمكنك أيضًا العثور على معلومات حول الآراء العامة المطابقة لكيانات Kaspersky Security Center Linux 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 klsql2 المساعدة ومثال الاستعلام.

لإنشاء استعلامات SQL أو آراء قاعدة البيانات، يمكنك أيضًا استخدام أي برنامج آخر للتعامل مع قوعد البيانات. يتم ذكر معلومات حول كيفية عرض المعلمات للاتصال بقاعدة بيانات Kaspersky Security Center Linux، مثل اسم المثيل، واسم قاعدة البيانات في القسم المقابل.

إنشاء استعلام SQL باستخدام أداة klsql2 المساعدة

يوضح هذا القسم كيفية تنزيل أداة klsql2 المساعدة واستخدامها، وكيفية إنشاء استعلام SQL باستخدام هذه الأداة المساعدة. عندما تقوم بإنشاء استعلام SQL بواسطة أداة klsql2 المساعدة، لا يتعين عليك توفير اسم قاعدة البيانات ومعلمات الوصول، لأن الاستعلام يتعامل مع الرؤى العامة لـ Kaspersky Security Center Linux بشكل مباشر.

لتنزيل أداة klsql2 المساعدة واستخدامها:

1. تنزيل klsql2 utility من الموقع الإلكتروني لـ Kaspersky.

2. انسخ ملف klsql2.zip الذي تم تنزيله وفك ضغطه في أي مجلد على الجهاز المثبت عليه خادم إدارة Kaspersky Security Center Linux.
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 Linux، 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 حديثًا 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 المعروض للحدث */
e.wstrDescription,*/ الوصف المعروض للحدث */
e.wstrGroupName,*/ اسم المجموعة حيث يوجد الجهاز */
h.wstrDisplayName,*/ الاسم المعروض 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 Linux

إذا كنت ترغب في الوصول إلى قاعدة بيانات Kaspersky Security Center Linux بواسطة خادم SQL 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 Linux:

1. انقر على أيقونة الإعدادات() بجوار اسم خادم الإدارة المطلوب.

تفتح نافذة خصائص خادم الإدارة.

2. في علامة التبويب **عام**، ثم حدد قسم **تفاصيل قاعدة البيانات الحالية**.

يتم تحديد اسم قاعدة البيانات في حقل **اسم قاعدة البيانات**. استخدام اسم قاعدة البيانات لمعالجة قاعدة البيانات في استعلامات SQL الخاصة بك.

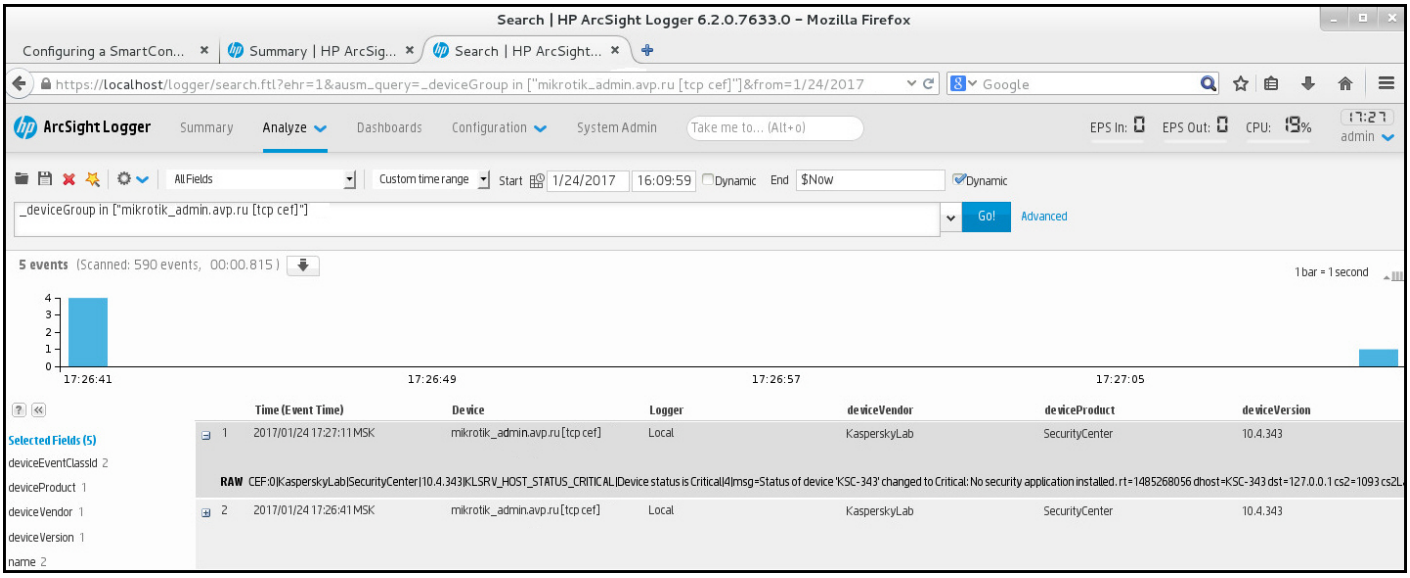
عرض نتائج التصدير

يمكنك التحكم في إكمال إجراء تصدير الحدث بنجاح. وللقيام بهذا الإجراء، تحقق من استلام نظام SIEM الخاص بك للرسائل المشتملة على أحداث التصدير

إذا تم استلام الأحداث المرسلة من Kaspersky Security Center Linux 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 Linux مقابلة للتكوين في نظام SIEM الخاص بك.

يوضح الشكل أدناه الأحداث التي تم تصديرها إلى ArcSight. على سبيل المثال، يعتبر الحدث الأول حدثًا مهمًا لخادم الإدارة: "حالة الجهاز حرجة".

يتباين تمثيل أحداث التصدير في نظام SIEM بحسب نظام SIEM الذي تستخدمه.



مثال للأحداث

تحديدات الأجهزة

تحديدات الأجهزة هي أداة لتصفية الأجهزة وفق شروط محددة. يمكنك استخدام تحديدات الأجهزة لإدارة عدة أجهزة: يمكن على سبيل المثال عرض تقرير حول هذه الأجهزة فقط أو من أجل نقل جميع هذه الأجهزة إلى مجموعة أخرى.

يوفر Kaspersky Security Center نطاق كبير التحديدات المحددة مسبقًا (مثل **الأجهزة ذات الحالة حرج**، **تم تعطيل الحماية**، **تم اكتشاف تهديدات نشطة**). لا يمكن حذف التحديدات المحددة مسبقًا. 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. جدد 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. انتقل إلى **الأجهزة** ← **تحديدات الأجهزة**.
   سيتم عرض صفحة بقائمة تحديدات الأجهزة.

2. انقر على تحديد الجهاز الذي حدده المستخدم ذو الصلة.
   ستفتح 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 افتراضيًا.

الشبكة

في القسم **الشبكة**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لبيانات الشبكة الخاصة بهم:

- **اسم الجهاز أو عنوان IP**
- **مجال Windows**

عرض كل الأجهزة المضمنة في مجموعة العمل المحددة.

- **مجموعة الإدارة**

عرض الأجهزة المضمنة في مجموعة الإدارة المحددة.

- **الوصف**

نص في نافذة خصائص الجهاز: في حقل **الوصف**بقسم **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 عبارات مثل **SUSE Linux Enterprise Server 12** أو **SUSE Linux Enterprise Server 15**، يمكنك إدخال **SUSE Linux Enterprise Server 1؟** .

لا يمكن استخدام نجمة (*) أو علامة استفهام (؟) كأول حرف في الاستعلام.

- للبحث عن كلمات متعددة:
  - مسافة. تعرض جميع الأجهزة التي يحتوي وصفها على أي كلمة من الكلمات المدرجة.

مثال:

للبحث عن عبارة تحتوي على كلمة **تابع** أو **ظاهري**، يمكنك إدخال **تابع ظاهري** في الاستعلام.

  - +. عندما تأتي علامة الزائد قبل كلمة، ستحتوي جميع نتائج البحث على هذه الكلمة.

مثال:

للبحث عن عبارة تحتوي على الكلمتين **تابع** و**ظاهري**، أدخل الاستعلام **+تابع+ظاهري**.

  - -. عندما تأتي علامة الناقص قبل كلمة، لن تحتوي نتائج البحث على هذه الكلمة.

