kaspersky

Kaspersky Security Center 14

Contenido

Cliente del Servidor de administración (dispositivo cliente)
Complemento de administración
Configuración de programa
Configuración de tarea
Consola de administración
Consola de administración de AWS
Copia de seguridad de datos del Servidor de administración
Derechos de administrador
Directiva
Dispositivo con protección de UEFI
Dispositivo EAS
Dispositivo KES
Dispositivo MDM con iOS
Dispositivos administrados
Dominio de difusión
Entorno de nube
Estación de trabajo del administrador
Estado de la protección
Estado de la protección de la red
Función de IAM
Gravedad del evento
Grupo de administración
Grupo de aplicaciones con licencia
Grupo de funciones
HTTPS
Imagen de máquina de Amazon (AMI)
Instalación forzada
Instalación local
Instalación manual
Instalación remota
Instancia de Amazon EC2
Interfaz de programación de aplicaciones de AWS (API de AWS)
JavaScript
Kaspersky Private Security Network (KSN privada)
Kaspersky Security Network (KSN)
Nivel de importancia del parche
Operador de Kaspersky Security Center
Paquete de instalación
Perfil
Perfil de aprovisionamiento
Perfil de configuración
Perfil de MDM para iOS
Periodo de vigencia de la licencia
Propietario del dispositivo
Protección antivirus de la red
Protección antivirus: proveedor de servicio
Puerta de enlace de conexión
Punto de distribución

Ayuda de Kaspersky Security Center 14

Novedades Descubra las novedades de esta versión del programa.	**Configuración de protección de la red** Administrar la seguridad de la organización.
Requisitos de hardware y software Compruebe qué sistemas operativos y versiones de aplicación se admiten.	**Aplicaciones de Kaspersky. Actualización de bases de datos y módulos de software** Mantener la fiabilidad del sistema de protección.
Despliegue y configuración inicial Planifique el uso de los recursos, instale el Servidor de administración, instale el Agente de red y las aplicaciones de seguridad en los dispositivos cliente y consolide los dispositivos en grupos de administración.	**Supervisión e informes** Vea su infraestructura, estados de protección y las estadísticas.
Detección de dispositivos en red Descubra los dispositivos existentes y nuevos en la red de su organización.	**Sustitución de aplicaciones de seguridad de terceros** Más información sobre métodos para no instalar aplicaciones incompatibles.
Aplicaciones de Kaspersky. Despliegue centralizado Desplegar aplicaciones de Kaspersky.	**Ajuste de puntos de distribución y puertas de enlace de conexión** Configurar puntos de distribución.
Actualización de Kaspersky Security Center desde una versión anterior Actualización de Kaspersky Security Center 14 desde una versión anterior.	**Prácticas recomendadas para proveedores de servicios (Ayuda en línea únicamente)** Más información sobre recomendaciones sobre cómo desplegar, configurar y usar la aplicación y, además, formas de resolver los problemas habituales en la operación de la aplicación.
Aplicaciones de Kaspersky. Licencia y activación Activar aplicaciones de Kaspersky en unos pasos.	**Guía de dimensionamiento (Ayuda en línea únicamente)** Para un rendimiento óptimo en diferentes condiciones, debe tener en cuenta la cantidad de dispositivos en red, la topología de red y el conjunto de funciones de Kaspersky Security Center que necesita.
Exportación de eventos a sistemas SIEM Configure la exportación de eventos a los sistemas SIEM para su análisis.	**Administración de vulnerabilidades y parches** Búsqueda y reparación de vulnerabilidades en software de terceros
Trabajo en un entorno de nube Despliegue Kaspersky Security Center en entornos de nube: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.	

Novedades

Kaspersky Security Center 14

Kaspersky Security Center 14 tiene varias mejoras y funciones nuevas:

- Puede instalar actualizaciones y corregir vulnerabilidades de software de terceros (excepto el software de Microsoft) en una red aislada. Dichas redes incluyen Servidores de administración y dispositivos administrados que no tienen acceso a Internet. Para solucionar las vulnerabilidades en este tipo de red, debe descargar las actualizaciones necesarias mediante un Servidor de administración que tenga acceso a Internet y luego transmitir los parches a los Servidores de administración aislados.

- Se han agregado perfiles de conexión para usuarios fuera de la oficina para dispositivos macOS. Mediante el uso de perfiles de conexión, puede configurar reglas para que los Agentes de red en dispositivos macOS se conecten al mismo Servidor de administración o a diferentes, según la ubicación del dispositivo.

- El Agente de red ahora se puede instalar en dispositivos que ejecutan Microsoft Windows 10 IoT Enterprise.

- En **Informe de amenazas**, ahora puede filtrar la lista de amenazas para ver solo las que fueron detectadas por Cloud Sandbox.

Kaspersky Security Center 14 Web Console tiene varias mejoras y funciones nuevas:

- Puede configurar el modo Solo panel para los empleados que no administran la red pero que desean ver las estadísticas de protección de la red en Kaspersky Security Center (por ejemplo, un alto directivo). Cuando un usuario tiene este modo activado, solo se le muestra un panel con un conjunto predefinido de widgets. Así, puede monitorear las estadísticas especificadas en los widgets, por ejemplo, el estado de protección de todos los dispositivos administrados, la cantidad de amenazas recién detectadas o la lista de las amenazas más frecuentes en la red.

- Kaspersky Security Center 14 Web Console ahora acepta Kaspersky Security for iOS como aplicación de seguridad.

- En las propiedades de la tarea, puede especificar si desea o no aplicar la tarea a subgrupos y Servidores de administración secundarios (incluidos los virtuales).

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 tiene varias mejoras y funciones nuevas:

- Ahora puede instalar el Servidor de administración, la Consola de administración, Kaspersky Security Center 13.2 Web Console y el Agente de red en los siguientes sistemas operativos nuevos (vea los requisitos de software para obtener más información):

  - Microsoft Windows 11.

  - Microsoft Windows 10 21H2 (actualización de octubre de 2021).

  - Windows Server 2022.

- Puede usar MySQL 8.0 como la base de datos.

- Puede desplegar Kaspersky Security Center en un clúster de conmutación por error de Kaspersky para proporcionar alta disponibilidad de Kaspersky Security Center.

- Kaspersky Security Center ahora funciona con las direcciones IPv6 y las direcciones IPv4. El Servidor de administración puede sondear las redes que tienen dispositivos con direcciones IPv6.

Kaspersky Security Center 13.2 Web Console tiene varias mejoras y funciones nuevas:

- Ahora puede administrar dispositivos móviles con Android a través de Kaspersky Security Center 13.2 Web Console.
- Kaspersky Marketplace está disponible como una nueva sección de menú: puede buscar la aplicación de Kaspersky a través de Kaspersky Security Center 13.2 Web Console.
- Kaspersky Security Center ahora admite las siguientes aplicaciones de Kaspersky:
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 tiene varias mejoras y funciones nuevas:

- Se ha mejorado la integración con los sistemas SIEM. Ahora puede exportar eventos a los sistemas SIEM mediante el canal cifrado (TLS). La función está disponible para Kaspersky Security Center 14 Web Console y Consola de administración basada en MMC.
- Ahora puede recibir parches del Servidor de administración como un paquete de distribución, el cual puede usar para futuras actualizaciones de versiones posteriores.
- Se ha añadido una nueva sección, **Alertas**, para Kaspersky Endpoint Detection and Response Optimum a Kaspersky Security Center 13.1 Web Console. También se han añadido nuevos widgets para trabajar con las amenazas que detecte Kaspersky Endpoint Detection and Response Optimum.
- En Kaspersky Security Center 13.1 Web Console, ahora puede recibir notificaciones sobre licencias que caduquen de las aplicaciones de Kaspersky.
- El tiempo de respuesta de Kaspersky Security Center 13.1 Web Console ha disminuido.