مثال:

للبحث عن عبارة تحتوي على كلمة **تابع** ولا تحتوي على كلمة **ظاهري**، أدخل الاستعلام **+تابع-ظاهري**.

  - **"<some text>"**. النص الموضوع بين علامتي الاقتباس يجب أن يكون موجودًا في النص.

مثال:

للبحث عن عبارة تحتوي على الكلمة المركّبة **الخادم التابع**، أدخل **"الخادم التابع"** في الاستعلام.

- **نطاق IP**

إذا تم تمكين هذا الخيار، فيمكنك إدخال عناوين IP الأولية والنهائية لنطاق IP الذي يجب تضمين الأجهزة ذات الصلة فيه.

يتم تعطيل هذا الخيار افتراضيًا.

العلامات

في القسم **العلامات**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على الكلمات المفتاحية (العلامات) التي تمت إضافتها سابقًا إلى أوصاف الأجهزة المدارة:

- **تطبيق في حالة مطابقة علامة محددة واحدة على الأقل**

إذا تم تمكين هذا الخيار، فستعرض نتائج البحث الأجهزة التي تحتوي أوصافها على علامة واحدة من العلامات على الأقل.

إذا تم تعطيل هذا الخيار، فستعرض نتائج البحث فقط الأجهزة التي تحتوي أوصافها على جميع العلامات المحددة.

يتم تعطيل هذا الخيار افتراضيًا.

- **يجب تضمين العلامة**

إذا تم تحديد خانة الاختيار هذه، فستعرض نتائج البحث الأجهزة التي تحتوي أوصافها على العلامة المحددة. للعثور على الأجهزة، يمكنك استخدام علامة النجمة، التي ترمز إلى أي سلسلة بها أي عدد من الحروف.

يتم تحديد هذا الخيار افتراضيًا.

- **يجب استثناء العلامة**

إذا تم تحديد خانة الاختيار هذه، فستعرض نتائج البحث الأجهزة التي لا تحتوي أوصافها على العلامة المحددة. للعثور على الأجهزة، يمكنك استخدام علامة النجمة، التي ترمز إلى أي سلسلة بها أي عدد من الحروف.

نشاط الشبكة

في القسم **نشاط الشبكة** يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لنشاط الشبكة الخاص بهم:

- **هذا الجهاز هو عبارة عن نقطة توزيع**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. سوف يتضمن التحديد أجهزة الكمبيوتر التي تعمل كنقاط توزيع.
- **لا**. لن يتم تضمين الأجهزة التي تعمل كنقاط توزيع في التحديد.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **عدم قطع الاتصال عن خادم الإدارة**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **مُمكّن**. سيتضمن التحديد الأجهزة التي تم تحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة** عليها.
- **معطل**. سيتضمن التحديد الأجهزة التي تم إلغاء تحديد خانة الاختيار **عدم قطع الاتصال عن خادم الإدارة** عليها.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تم تبديل ملف تعريف الاتصال**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. سوف يتضمن التحديد الأجهزة المتصلة بخادم الإدارة بعد تبديل ملف تعريف الاتصال.
- **لا**. لن يتضمن التحديد الأجهزة المتصلة بخادم الإدارة بعد تبديل ملف تعريف الاتصال.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تاريخ آخر اتصال بخادم الإدارة**

يمكنك استخدام خانة الاختيار هذه لتعيين معيار للبحث عن الأجهزة إلى وقت آخر اتصال بخادم الإدارة.

إذا تم تحديد خانة الاختيار هذه، فيمكنك في حقول الإدخال تحديد الفاصل الزمني (التاريخ والوقت) الذي تم خلاله إنشاء آخر اتصال بين عميل الشبكة المثبت على الجهاز العميل وخادم الإدارة. سوف يتضمن الاختيار الأجهزة التي تقع ضمن الفاصل الزمني المحدد.

إذا تم إلغاء خانة الاختيار هذه، لن يتم تطبيق المعيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **تم اكتشاف أجهزة جديدة بواسطة استقصاء الشبكة**

عمليات البحث عن أجهزة جديدة تم اكتشافها بواسطة استقصاء الشبكة على مدار الأيام القليلة الماضية.

إذا تم تمكين هذا الخيار، فسيتضمن التحديد فقط الأجهزة الجديدة التي تم اكتشافها بواسطة خاصية اكتشاف الأجهزة على مدار عدد الأيام المحددة في حقل **فترة الكشف (بالأيام)**.

إذا تم تعطيل هذا الخيار، فسيتضمن التحديد جميع الأجهزة التي تم اكتشافها بواسطة خاصية اكتشاف الأجهزة.

يتم تعطيل هذا الخيار افتراضيًا.

- **الجهاز مرئي**

في القائمة المنسدلة، يمكنك تعيين معيار للأجهزة المضمنة في اختيار عند إجراء البحث:

- **نعم**. يشمل التطبيق في الاختيار الأجهزة المرئية في الوقت الحالي على الشبكة.
- **لا**. يشمل التطبيق في 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**

في القائمة المنسدلة، يمكنك إعداد معيار لتضمين الأجهزة في تحديد عند إجراء بحث باسم تطبيق Kaspersky.

توفر القائمة أسماء التطبيقات مع الأدوات الإضافية للإدارة فقط والمثبتة على محطة عمل المسؤول.

إذا لم يتم تحديد تطبيق، لن يتم تطبيق المعيار.

- **إصدار التطبيق**

في حقل الإدخال، يمكنك تحديد معيار لتضمين الأجهزة في تحديد عند إجراء بحث برقم إصدار تطبيق Kaspersky.

إذا لم يتم تحديد رقم إصدار، لن يتم تطبيق المعيار.

- **اسم التحديث الحرج**

في حقل الإدخال، يمكنك تحديد معيار للأجهزة المشمولة في التحديد عند إجراء بحث باسم التطبيق أو برقم حزمة التحديث.

إذا تم ترك الحقل فارغًا، لن يتم تطبيق المعيار.

- **آخر تحديث للوحدات**

يمكنك استخدام هذا الخيار لتعيين معيار للبحث في الأجهزة على وقت آخر تحديث للوحدات النمطية الخاصة بالتطبيقات المثبتة على تلك الأجهزة.

إذا تم تحديد خانة الاختيار هذه، يمكنك تحديد في حقل الإدخال الفاصل الزمني (الوقت والتاريخ) الذي تم خلاله إجراء التحديث الأخير للوحدات النمطية المثبتة على تلك الأجهزة.

إذا تم إلغاء خانة الاختيار هذه، لن يتم تطبيق المعيار.

تكون خانة الاختيار غير محددة بشكل افتراضي.

- **الجهاز مُدار بواسطة Kaspersky Security Center 14**

في هذه القائمة المنسدلة، يمكنك تضمين الأجهزة المدارة بواسطة Kaspersky Security Center Linux في التحديد:

- **نعم**. يشمل التطبيق في الاختيار الأجهزة المدارة بواسطة Kaspersky Security Center Linux في الاختيار.
- **لا**. يشمل التطبيق الأجهزة الموجودة في التحديد ما لم تكن مدارة من خلال Kaspersky Security Center Linux.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

- **تم تثبيت تطبيق الأمان**

في هذه القائمة المنسدلة، يمكنك تضمين جميع الأجهزة المدارة المثبت عليها تطبيق الأمان في التحديد:

- **نعم**. يشمل التطبيق في الاختيار جميع الأجهزة المدارة بواسطة تطبيق الأمان الذي تم تثبيته:
- **لا**. يشمل التطبيق في الاختيار جميع الأجهزة غير المثبت عليها تطبيق الأمان.
- **لم يتم تحديد قيمة**. لن يتم تطبيق المعيار.

نظام التشغيل

في القسم **نظام التشغيل**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لنوع نظام التشغيل الخاص بهم.

- **إصدار نظام التشغيل**

إذا تم تحديد خانة الاختيار، فيمكنك تحديد نظام تشغيل من القائمة. يتم تضمين الأجهزة المثبت عليها أنظمة التشغيل المحددة في نتائج البحث.

- **حجم نظام التشغيل بالبت**

في القائمة المنسدلة، يمكنك تحديد بنية نظام التشغيل والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز (**غير معروف**, **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**

في هذا الحقل، يمكنك تحديد إصدار حزمة نظام التشغيل (بتنسيق X.Y)، والتي ستحدد كيفية تطبيق قاعدة النقل على الجهاز. وبشكل افتراضي، لا يتم تحديد أي قيمة إصدار.