Kaspersky Security Center 13

Se han realizado las siguientes mejoras en Kaspersky Security Center 13 Web Console:

- Se ha implementado la verificación en dos pasos. Puede activar la verificación en dos pasos para reducir el riesgo de acceso no autorizado a Kaspersky Security Center 13 Web Console.
- Implementación de la autenticación de dominio mediante los protocolos NTLM y Kerberos (single sign-on). La función de inicio de sesión único permite a un usuario de Windows activar la autenticación segura en Kaspersky Security Center 13 Web Console sin tener que volver a introducir la contraseña en la red corporativa.
- Ahora puede configurar un complemento para que funcione con Kaspersky Managed Detection and Response. Puede utilizar esta integración para ver incidentes y administrar estaciones de trabajo.

- Ahora puede especificar la configuración de Kaspersky Security Center 13 Web Console en el asistente de instalación del Servidor de administración.

- Se muestran notificaciones sobre nuevas versiones de actualizaciones y parches. Puede instalar una actualización inmediatamente o más tarde en cualquier momento. Ahora puede instalar parches para el Servidor de administración a través de Kaspersky Security Center 13 Web Console.

- Al trabajar con tablas, ahora puede especificar el orden y el ancho de las columnas, ordenar los datos y especificar el tamaño de la página.

- Ahora puede abrir cualquier informe haciendo clic en su nombre.

- Kaspersky Security Center 13 Web Console ahora está disponible en coreano.

- Una nueva sección, Anuncios de Kaspersky, está disponible en el menú **SUPERVISIÓN E INFORMES**. Esta sección le mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas que están instaladas en los dispositivos administrados. Kaspersky Security Center actualiza periódicamente la información de esta sección, eliminando anuncios desactualizados y añadiendo nueva información. Sin embargo, si lo desea, puede desactivar los anuncios de Kaspersky.

- Se implementó la autenticación adicional después de cambiar la configuración de una cuenta de usuario. Puede habilitar la protección de una cuenta de usuario contra modificaciones no autorizadas. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario requiere la autorización de un usuario con derechos de modificación.

Se han añadido las siguientes funciones a Kaspersky Security Center 13:

- Se ha implementado la verificación en dos pasos. Puede activar la verificación en dos pasos para reducir el riesgo de acceso no autorizado a la Consola de administración. Si esta opción está activada, la modificación de la configuración de la cuenta de usuario requiere la autorización del usuario con derechos de modificación. Ahora puede habilitar o deshabilitar la verificación en dos pasos para dispositivos KES.

- Puede enviar mensajes al Servidor de administración a través del protocolo HTTP. Hay disponibles una guía de referencia y una biblioteca Python para trabajar con la OpenAPI del Servidor de administración.

- Puede emitir un certificado adicional para usar en los perfiles de configuración de MDM de iOS, para garantizar un cambio sin problemas de los dispositivos iOS administrados después de que expire el certificado del servidor de MDM para iOS.

- La carpeta de aplicaciones de tenencia múltiple ya no se muestra en la Consola de administración.

Kaspersky Security Center 14

Esta sección proporciona información sobre el uso de Kaspersky Security Center 14.

La información proporcionada en la Ayuda en línea puede diferir de la información proporcionada en los documentos enviados con la aplicación; en este caso, la Ayuda en línea se considera actualizada. Puede pasar a la Ayuda en línea haciendo clic en los enlaces que verá en la interfaz de la aplicación o haciendo clic en el enlace de la Ayuda en línea en los documentos. La Ayuda en línea se puede actualizar sin previo aviso. De ser necesario, puede cambiar entre la Ayuda en línea y la Ayuda sin conexión.

Acerca de Kaspersky Security Center

Esta sección incluye información acerca del objetivo de Kaspersky Security Center y de sus características y componentes principales.

La información proporcionada en la Ayuda en línea puede diferir de la información proporcionada en los documentos enviados con la aplicación; en este caso, la Ayuda en línea se considera actualizada. Puede pasar a la Ayuda en línea haciendo clic en los enlaces que verá en la interfaz de la aplicación o haciendo clic en el enlace de la Ayuda en línea en los documentos. La Ayuda en línea se puede actualizar sin previo aviso. De ser necesario, puede cambiar entre la Ayuda en línea y la Ayuda sin conexión.

Kaspersky Security Center está diseñado para la ejecución centralizada de las tareas básicas de administración y de mantenimiento en la red de una organización. La aplicación proporciona al administrador acceso a información detallada acerca del nivel de seguridad de la red de la organización; asimismo, permite configurar todos los componentes de protección que se crearon con las aplicaciones Kaspersky.