- **نظام التشغيل بناء**

لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

رقم نسخة نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك رقم نسخة مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام النسخة باستثناء الرقم المحدد.

- **معرف تحرير نظام التشغيل**

لا يكون هذا الإعداد قابلًا للتطبيق إلا على أنظمة التشغيل Windows.

معرف إصدار (ID) نظام التشغيل. يمكنك تحديد ما إذا كان نظام التشغيل المحدد يجب أن يمتلك معرف إصدار مماثل أو سابق أو أحدث. يمكنك أيضًا تكوين البحث عن جميع أرقام معرف الإصدار باستثناء الرقم المحدد.

حالة الجهاز

في القسم **حالة الجهاز**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على وصف حالة الأجهزة من التطبيق المدار:

- **حالة الجهاز**

القائمة المنسدلة التي يمكنك فيها تحديد إحدى حالات الجهاز: موافق، أو حرج، أو تحذير.

- **وصف حالة الجهاز**

يمكنك في هذا الحقل، تحديد خانات الاختيار بجانب الشروط التي تحدد، إن تم استيفائها، إحدى الحالات التالية لجهاز الكمبيوتر: موافق أو حرج أو تحذير.

- **حالة الجهاز المحددة بواسطة التطبيق**

يمكنك في القائمة المنسدلة تحديد حالة الحماية في الوقت الحقيقي. يتم تضمين الأجهزة مع حالة الحماية في الوقت الحقيقي في التحديد.

مكونات الحماية

في القسم **مكونات الحماية**، يمكنك إعداد معايير لتضمين الأجهزة في تحديد بناءً على حالة الحماية الخاصة بها:

- **تم إصدار قاعدة البيانات**

إذا تم تحديد هذا الخيار، يمكنك البحث عن أجهزة العميل حسب تاريخ إصدار قاعدة بيانات تطبيق مكافحة الفيروسات. في حقول الإدخال، يمكنك تعيين الفاصل الزمني الذي يتم إجراء البحث بناءً عليه.

يتم تعطيل هذا الخيار افتراضيًا.

- **عملية الفحص الأخيرة**

إذا تم تمكين هذا الخيار، فيمكنك البحث عن أجهزة العميل حسب وقت آخر فحص للفيروسات. في حقول الإدخال، يمكنك تحديد الفترة الزمنية التي تم فيها آخر فحص للفيروسات.

يتم تعطيل هذا الخيار افتراضيًا.

- **إجمالي عدد التهديدات المكتشفة**

إذا تم تمكين هذا الخيار، يمكنك البحث عن أجهزة العميل حسب عدد الفيروسات التي تم العثور عليها. في حقول الإدخال، يمكنك تعيين قيم الحد الأدنى والأعلى لعدد الفيروسات التي تم العثور عليها.

يتم تعطيل هذا الخيار افتراضيًا.

سجل التطبيقات

في القسم **سجل التطبيقات**، يمكنك إعداد معايير البحث عن الأجهزة وفقًا للتطبيقات المثبتة عليها:

- **اسم التطبيق**

القائمة المنسدلة التي يمكنك فيها تحديد أي تطبيق. يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

- **إصدار التطبيق**

يمكنك في حقل الإدخال تحديد إصدار التطبيق المحدد.

- **المورّد**

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة لأي تطبيق مثبت على الجهاز.

- **حالة التطبيق**

يمكنك في القائمة المنسدلة تحديد حالة أي تطبيق (مثبت، غير مثبت). سيتم تضمين الأجهزة التي تم تثبيت التطبيق المحدد أو لم يتم تثبيته عليها، بناءً على الحالة المحددة، في التحديد.

- **بحث حسب التحديث**

إذا تم تمكين هذا الخيار، فسيتم إجراء البحث باستخدام تفاصيل تحديثات التطبيقات المثبتة على الأجهزة ذات الصلة. بعد تحديد خانة الاختيار، تتغير الحقول **اسم التطبيق** و**إصدار التطبيق** و**حالة التطبيق** إلى **اسم التحديث** و**إصدار التحديث** و**الحالة** على التوالي.

يتم تعطيل هذا الخيار افتراضيًا.

- **اسم تطبيق الأمان غير المتوافق**

القائمة المنسدلة التي يمكنك فيها تحديد تطبيقات الحماية الخاصة بالجهة الخارجية. خلال البحث، يتم تضمين الأجهزة التي يتم تثبيت التطبيق المحدد عليها في التحديد.

- **علامة التطبيق**

يمكنك في القائمة المنسدلة تحديد علامة التطبيق. يتم تضمين جميع الأجهزة المثبت عليها تطبيقات مشتملة على العلامة المحددة في الوصف، في تحديد الجهاز.

- **التطبيق على الأجهزة بدون العلامات المحددة**

إذا تم تمكين هذا الخيار، فسيتضمن التحديد أجهزة أوصافها لا تحتوي على أي من العلامات المحددة.

إذا تم تعطيل هذا الخيار، فلن يتم تطبيق المعيار.

يتم تعطيل هذا الخيار افتراضيًا.

سجل الأجهزة

في القسم **سجل الأجهزة**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناء على الأجهزة المثبتة:

- **الجهاز**

يمكنك في القائمة المنسدلة تحديد نوع الوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث.

يدعم الحقل البحث بالنص الكامل.

- **المورّد**

يمكنك في القائمة المنسدلة تحديد اسم الشركة المصنعة للوحدة. يتم تضمين جميع الأجهزة الموجود بها هذه الوحدة في نتائج البحث.

يدعم الحقل البحث بالنص الكامل.

- **اسم الجهاز**

سيتم تضمين الجهاز ذي الاسم المحدد في التحديد.

- **الوصف**

وصف الجهاز أو وحدة الجهاز. سيتم تضمين الأجهزة ذات الوصف المحدد في هذا الحقل في التحديد.

يمكن إدخال وصف الجهاز بأي تنسيق في نافذة خصائص هذا الجهاز. يدعم الحقل البحث بالنص الكامل.

- **بائع الجهاز**

اسم الشركة المصنعة للجهاز. سيتم تضمين الأجهزة التي تنتجها الشركة المصنعة المحددة في هذا الحقل في التحديد.

يمكنك إدخال اسم الشركة المصنعة في نافذة خصائص جهاز.

- **الرقم التسلسلي**

سيتم تضمين جميع وحدات الأجهزة ذات الرقم التسلسلي المحددة في هذا الحقل في التحديد.

- **رقم المخزون**

سيتم تضمين الأجهزة ذات رقم المخزون والمحدد في هذا الحقل في التحديد.

- **المستخدم**

سيتم تضمين جميع وحدات أجهزة المستخدم المحدد في هذا الحقل في التحديد.

- **الموقع**

موقع جهاز أو وحدة أجهزة (على سبيل المثال، في المقر الرئيسي أو مكتب فرعي). سيتم تضمين أجهزة الكمبيوتر أو الأجهزة الأخرى التي تم نشرها في الموقع المحدد في هذا الحقل في التحديد.

يمكنك وصف موقع جهاز بأي تنسيق في نافذة خصائص هذا الجهاز.

- **سرعة وحدة المعالجة المركزية (CPU) (بالميجاهرتز)**

نطاق تردد وحدة المعالجة المركزية. سيتم تضمين الأجهزة ذات وحدة المعالجة المركزية التي تتطابق مع نطاق التردد في حقوق الإدخال هذه (شامل) في التحديد.

- **مراكز CPU الظاهرية**

نطاق عدد النوى الظاهري في وحدة معالجة مركزية. سيتم تضمين أجهزة الكمبيوتر ذات وحدات المعالجة المركزية والتي تتطابق مع النطاق في حقوق الإدخال هذه (شامل) في التحديد.

- **حجم القرص الثابت بالجيجابايت**

نطاق القيم لحجم محرك القرص الثابت على الجهاز. سيتم تضمين الأجهزة ذات محركات الأقراص الثابتة والتي تطابق مع النطاق في حقوق الإدخال هذه (شامل) في التحديد.

- **حجم ذاكرة الوصول العشوائي RAM، بالميجابايت**

نطاق القيم لحجم ذاكرة الوصول العشوائي للجهاز. سيتم تضمين الأجهزة التي تحتوي على ذاكرة الوصول العشوائي، والتي تطابق النطاق في حقول الإدخال هذه (ضمناً) في التحديد.