Kaspersky Security Center es una aplicación pensada para administradores de redes corporativas y empleados responsables de la protección de dispositivos para una amplia variedad de organizaciones.

Con Kaspersky Security Center puede realizar lo siguiente:

- Crear una jerarquía de Servidores de administración para gestionar la red de la organización, así como las redes de oficinas remotas u organizaciones cliente.

  La *organización cliente* es una organización que tiene asegurada la protección antivirus por un proveedor de servicio.

- Crear una jerarquía de grupos de administración para administrar una selección de dispositivos cliente como un todo.

- Administre un sistema de protección antivirus creado según las aplicaciones Kaspersky.

- Crear imágenes de sistemas operativos y desplegarlas en los dispositivos cliente en la red; además de realizar la instalación remota de aplicaciones Kaspersky y de otros proveedores de software.

- Administrar remotamente las aplicaciones de Kaspersky y de otros desarrolladores que estén instaladas en los dispositivos cliente. Instalar actualizaciones, buscar y solucionar vulnerabilidades.

- Lleve a cabo el despliegue centralizado de las claves de licencia de las aplicaciones Kaspersky en dispositivos cliente, supervise su utilización y renueve las licencias.

- Recibir estadísticas e informes sobre el funcionamiento de aplicaciones y de dispositivos.

- Recibir notificaciones sobre eventos críticos durante la operación de aplicaciones Kaspersky.
- Administrar dispositivos móviles.
- Administrar el cifrado de la información almacenada en las unidades de disco duro de dispositivos y unidades extraíbles, así como el acceso de los usuarios a los datos cifrados.
- Realizar el inventario del hardware conectado a la red de la organización.
- Administrar de forma centralizada los archivos que las aplicaciones de seguridad han trasladado a Cuarentena o Copia de seguridad, así como administrar archivos cuyo procesamiento por parte de las aplicaciones de seguridad se ha pospuesto.

Kit de distribución

Puede adquirir la aplicación en las tiendas online de Kaspersky (por ejemplo, https://www.kaspersky.es) o a empresas asociadas.

Si compra Kaspersky Security Center en una tienda en línea, copia la aplicación del sitio web de esta. La información necesaria para la activación de la aplicación se le envía por correo electrónico tras la realización del pago.

Requisitos de hardware y software

Servidor de administración

Requisitos mínimos de hardware:

- CPU con una frecuencia de funcionamiento de 1 GHz o superior. Para un sistema operativo de 64 bits, la frecuencia de CPU mínima es de 1.4 GHz.
- RAM: 4 GB.
- Espacio disponible en disco: 10 GB. Para usar Administración de vulnerabilidades y parches, debe haber disponible al menos 100 GB de espacio en disco.

Para la implementación en entornos de nube, los requisitos para el Servidor de administración y el servidor de base de datos son los mismos que los del Servidor de administración físico (según el número de dispositivos que desee administrar).

Requisitos de software:

- Microsoft® Data Access Components (MDAC) 2.8.
- Microsoft Windows® DAC 6.0.
- Microsoft Windows Installer 4.5.

Se admiten los siguientes sistemas operativos:

- Microsoft Windows 10 Enterprise 2015 LTSB de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 2016 LTSB de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 2019 LTSC de 32 bits / 64 bits.
- Microsoft Windows 10 Pro RS5 (Actualización de octubre de 2018, 1809) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro for Workstations RS5 (Actualización de octubre de 2018, 1809) de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise RS5 (Actualización de octubre de 2018, 1809) de 32 bits / 64 bits.
- Microsoft Windows 10 Education RS5 (Actualización de octubre de 2018, 1809) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Pro for Workstations 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Education 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Pro 19H2 de 32 bits / 64 bits.
- Microsoft Windows 10 Pro for Workstations 19H2 de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 19H2 de 32 bits / 64 bits.
- Microsoft Windows 10 Education 19H2 de 32 bits / 64 bits.
- Microsoft Windows 10 Home 20H1 (actualización de mayo de 2020) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro 20H1 (actualización de mayo de 2020) de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 20H1 (actualización de mayo de 2020) de 32 bits / 64 bits.
- Microsoft Windows 10 Education 20H1 (actualización de mayo de 2020) de 32 bits / 64 bits.
- Microsoft Windows 10 Home 20H2 (actualización de octubre de 2020) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 20H2 (actualización de octubre de 2020) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 20H2 (actualización de octubre de 2020) 32 bits / 64 bits.
- Microsoft Windows 10 Education 20H2 (actualización de octubre de 2020) 32 bits / 64 bits.
- Microsoft Windows 10 Home 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Education 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Home 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.