الأجهزة الظاهرية

في القسم **الأجهزة الظاهرية**، يمكنك إعداد المعايير لتضمين الأجهزة في التحديد بناءً على ما إذا كانت تعد أجهزة ظاهرية أو جزءًا من البنية الأساسية لسطح المكتب الافتراضي (VDI):

- **هذا جهاز ظاهري**

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- **ليس هامًا**.
- **لا**. البحث عن الأجهزة التي لا تعد أجهزة ظاهرية.
- **نعم**. البحث عن الأجهزة التي تعد أجهزة ظاهرية.

- **نوع الجهاز الظاهري**

يمكنك في القائمة المنسدلة تحديد الشركة المصنعة للجهاز الظاهري.

هذه القائمة المنسدلة متاحة إذا تم تحديد القيمة **نعم** أو **ليس هامًا** تم تحديد القيمة **هذا جهاز ظاهري** في القائمة المنسدلة.

- **جزء من البنية الأساسية لسطح المكتب الافتراضي**

يمكنك في القائمة المنسدلة تحديد الخيارات التالية:

- **ليس هامًا**.
- **لا**. البحث عن الأجهزة التي لا تعد جزءًا من البنية الأساسية لسطح المكتب الافتراضي.
- **نعم**. البحث عن الأجهزة التي تعد جزءًا من البنية الأساسية لسطح المكتب الافتراضي (VDI).

المستخدمون

في القسم **المستخدمون**، يمكنك إعداد المعايير لتضمين الأجهزة في التحديد بحسب حسابات المستخدمين الذين قاموا بتسجيل الدخول إلى نظام التشغيل.

- **آخر مستخدم سجّل الدخول إلى النظام**

إذا تم تمكين هذا الخيار، فانقر فوق زر **استعراض** لتحديد حساب مستخدم. تشتمل نتائج البحث على الأجهزة التي قام مستخدم محدد بإجراء آخر تسجيل دخول عليها إلى النظام.

- **مستخدم قام بتسجيل الدخول إلى النظام مرة واحدة على الأقل**

إذا تم تمكين هذا الخيار، فانقر فوق زر **استعراض** لتحديد حساب مستخدم. ستتضمن نتائج البحث الأجهزة التي قام مستخدم محدد بتسجيل الدخول عليها مرة واحدة على الأقل.

مشاكل تؤثر على الحالة في التطبيقات المُدارة

في القسم **مشاكل تؤثر على الحالة في التطبيقات المُدارة**، يمكنك تحديد المعايير التي ستُستخدم لتضمين الأجهزة في التحديد وفقًا لقائمة المشكلات المحتملة التي يتم اكتشافها بواسطة التطبيق المُدار. إذا كانت مشكلة واحدة على الأقل من المشكلات التي حددتها موجودة على جهاز، فسيتم تضمين الجهاز في القسم. في حالة اختيار مشكلة مدرجة للعديد من التطبيقات، فلديك الخيار لتحديد هذه المشكلة في جميع القوائم تلقائيًا.

وصف حالة الجهاز

يمكنك تحديد خانات الاختيار الخاصة بأوصاف الحالات من تطبيق مدار؛ وفور استلام هذه الحالات، سيتم تضمين الأجهزة في التحديد. في حالة اختيار حالة مدرجة للعديد من التطبيقات، فلديك الخيار لتحديد هذه الحالة في جميع القوائم تلقائيًا.

حالات المكونات في التطبيقات المُدارة

في القسم **حالات المكونات في التطبيقات المُدارة**، يمكنك تكوين معايير لتضمين الأجهزة في تحديد بناءً على حالات المكونات في التطبيقات المُدارة:

- **حالة منع تسريب البيانات**

البحث عن الأجهزة حسب حالة منع تسرب البيانات (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).

مكونات التطبيق

يحتوي هذا القسم على قائمة المكونات لهذه التطبيقات التي لديها مكونات إدارة إضافية مطابقة مُثبتة في وحدة تحكم الإدارة.

في القسم **مكونات التطبيق**، يمكنك تحديد معايير لتضمين الأجهزة في تحديد وفقًا للحالات ولأرقام الإصدار المكونات التي تشير للتطبيق الذي حددته:

- **الحالة**

البحث عن الأجهزة وفقًا لحالة المكون المُرسلة بواسطة تطبيق إلى خادم الإدارة. يمكنك تحديد أحد الحالات التالية: لا بيانات من الجهاز، أو متوقف، أو بدء التشغيل، أو تم الإيقاف مؤقتًا، أو قيد التشغيل، أو اختلال تشغيل أو غير مثبت. إذا كان للمكون المحدد للتطبيق المُثبت على جهاز مُدار حالة محددة، فإنه يتم تضمين الجهاز في تحديد الجهاز.

الحالات المرسلة بواسطة التطبيقات:

- بدء تشغيل—يكون المكون في عملية التهيئة في الوقت الحالي.
- قيد التشغيل—يكون المكون ممكنًا ويعمل على النحو الصحيح.
- تم الإيقاف مؤقتًا—تم تعليق المكون، على سبيل المثال، بعد إيقاف المستخدم للحماية مؤقتًا في التطبيق المُدار.
- اختلال التشغيل—حدث خطأ أثناء تشغيل المكون.
- متوقف—تم تعطيل المكون وهو لا يعمل في الوقت الحالي.
- غير مثبت—لم يقم المستخدم بتحديد المكون للتثبيت عند تكوين التثبيت المخصص للتطبيق.

بخلاف التطبيقات الأخرى، فإن الحالة لا بيانات من الجهاز لا تُرسل بواسطة التطبيقات. يُظهر هذا الخيار عدم امتلاك التطبيقات لمعلومات حول حالة المكون المحدد. على سبيل المثال، قد يحدث هذا عندما يكون المكون المحدد لا ينتمي لأي من التطبيقات المثبتة على الجهاز، أو عند إيقاف تشغيل الجهاز.

- **الإصدار**

البحث عن الأجهزة وفقًا لرقم الإصدار للمكون الذي حددته في القائمة. يمكنك كتابة رقم الإصدار، على سبيل المثال `3.4.1.0`، ثم تحديد ما إذا كان المكون المحدد يجب أن يمتلك إصدارًا مماثلاً أو إصدارًا سابقًا أو إصدارًا أحدث. يمكنك أيضًا تكوين البحث عن جميع الإصدارات عدا الإصدار المحدد.

الدليل المرجعي لـ API

تم تصميم هذا الدليل المرجعي من Kaspersky Security Center OpenAPI للمساعدة في المهام التالية:

- الأتمتة والتخصيص. يمكنك أتمتة المهام التي قد لا ترغب في معالجتها يدويًا. على سبيل المثال، يمكنك بصفتك مشرفًا استخدام Kaspersky Security Center OpenAPI لإنشاء وتشغيل البرامج النصية التي من شأنها تسهيل تطوير بنية مجموعات الإدارة والحفاظ على تحديث الهيكل.
- التنمية المخصصة. باستخدام OpenAPI، يمكنك تطوير تطبيق عميل.

يمكنك استخدام حقل البحث في الجزء الأيمن من الشاشة لتحديد موقع المعلومات التي تحتاج إليها في الدليل المرجعي OpenAPI.

الدليل المرجعي لـ OPENAPI

نماذج من البرامج النصية

يحتوي الدليل المرجعي OpenAPI على نماذج من برامج Python النصية المدرجة في الجدول أدناه. توضح العينات كيف يمكنك استدعاء أساليب OpenAPI وإنجاز المهام المختلفة تلقائيًا لحماية شبكتك، على سبيل المثال، إنشاء تسلسل هرمي "أساسي/ثانوي"، أو تشغيل المهام في Kaspersky Security Center، أو تعيين نقاط التوزيع . يمكنك تشغيل النماذج كما هي أو إنشاء البرامج النصية الخاصة بك بناءً على النماذج.

لاستدعاء أساليب OpenAPI وتشغيل البرامج النصية:

1. قم بتنزيل أرشيف KlAkOAPI.tar.gz . يتضمن هذا الأرشيف حزمة ونماذج KlAkOAPI (يمكنك نسخها من الأرشيف أو الدليل المرجعي OpenAPI).
2. قم بتثبيت حزمة KlAkOAPI من أرشيف KlAkOAPI.tar.gz على جهاز مثبت عليه خادم الإدارة.

يمكنك استدعاء أساليب OpenAPI وتشغيل النماذج والبرامج النصية الخاصة بك فقط على الأجهزة حيث تم تثبيت خادم الإدارة وحزمة KlAkOAPI.