- Microsoft Windows 10 Pro 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Education 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 11 Home 64 bits.
- Microsoft Windows 11 Pro 64 bits.
- Microsoft Windows 11 Enterprise 64 bits.
- Microsoft Windows 11 Education 64 bits.
- Microsoft Windows 8.1 Pro de 32 bits / 64 bits.
- Microsoft Windows 8.1 Enterprise de 32 bits / 64 bits.
- Microsoft Windows 8 Pro de 32 bits / 64 bits.
- Microsoft Windows 8 Enterprise de 32 bits / 64 bits.
- Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores de 32 bits / 64 bits.
- Microsoft Windows 7 Enterprise/Ultimate con Service Pack 1 y versiones posteriores de 32 bits / 64 bits.
- Windows Server 2008 R2 Standard Service Pack 1 y versiones posteriores de 64 bits.
- Windows Server 2008 R2 Service Pack 1 (todas las ediciones) 64 bits.
- Windows Server 2012 Server Core 64 bits.
- Windows Server 2012 Datacenter 64 bits.
- Windows Server 2012 Essentials 64 bits.
- Windows Server 2012 Foundation 64 bits.
- Windows Server 2012 Standard 64 bits.
- Windows Server 2012 R2 Server Core 64 bits.
- Windows Server 2012 R2 Datacenter 64 bits.
- Windows Server 2012 R2 Essentials 64 bits.
- Windows Server 2012 R2 Foundation 64 bits.
- Windows Server 2012 R2 Standard 64 bits.
- Windows Server 2016 Datacenter (LTSB) 64 bits.
- Windows Server 2016 Standard (LTSB) 64 bits.
- Windows Server 2016 Server Core (Opción de instalación) (LTSB) 64 bits.

- Windows Server 2019 Standard 64 bits.
- Windows Server 2019 Datacenter 64 bits.
- Windows Server 2019 Core 64 bits.
- Windows Server 2022 Standard 64 bits.
- Windows Server 2022 Datacenter 64 bits.
- Windows Server 2022 Core 64 bits.
- Windows Storage Server 2012 64 bits.
- Windows Storage Server 2012 R2 64 bits.
- Windows Storage Server 2016 64 bits.
- Windows Storage Server 2019 64 bits.

Se admiten las plataformas de virtualización siguientes:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- VMware Workstation 16 Pro.
- Microsoft Hyper-V Server 2012 64 bits.
- Microsoft Hyper-V Server 2012 R2 64 bits.
- Microsoft Hyper-V Server 2016 64 bits.
- Microsoft Hyper-V Server 2019 64 bits.
- Microsoft Hyper-V Server 2022 64 bits.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Parallels Desktop 17.
- Oracle VM VirtualBox 6.x (solo con inicio de sesión como invitado en Windows)

Se admiten los siguientes servidores de bases de datos (se pueden instalar en un dispositivo diferente):

- Microsoft SQL Server 2012 Express 64 bits.
- Microsoft SQL Server 2014 Express 64 bits.
- Microsoft SQL Server 2016 Express 64 bits.
- Microsoft SQL Server 2017 Express 64 bits.

- Microsoft SQL Server 2019 Express 64 bits.
- Microsoft SQL Server 2014 (todas las ediciones) 64 bits.
- Microsoft SQL Server 2016 (todas las ediciones) 64 bits.
- Microsoft SQL Server 2017 (todas las ediciones) en Windows 64 bits.
- Microsoft SQL Server 2017 (todas las ediciones) en Linux 64 bits.
- Microsoft SQL Server 2019 (todas las ediciones) en Windows 64 bits (requiere acciones adicionales).
- Microsoft SQL Server 2019 (todas las ediciones) en Linux 64 bits (requiere acciones adicionales).
- Microsoft Azure SQL Database.
- Todas las ediciones de SQL Server compatibles en las plataformas de la nube de Amazon RDS y Microsoft Azure.
- MySQL 5.7 Community 32 bits/64 bits.
- MySQL Standard Edition 8.0 (versión 8.0.20 y superior) de 32 bits / 64 bits.
- MySQL Enterprise Edition 8.0 (versión 8.0.20 y superior) de 32 bits / 64 bits.
- MariaDB 10.5.x de 32 bits / 64 bits.
- MariaDB 10.4.x de 32 bits / 64 bits.
- MariaDB 10.3.22 y superior de 32 bits / 64 bits.
- El servidor MariaDB 10.3 de 32 bits o 64 bits con motor de almacenamiento InnoDB.
- MariaDB Galera Cluster 10.3 32 bits/64 bits con motor de almacenamiento InnoDB.
- MariaDB 10.1.30 y superior de 32 bits / 64 bits.

Se recomienda utilizar MariaDB 10.3.22; Si utiliza una versión anterior, la tarea Realizar actualización de Windows puede tardar más de un día en funcionar.

SIEM y otros sistemas de gestión de la información:

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

Kaspersky Security Center 14 Web Console

Servidor de Kaspersky Security Center 14 Web Console

Requisitos mínimos de hardware:

- CPU: 4 núcleos, frecuencia de operación de 2,5 GHz.
- Memoria RAM: 8 GB
- Espacio disponible en disco: 40 GB.

Se admiten los siguientes sistemas operativos:

- Sistema operativo (versiones de solo 64 bits):
  - Microsoft Windows 10 Enterprise 2015 LTSB.
  - Microsoft Windows 10 Enterprise 2016 LTSB.
  - Microsoft Windows 10 Enterprise 2019 LTSC.
  - Microsoft Windows 10 Pro RS5 (Actualización de octubre de 2018, 1809).
  - Microsoft Windows 10 Pro for Workstations RS5 (Actualización de octubre de 2018, 1809).
  - Microsoft Windows 10 Enterprise RS5 (Actualización de octubre de 2018, 1809).
  - Microsoft Windows 10 Education RS5 (Actualización de octubre de 2018, 1809).
  - Microsoft Windows 10 Pro 19H1.
  - Microsoft Windows 10 Pro for Workstations 19H1.
  - Microsoft Windows 10 Enterprise 19H1.
  - Microsoft Windows 10 Education 19H1.
  - Microsoft Windows 10 Pro 19H2.
  - Microsoft Windows 10 Pro for Workstations 19H2.
  - Microsoft Windows 10 Enterprise 19H2.
  - Microsoft Windows 10 Education 19H2.
  - Microsoft Windows 10 Home 20H1 (actualización de mayo de 2020).
  - Microsoft Windows 10 Pro 20H1 (actualización de mayo de 2020).
  - Microsoft Windows 10 Enterprise 20H1 (actualización de mayo de 2020).
  - Microsoft Windows 10 Education 20H1 (actualización de mayo de 2020).
  - Microsoft Windows 10 Home 20H2 (actualización de octubre de 2020).
  - Microsoft Windows 10 Pro 20H2 (actualización de octubre de 2020).
  - Microsoft Windows 10 Enterprise 20H2 (actualización de octubre de 2020).

- Microsoft Windows 10 Education 20H2 (actualización de octubre de 2020).
- Microsoft Windows 10 Home 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Education 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Home 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Education 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 11 Home.
- Microsoft Windows 11 Pro.
- Microsoft Windows 11 Enterprise.
- Microsoft Windows 11 Education.
- Windows Server 2012 Server Core.
- Windows Server 2012 Datacenter.
- Windows Server 2012 Essentials.
- Windows Server 2012 Foundation.
- Windows Server 2012 Standard.
- Windows Server 2012 R2 Server Core.
- Windows Server 2012 R2 Datacenter.
- Windows Server 2012 R2 Essentials.
- Windows Server 2012 R2 Foundation.
- Windows Server 2012 R2 Standard.
- Windows Server 2016 Datacenter (LTSB).
- Windows Server 2016 Standard (LTSB).
- Windows Server 2016 Server Core (Opción de instalación) (LTSB).
- Windows Server 2019 Standard 64 bits.
- Windows Server 2019 Datacenter 64 bits.