المطابقة بين سيناريوهات المستخدمين وعينات من أساليب Kaspersky Security Center OpenAPI

عينة	الغرض من العينة	سيناريو
سجل KlAkParams	يمكنك استخلاص البيانات ومعالجتها وجمعها باستخدام هيكل بيانات `KlAkParams`. يوضح النموذج كيفية العمل مع هيكل البيانات هذا. قد يكون إخراج النموذج موجودًا بطرق مختلفة. يمكنك الحصول على البيانات لإرسال طريقة HTTP أو استخدامها في التعليمات البرمجية الخاصة بك.	المراقبة وإعداد التقارير
إنشاء وحذف تسلسل هرمي"رئيسي/ثانوي"	يمكنك إضافة خادم إدارة كخادم إدارة ثانوي، والذي يقوم بإنشاء تسلسل هرمي "رئيسي/ثانوي". بالتناوب، يمكنك فصل خادم الإدارة الثانوي من التسلسل الهرمي.	إنشاء تسلسل هرمي لخوادم الإدارة، وإضافة خادم إدارة ثانوي وحذف التسلسل الهرمي لخوادم الإدارة
تنزيل ملفات قائمة الشبكة عبر بوابة الاتصال للمضيف المحدد	يمكنك الاتصال بوكيل الشبكة على الجهاز المطلوب عن طريق استخدام بوابة اتصال، وبعدها قم بتنزيل ملف بقائمة الشبكات على جهازك.	تعديل نقاط التوزيع وبوابات الاتصال
قم بتثبيت مفتاح ترخيص مخزن في مستودع خادم الإدارة الرئيسي على خوادم الإدارة الثانوية	يمكنك الاتصال بخادم الإدارة الرئيسي، وتنزيل مفتاح الترخيص المطلوب منه، ونقل هذا المفتاح إلى جميع خوادم الإدارة الثانوية المضمنة في التسلسل الهرمي.	ترخيص التطبيقات المُدارة
إنشاء تقرير بحقوق المستخدم النشطة	تستطيع إنشاء تقارير مختلفة . يمكنك على سبيل المثال إنشاء تقرير عن حقوق المستخدم النشطة باستخدام هذا النموذج. يصف هذا التقرير الحقوق التي يمتلكها المستخدم اعتمادًا على مجموعته ودوره. يمكنك تنزيل التقرير بصيغة HTML أو PDF أو Excel.	إنشاء تقرير وعرضه
بدء مهمة الجهاز	يمكنك الاتصال بوكيل الشبكة على الجهاز المطلوب عن طريق استخدام بوابة اتصال ثم تشغيل المهمة المطلوبة.	بدء مهمة يدويًا

تسجيل نقاط التوزيع للأجهزة في مجموعة	يمكنك تعيين الأجهزة المُدارة كنقاط توزيع (كانت معروفة سابقًا باسم وكلاء التحديث).	تحديث قواعد بيانات Kaspersky وتطبيقاته
عد كل المجموعات	يمكنك تنفيذ العديد من الإجراءات على مجموعات الإدارة. يوضح النموذج كيفية فعل ذلك: • احصل على معرّف لمجموعة الجذر "الأجهزة المُدارة" • تنقل عبر التسلسل الهرمي للمجموعة • استرجع التسلسل الهرمي الكامل والموسع للمجموعات، جنبًا إلى جنب مع أسمائها وتداخلها	تكوين خادم الإدارة
عد المهام والاستعلام عن إحصائيات المهام وتشغيل مهمة	يمكنك معرفة المعلومات التالية: • تاريخ تقدم المهمة • حالة المهمة الحالية • عدد المهام في حالات مختلفة يمكنك أيضًا تشغيل مهمة. بشكل افتراضي، يقوم النموذج بتشغيل مهمة بعد إخراج الإحصائيات.	مراقبة تنفيذ المهمة
إنشاء وتشغيل مهمة	يمكنك إنشاء مهمة. حدد معلمات المهمة التالية في النموذج: • النوع • طريقة التشغيل • الاسم • مجموعة الأجهزة التي سيتم استخدام المهمة لها بشكل افتراضي، يقوم النموذج بإنشاء مهمة من النوع "إظهار الرسالة". يمكنك تشغيل هذه المهمة لجميع الأجهزة المدارة لخادم الإدارة. يمكنك إذا لزم الأمر تحديد معلمات المهمة الخاصة بك.	إنشاء مهمة
عد مفاتيح الترخيص	يمكنك الحصول على قائمة بجميع مفاتيح الترخيص النشطة لتطبيقات Kaspersky المثبتة على الأجهزة المُدارة لخادم الإدارة. تحتوي القائمة على بيانات مفصلة حول كل مفتاح ترخيص، مثل الاسم أو النوع أو تاريخ انتهاء الصلاحية.	عرض معلومات حول مفاتيح التراخيص قيد الاستخدام
إنشاء والعثور على مستخدم داخلي	يمكنك إنشاء حساب لمزيد من العمل.	تحديد الحساب لتشغيل خادم الإدارة
إنشاء فئة مخصصة	يمكنك إنشاء فئة التطبيق بالمعلمات المطلوبة.	إنشاء فئة تطبيق مضافًا إليها المحتوى يدويًا
عد المستخدمين باستخدام SrvView	يمكنك استخدام الفئة SrvView لطلب معلومات مفصلة من خادم الإدارة. يمكنك على سبيل المثال الحصول على قائمة المستخدمين عن طريق استخدام هذا النموذج.	إدارة حسابات المستخدمين

التطبيقات التي تتفاعل مع Kaspersky Security Center عبر OpenAPI

تتفاعل بعض التطبيقات مع Kaspersky Security Center عبر OpenAPI. تشمل هذه التطبيقات على سبيل المثال، Kaspersky Anti Targeted Attack Platform أو Kaspersky Security for Virtualization. يمكن أن يكون هذا أيضًا تطبيق عميل مخصص تم تطويره من خلالك بناءً على OpenAPI.

التطبيقات التي تتفاعل مع Kaspersky Security Center عبر OpenAPI تتصل بخادم الإدارة. في حالة تكوين ملف قائمة السماح لعناوين IP للاتصال بخادم الإدارة، فأضف عناوين IP للأجهزة حيث يتم تثبيت التطبيقات التي تستخدم Kaspersky Security Center OpenAPI. لمعرفة ما إذا كان التطبيق الذي تستخدمه يعمل بواسطة OpenAPI، راجع تعليمات هذا التطبيق.

التكامل بين Kaspersky Security Center Web Console وحلول Kaspersky 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 (KATA / KEDR Web Console). إذا كنت تستخدم كلاً من Kaspersky Security Center 14 Web Console وKATA/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 نافذة التطبيق الرئيسية، انقر على **إعدادات وحدة التحكم** في الجزء العلوي من الشاشة.
2. في القائمة المنسدلة، حدد **التكامل**.

   ستفتح نافذة إعدادات وحدة التحكم.
3. في علامة التبويب **التكامل**، أدخل رابط KATA/KEDR Web Console في حقل **عنوان URL إلى KATA/KEDR Web Console**.
4. 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

من أجل تكوين التفاعل بين Kaspersky Security Center وتطبيق أو حل آخر من Kaspersky، مثل Kaspersky Managed Detection and Response (الذي يُشار إليه كذلك باسم MDR)، يجب عليك إنشاء اتصال في الخلفية بين Kaspersky Security Center Web Console وخادم الإدارة. يمكنك إنشاء هذا الاتصال فقط إذا كان حسابك له حق تعديل قوائم التحكم في الوصول للكائن مباشرةً في المجال الوظيفي **الميزات العامة: أذونات المستخدم**.

يمكنك تكوين التفاعل فقط بين Kaspersky Managed Detection and Response والإصدار الذي يستخدم Windows من Kaspersky Security Center.

لإنشاء اتصال في الخلفية:

1. في القائمة المنسدلة **إعدادات وحدة التحكم**، حدد **التكامل**.

   ستفتح نافذة **إعدادات وحدة التحكم**.
2. حدد تبويب **التكامل**.
3. في علامة التبويب **التكامل**، حدد القسم **التكامل**.

4. قم بتشغيل زر التشغيل لإنشاء اتصال في الخلفية إلى الموضع: **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 حسابًا للاتصال في الخلفية، ويتم استخدام هذا الحساب كحساب خدمة للحفاظ على التفاعل بين Kaspersky Security Center وتطبيق أو حل آخر من Kaspersky. اسم حساب الخدمة هذا يضم البادئة NWCSvcUser. يقوم خادم الإدارة تلقائيًا بتغيير كلمة مرور حساب الخدمة مرة واحدة كل 30 يومًا لأسباب أمنية. لا يمكنك حذف حساب الخدمة يدويًا. خادم الإدارة يحذف هذا الحساب تلقائيًا عند تعطيل اتصال عبر الخدمات. خادم الإدارة ينشئ حساب خدمة واحد لكل Kaspersky Security Center 14 Web Console في الإدارة ويعيّن جميع حسابات الخدمة لمجموعة الأمان التي تحمل الاسم ServiceNwcGroup. خادم الإدارة ينشئ مجموعة الأمان هذه تلقائيًا أثناء عملية تثبيت Kaspersky Security Center. لا يمكنك حذف مجموعة الأمان هذه يدويًا.

الاتصال بالدعم الفني

يصف هذا القسم كيفية الحصول على الدعم الفني والبنود التي تتوافر على أساسها.

كيفية الحصول على الدعم الفني

إذا لم تتمكن من العثور على حل لمشكلتك في مستندات Kaspersky Security Center Linux أو في أحد مصادر المعلومات عن Kaspersky Security Center Linux، اتصل بخدمة الدعم الفني. سيجيب أخصائيو خدمة الدعم الفني على كافة تساؤلاتك المتعلقة بتثبيت Kaspersky Security Center Linux واستخدامه.

Kaspersky توفّر الدعم لتطبيق Kaspersky Security Center Linux أثناء دورة حياته (انظر صفحة دورة حياة دعم المنتج). قبل الاتصال بالدعم الفني، يرجى قراءة قواعد الدعم.

يمكنك الاتصال بالدعم الفني بإحدى الطرق التالية:

- من خلال زيارة موقع الويب للدعم الفني
- عن طريق إرسال طلب إلى الدعم الفني من بوابة Kaspersky CompanyAccount

الحصول على الدعم الفني عبر الهاتف

يمكنك الاتصال بأخصائيين الدعم الفني من معظم المناطق حول العالم. يمكنك العثور على معلومات حول كيفية الحصول على الدعم الفني في منطقتك ومعلومات جهات الاتصال الخاصة بالدعم الفني على موقع الويب الخاص بخدمة العملاء في Kaspersky.

قبل الاتصال بالدعم الفني، يرجى قراءة قواعد الدعم.

الدعم الفني من خلال Kaspersky CompanyAccount

حساب شركة Kaspersky هي بوابة للشركات التي تستخدم تطبيقات Kaspersky. تم تصميم بوابة Kaspersky CompanyAccount لتسهيل التفاعل بين المستخدمين والأخصائيين في Kaspersky من خلال طلبات عبر الإنترنت. يمكنك استخدام Kaspersky CompanyAccount لتتبع حالة طلباتك على الإنترنت وتخزين سجل لها أيضًا.

يمكنك تسجيل جميع موظفي المؤسسة الخاصة بك بحساب موحد على Kaspersky CompanyAccount. يسمح لك الحساب الموحد بإدارة الطلبات الإلكترونية المقدمة من الموظفين المسجلين إلى Kaspersky بصورة مركزية وكذلك إدارة امتيازات هؤلاء الموظفين عبر Kaspersky CompanyAccount.

تتاح بوابة Kaspersky CompanyAccount باللغات التالية:

- الإنجليزية
- الإسبانية
- الإيطالية
- الألمانية

- البولندية
- البرتغالية
- الروسية
- الفرنسية
- اليابانية

لتعلم المزيد بشأن حساب شركة Kaspersky، قم بزيارة موقع ويب الدعم الفني.

مصادر المعلومات المتعلقة بالتطبيق

صفحة Kaspersky Security Center على الموقع الإلكتروني لـ Kaspersky

في صفحة Kaspersky Security Center الموجودة في الموقع الإلكتروني لـ Kaspersky ، يمكنك عرض معلومات عامة حول التطبيق ووظائفه ومزاياه.

صفحة Kaspersky Security Center على قاعدة المعارف

قاعدة المعارف هي قسم على الموقع الإلكتروني الخاص بالدعم الفني لـ Kaspersky.

على صفحة Kaspersky Security Center Linux في قاعدة المعارف، يمكنك قراءة مقالات والتي تُقدم معلومات مفيدة وتوصيات وإجابات على الأسئلة المتكررة حول كيفية شراء التطبيق وتثبيته واستخدامه.

قد توفر المقالات الموجودة في قاعدة المعارف إجابات عن الأسئلة التي تتعلق بكل من Kaspersky Security Center وكذلك تطبيقات Kaspersky الأخرى. قد تشتمل أيضًا المقالات في قاعدة المعارف على أخبار الدعم الفني.

مناقشة تطبيقات Kaspersky مع المجتمع

إذا لم يكن سؤالك يتطلب توفير إجابة فورية، فيمكنك مناقشته مع خبراء Kaspersky والمستخدمين الآخرين في منتدانا .

في هذا المنتدى، يمكنك عرض موضوعات المناقشة، ونشر تعليقاتك، وإنشاء موضوعات جديدة للمناقشة.

يلزم وجود اتصال بالإنترنت للوصول إلى مصادر موقع الويب.

إذا لم تستطع العثور على حل لمشكلتك، قم بالاتصال بالدعم الفني.

المشكلات المعروفة

Kaspersky Security Center Linux يحتوي على عدد من القيود التي ليست حرجة لتشغيل التطبيق:

- في مهمة تنزيل التحديثات إلى مخزن خادم الإدارة ومهمة تنزيل التحديثات إلى مستودعات نقاط التوزيع، لا تعمل مصادقة المستخدم إذا قمت بتحديد مجلد محلي أو شبكة محمي بكلمة مرور كمصدر تحديث. لحل هذه المشكلة، أولاً حمّل المجلد المحمي بكلمة مرور، ثم حدد بيانات الاعتماد المطلوبة، على سبيل المثال، عن طريق نظام التشغيل. بعد ذلك، يمكنك تحديد هذا المجلد كمصدر تحديث في مهمة تنزيل التحديث. لن يطلب Kaspersky Security Center إدخال بيانات الاعتماد.

- لا تبدأ مهمة تغيير خادم الإدارة تلقائيًا بعد تعيين الخيار **فورًا** في جدول المهام وحفظ التغييرات.

- 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.

- الإعدادات المقفلة في السياسة الرئيسية لـ Kaspersky Endpoint Security for Linux موروثة، ولكنها غير مقفلة في السياسات الفرعية.

- قد لا تكون معلومات الأجهزة المرسلة من جهاز مُدار إلى خادم الإدارة كاملة؛ وقد لا يتم تحديد بعض عناصر الأجهزة.

- يمكن حذف فئة التطبيق التي أضفتها إلى ميزة التحكم في التطبيق في سياسة Kaspersky Endpoint Security for Linux.

- يرسل الجهاز المُدار الذي يحتوي على أكثر من محول شبكة واحد معلومات خادم الإدارة حول عنوان MAC لمحول الشبكة غير المستخدم للاتصال بخادم الإدارة.

- إذا قمت بتحديد حسابات مستخدمين مخصصة في معلمات webConsoleAccount و managementServiceAccount في ملف استجابة لتثبيت Kaspersky Security Center 14 Web Console وكانت هذه الحسابات تنتمي إلى مجموعات أمان مختلفة ، فلن يعمل Kaspersky Security Center 14 Web Console بعد التثبيت.

- في إصدار 64 بت من Astra Linux، يتعذّر ترقية حزمة klnagent-astra باستخدام حزمة klnagent64_14: ستتم إزالة الحزمة القديمة klnagent64-astra، وسيتم تثبيت الحزمة الجديدة klnagent64 بدلاً من الترقية، وبالتالي فإن الرمز الجديد للجهاز المزود بحزمة klnagent64_14 سوف تتم اضافته. يمكنك إزالة الرمز القديم لهذا الجهاز.

مسرد المصطلحات

HTTPS

بروتوكول أمان لنقل البيانات باستخدام التشفير بين مستعرض وخادم الويب. يتم استخدام HTTPS للوصول إلى المعلومات المقيدة، مثل بيانات الشركة أو البيانات المالية.

JavaScript

لغة برمجة تعمل على توسيع أداء صفحات الويب. يمكن لصفحات الويب التي تم إنشاؤها باستخدام JavaScript تنفيذ الوظائف (على سبيل المثال، تغيير عرض عناصر الواجهة أو فتح نوافذ إضافية) بدون تحديث صفحة الويب باستخدام البيانات الجديدة من مستعرض الويب. لعرض الصفحات التي تم إنشاؤها باستخدام JavaScript، قم بتكوين دعم JavaScript في تكوين المستعرض الخاص بك.

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 معًا مع خادم الإدارة. تم تصميم خادم الويب لنقل حزم التثبيت المستقلة وملفات تعريف iOS MDM وملفات من المجلد المشترك، عبر أحد الشبكات.

SSL

بروتوكول تشفير البيانات المستخدمة في الإنترنت والشبكات المحلية. يتم استخدام طبقة مآخذ توصيل آمنة (SSL) في تطبيقات الويب لإنشاء اتصال آمن بين العميل والخادم.

أداة التحقق من سلامة نظام Kaspersky Security Center (SHV)

تم تصميم مكون Kaspersky Security Center للتحقق من إمكانية تشغيل نظام التشغيل في حالة التشغيل المتزامن لـ Kaspersky Security Center وMicrosoft 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 التثبيت للتثبيت البعيد للتطبيقات (محتوى المجلدات: الحزم وإزالة تثبيت 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 المحلي

تثبيت تطبيق أمن على جهاز على شبكة الشركة الذي يفترض بدء تشغيل التثبيت اليدوي من حزمة توزيع تطبيق الأمان أو بدء التشغيل اليدوي لحزمة تثبيت منشورة كان قد تم تنزيلها مسبقًا على الجهاز.

التثبيت اليدوي

تثبيت تطبيق أمن على جهاز في شبكة الشركة من حزمة التثبيت. يتطلب التثبيت اليدوي مشاركة مسؤول أو متخصص تقنية معلومات آخر. ويتم إجراء التثبيت اليدوي عادة إذا تم إجراء التثبيت عن بُعد مع وجود خطأ.

التثبيت عن بُعد

تثبيت تطبيقات Kaspersky عن طريق استخدام الخدمات المقدمة بواسطة Kaspersky Security Center Linux.

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 Linux.

الحماية ضد فيروسات الشبكة

مجموعة من الإجراءات الفنية والمؤسسية التي تقلل من خطر السماح للفيروسات والبرامج الخبيثة من اختراق شبكة المؤسسة مما يمنع هجمات الشبكة والتصيد الاحتيالي وتهديدات أخرى. يزداد أمن الشبكة عندما تستخدم تطبيقات وخدمات الأمن وعندما تُطبق وتلتزم بسياسة أمن بيانات الشركة.

الشهادة المشتركة

شهادة تهدف إلى تحديد جهاز محمول المستخدم

المهمة

يتم تنفيذ الوظائف التي يتم إجراؤها بواسطة تطبيق Kaspersky كمهام، مثل: حماية الملفات في الوقت الحقيقي، والفحص الكامل لجهاز الكمبيوتر، وتحديث قاعدة البيانات.

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.

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 المُثبتة واستخدام مفاتيح الترخيص وعدد التهديدات المُكتشفة وأنواعها.

حزمة التثبيت

مجموعة من الملفات التي يتم إنشاؤها للتثبيت عن بُعد لأحد تطبيقات Kaspersky باستخدام نظام الإدارة عن بُعد لـ Kaspersky Security Center. تحتوي حزمة التثبيت على مجموعة إعدادات ضرورية لتثبيت التطبيق وتشغيله فورًا بعد التثبيت. الإعدادات المقابلة للإعدادات الافتراضية للتطبيق. يتم إنشاء حزمة التثبيت باستخدام ملفات بامتداد .kpd و.kud المضمنة في مجموعة توزيع التطبيق.

حقوق المسؤول

مستوى حقوق وامتيازات المستخدم المطلوبة لإدارة كائنات Exchange ضمن مؤسسة Exchange.

خادم 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.

خطورة الحدث

خصائص الحدث الذي تمت مواجهته أثناء تشغيل تطبيق Kaspersky. توجد مستويات الخطورة التالية:

- حدث حرج
- خلل وظيفي
- تحذير
- معلومات

يمكن أن يكون للأحداث من نفس النوع مستويات خطورة مختلفة اعتمادًا على الموقف الذي وقع فيه الحدث.

خوادم تحديث Kaspersky

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

سياسة

وتحدد السياسة إعدادات التطبيق وتدير القدرة على تكوين هذا التطبيق على أجهزة كمبيوتر ضمن مجموعة الإدارة. يجب إنشاء سياسة فردية لكل تطبيق. يمكنك إنشاء سياسات متعددة للتطبيقات المثبتة على أجهزة الكمبيوتر في كل مجموعة إدارية، ولكن يمكن تطبيق سياسة واحدة فقط على كل تطبيق في الوقت نفسه ضمن مجموعة الإدارة.

شهادة خادم الإدارة

الشهادة التي يستخدمها خادم الإدارة للأغراض التالية:

- مصادقة خادم الإدارة عند الاتصال بـ Kaspersky Security Center 14 Web Console
- تفاعل آمن بين خادم الإدارة ووكلاء الشبكة على الأجهزة المدارة.
- مصادقة خوادم الإدارة عند توصيل خادم إدارة أساسي بخادم إدارة ثانوي

يتم إنشاء الشهادة تلقائيًا عند تثبيت خادم الإدارة، ومن ثم يتم تخزينها على خادم الإدارة.

عميل الشبكة

مكون Kaspersky Security Center الذي يُمكن التفاعل بين خادم الإدارة وتطبيقات Kaspersky التي يتم تثبيتها على عقدة شبكة معينة (محطة عمل أو خادم). يُعد هذا المكون مشتركًا بين جميع تطبيقات الشركة لـ Microsoft® Windows®. تتوفر إصدارات منفصلة من عميل الشبكة لتطبيقات Kaspersky التي تم تطويرها لأنظمة Unix-like OS وmacOS.

عميل خادم الإدارة (الجهاز العميل)

جهاز أو خادم أو محطة عمل يتم عليه تثبيت عميل الشبكة وتشغيل تطبيقات Kaspersky المُدارة.

فترة الترخيص

الفترة الزمنية التي يمكنك خلالها الوصول إلى ميزات التطبيق وحقوق استخدام خدمات إضافية. وتعتمد الخدمات التي يمكنك استخدامها على نوع الترخيص.

قواعد بيانات مكافحة الفيروسات

قواعد البيانات التي تحتوي على معلومات حول التهديدات الأمنية التي تهدد الجهاز والمعروفة لـ Kaspersky وقت إصدار قواعد بيانات مكافحة الفيروسات. تسمح الإدخالات في قواعد بيانات مكافحة الفيروسات باكتشاف الرمز الضار في الكائنات التي تم فحصها. يتم إنشاء قواعد بيانات مكافحة الفيروسات بواسطة أخصائيي Kaspersky ويتم تحديثها كل ساعة.

مالك الجهاز

مالك الجهاز هو مستخدم يمكن للمسؤول الاتصال به عند الحاجة إلى إجراء عمليات محددة على الجهاز.

متجر التطبيقات

مكون Kaspersky Security Center. يُستخدم متجر التطبيقات لتثبيت التطبيقات على الأجهزة التي تعمل بنظام Android والمملوكة بواسطة المستخدم. يتيح لك متجر التطبيقات نشر ملفات APK الخاصة بالتطبيقات وروابط التطبيقات في Google Play.

مجال البث

مساحة منطقية لشبكة تتمكن فيها كل العقد من تبادل البيانات باستخدام قناة بث على مستوى OSI (النموذج المرجعي الأساسي لترابط النظم المفتوحة).

مجلد النسخ الاحتياطي

مجلد خاص لتخزين نُسخ بيانات خادم الإدارة التي تم إنشاؤها باستخدام الأداة النسخ الاحتياطي.

مجموعة الإدارة

مجموعة من الأجهزة التي تم تجميعها بحسب الوظيفة وبحسب تطبيقات Kaspersky المثبتة. أجهزة تم تجميعها ككيان فردي لسهولة الإدارة. يمكن أن تتضمن المجموعة مجموعات أخرى. يمكن إنشاء سياسات جماعية ومهام جماعية لكل تطبيق يتم تثبيته في مجموعة.

مجموعة التطبيقات المرخصة

مجموعة من التطبيقات التي تم إنشاؤها على أساس معايير محددة بواسطة المسؤول (على سبيل المثال بواسطة البائع) حيث يتم الاحتفاظ بإحصاءات عمليات التثبيت على الأجهزة العميلة لها.

مجموعة الدور

مجموعة من مستخدمي الأجهزة المحمولة Exchange ActiveSync الذين تم منحهم حقوق مطابقة لحقوق المسؤول.

محطة عمل المسؤول

جهاز من ما تفتحه Kaspersky Security Center 14 Web Console. يقدم هذا المكون واجهة إدارة Kaspersky Security Center.

يتم استخدام محطة عمل المسؤول لتكوين وإدارة جهة خادم Kaspersky Security Center. باستخدام محطة عمل المسؤول، يقوم المسؤول بتأسيس وإدارة نظام حماية مركزي ضد الفيروسات لشبكة اتصال محلية (LAN) بشركة إلى تطبيقات Kaspersky.

مسؤول 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.

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 Linux.

مفتاح اشتراك إضافي

مفتاح يُصادق على حق استخدام التطبيق لكن لا يتم استخدامه حاليًا.

مفتاح مفعل

مفتاح الترخيص الذي يستخدمه التطبيق حاليًا.

ملف التعريف

مجموعة من الإعدادات الخاصة بـ الأجهزة المحمولة في 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 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 للتثبيت البعيد للتطبيقات (محتوى المجلدات: الحزم وإزالة تثبيت التحديثات).
- شهادة خادم الإدارة

نقطة توزيع

جهاز كمبيوتر مثبت عليه عميل الشبكة ويتم استخدامه لتوزيع التحديث، وتثبيت التطبيقات عن بُعد، والحصول على المعلومات حول أجهزة الكمبيوتر في مجموعة إدارة و/أو مجال البث. تم تصميم نقاط التوزيع لتقليل التحميل على خادم الإدارة أثناء توزيع التحديثات ولتحسين حركة الشبكة. يمكن تعيين نقاط التوزيع تلقائيًا، بواسطة خادم الإدارة أو يدويًا أو بواسطة المسؤول. كانت نقطة التوزيع تعرف فيما سبق بوكيل التحديث.

وحدة تحكم الإدارة

أحد مكونات Kaspersky Security Center المستندة إلى Windows (وتسمى أيضًا وحدة التحكم الإدارية المستندة إلى MMC). يوفر هذا المكون واجهة مستخدم للخدمات الإدارية لخادم الإدارة وعميل الشبكة. وحدة التحكم الإدارية هي نظير لـ Kaspersky Security Center 14 Web Console.

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 دليل التثبيت.

إشعارات العلامة التجارية

تُعد العلامات التجارية المسجلة وعلامات الخدمة ملكية خاصة لأصحابها.

Adobe وAcrobat وFlash و Shockwave وPostScript هم علامات تجارية مسجلة أو علامات تجارية لشركة Adobe في الولايات المتحدة و/أو بلدان أخرى.

إن AMD وAMD64 هي علامات تجارية أو علامات تجارية مسجلة لشركة Advanced Micro Devices, Inc.

تُعد Amazon وAmazon Web Services و AWS وAmazon EC2 وAWS Marketplace علامات مسجلة تملكها شركة Amazon.com, Inc. أو شركاتها التابعة في الولايات المتحدة الأمريكية و/أو في البلدان الأخرى.

Apache وشعار Apache هما علامتان تجاريتان لشركةApache Software Foundation.

إن وApple وAirPlay وAirDrop وAirPrint وApp Store وApple Configurator وAppleScript وFaceTime وFileVault وiBook وiBooks وiCloud وiPad وiPhone وiTunes وLeopard وmacOS وMac وMac OS وOS X وSafari وSnow Leopard وTiger وQuickTime وTouch ID هي علامات تجارية تابعة لشركة Apple Inc. ومسجّلة في الولايات المتحدة الأمريكية وبلدان ومناطق أخرى.

كلمة Bluetooth وعلامتها وشعاراتها تعتبر مملوكة لشركة Bluetooth SIG, Inc.

تُعد Ubuntu علامة تجارية مسجلة لشركة Canonical Ltd.

Cisco، وCisco Systems، وIOS هي علامات تجارية مسجلة لشركة Cisco Systems, Inc. و/أو الشركات التابعة لها في الولايات المتحدة وبلدان معينة أخرى.

تُعد Citrix وXenServer 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.

Dropbox هي علامة تجارية مملوكة لشركة Dropbox، Inc.

Firebird هي علامة تجارية مسجلة لمؤسسة Firebird Foundation.

Foxit هي علامة تجارية مسجلة لشركة Foxit Corporation.

إن FreeBSD علامة تجارية مسجلة لمؤسسة FreeBSD foundation.

Google وAndroid وChrome وChromium وDalvik وFirebase وGoogle Chrome وGoogle Earth وGoogle Play وGoogle Maps وHangouts وYouTube هي علامات تجارية لشركة Google LLC.

FusionCompute وFusionSphere علامتان تجاريتان لشركة Huawei Technologies Co.، Ltd المسجلة في الصين وبلدان أخرى.

تُعد Intel وCore وXeon علامات تجارية لشركة Intel Corporation في الولايات المتحدة و/أو بلدان أخرى.

إن IBM وQRadar علامات تجارية تابعة لشركة International Business Machines Corporation، مسجلة في العديد من البلدان حول العالم.

وعلامة Node.js هي علامة تجارية تابعة لشركة Joyent, Inc.

شركة Linux هي علامة تجارية مسجلة لصالح لشركة Linus Torvalds في الولايات المتحدة الأمريكية وبلدان أخرى.

Micro Focus هو علامة تجارية أو علامة تجارية مسجلة لشركة Micro Focus (IP) Limited أو فروعها في المملكة المتحدة والولايات المتحدة الأمريكية وبلدان أخرى.

تُعد Active Directory وActiveSync وBitLocker وExcel وForefront وInternet Explorer وInfoPath وHyper-V وMicrosoft وEdge وMultiPoint وMS-DOS وPowerShell وPowerPoint وSharePoint وSQL Server وOneNote وOutlook و Skype وTahoma وVisio وWin32 وWindows وWindows PowerShell وWindows Media وWindows Server وWindows Phone وWindows Vista وWindows Azure هي علامات تجارية مسجلة لمجموعة شركات Microsoft.

Mozilla وFirefox وThunderbird هي علامات تجارية مملوكة لمؤسسة Mozilla Foundation.

تُعد Novell علامة تجارية مسجلة لشركة Novell Enterprises Inc. في الولايات المتحدة الأمريكية وبلدان أخرى.

إن Oracle وJava وJavaScript وTouchDown علامات تجارية مسجلة لشركة Oracle و/أو شركاتها التابعة.

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 Chef علامة تجارية أو علامة تجارية مسجلة لشركة Progress Software Corporation و/أو إحدى الشركات التابعة لها أو الشركات التابعة لها في الولايات المتحدة و/أو البلدان الأخرى.

تُعد Puppet علامة تجارية أو علامة تجارية مسجلة لشركة Puppet, Inc.

تُعد Python علامة تجارية أو ماركة مسجلة لشركة Python Software Foundation.

إنRed Hat وAnsible وCentOS وFedora وLinux Red Hat Enterprise علامات تجارية أو علامات تجارية مسجلة لشركة Red Hat، Inc. أو الشركات التابعة لها في الولايات المتحدة وبلدان أخرى.

إن BlackBerry مملوكة لشركة Research In Motion Limited ومسجلة في الولايات المتحدة ويمكن أن تكون معلقة أو مسجلة في بلدان أخرى.

Debian هي علامة تجارية مسجلة لشركة Software in the Public Interest, Inc.

SPL وSplunk هي علامات تجارية مسجلة لشركة Splunk, Inc. في الولايات المتحدة الأمريكية وبلدان أخرى.

SUSE هي علامة تجارية مسجلة لشركة SUSE LLC في الولايات المتحدة الأمريكية وبلدان أخرى.

Symbian هي علامة تجارية مملوكة لشركة Symbian Foundation Ltd.

إن OpenAPI علامة تجارية لمؤسسة Linux Foundation.

إن VMware وVMware vSphere وVMware Workstation علامات تجارية مسجلة أو علامات تجارية لشركة VMware, Inc. في الولايات المتحدة و/أو نطاقات قضائية أخرى.

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.