- Windows Server 2019 Core 64 bits.
- Windows Server 2022 Standard 64 bits.
- Windows Server 2022 Datacenter 64 bits.
- Windows Server 2022 Core 64 bits.
- Windows Storage Server 2012 64 bits.
- Windows Storage Server 2012 R2 64 bits.
- Windows Storage Server 2016 64 bits.
- Windows Storage Server 2019 64 bits.

- Linux (solo versiones de 64 bits):
  - 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 (todos los Service Packs).
  - SUSE Linux Enterprise Server 15 (todos los Service Packs).
  - SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM.
  - Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio).
  - Astra Linux Special Edition 1.6 (incluido el modo de entorno de software cerrado y el modo obligatorio).
  - Astra Linux Common Edition 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 Certified Edition.

Entre las plataformas de virtualización, la máquina virtual basada en kernel es compatible con los siguientes sistemas operativos:

- Alt 8 SP Server (LKNV.11100-01) 64 bits.
- Alt Server 10 64 bits.
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits.
- Debian GNU/Linux 11.x (Bullseye) 32-bit / 64-bit.
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits.
- RED OS 7.3 Server 64 bits.
- RED OS 7.3 Certified Edition 64 bits.

Kaspersky Security Center 14 Web Console Server no es compatible con los siguientes sistemas operativos:

- Microsoft Windows Essential Business Server 2008 Standard/Premium.
- Microsoft Windows Small Business Server 2003 Standard/Premium con SP1.
- Microsoft Windows Small Business Server 2003 R2 Standard/Premium.
- Microsoft Windows Small Business Server 2008 Standard/Premium.
- Microsoft Windows Small Business Server 2011 Essentials.
- Microsoft Windows Small Business Server 2011 Premium Add-on.
- Microsoft Windows Small Business Server 2011 Standard.
- Microsoft Windows Home Server 2011.
- Microsoft Windows MultiPoint Server 2010 Standard/Premium.
- Microsoft Windows MultiPoint Server 2011 Standard/Premium.
- Microsoft Windows MultiPoint Server 2012 Standard/Premium.
- Microsoft Windows Server 2000.
- Microsoft Windows Server 2003 Enterprise con SP2.
- Microsoft Windows Server 2003 Standard con SP2.
- Microsoft Windows Server 2003 R2 Enterprise con SP2.

- Microsoft Windows Server 2003 R2 Standard con SP2.

Dispositivos cliente

Para un dispositivo cliente, el uso de Kaspersky Security Center 14 Web Console solo requiere un navegador.

Los requisitos de hardware y software del dispositivo son idénticos a los del navegador utilizado para Kaspersky Security Center 14 Web Console.

Navegadores:

- Mozilla Firefox Extended Support Release 91.8.0 o superior (la versión 91.8.0 se lanzó el 5 de abril de 2022)
- Mozilla Firefox Release 99.0 o superior (la versión 99.0 se lanzó el 5 de abril de 2022)
- Google Chrome 100.0.4896.88 o superior (compilación oficial)
- Microsoft Edge 100 o superior
- Safari 15 en macOS.

Servidor de administración de dispositivos móviles con iOS (MDM de iOS)

Requisitos de hardware:

- CPU con una frecuencia de funcionamiento de 1 GHz o superior. Para un sistema operativo de 64 bits, la frecuencia de CPU mínima es de 1.4 GHz.
- RAM: 2 GB.
- Espacio disponible en disco: 2 GB.

Requisitos de software: Microsoft Windows (la versión del sistema operativo compatible depende de los requisitos del Servidor de administración).

Servidor de dispositivos móviles de Exchange

Todos los requisitos de software y hardware del Servidor de dispositivos móviles Exchange se incluyen en los requisitos del servidor Exchange de Microsoft.

Se admite la compatibilidad con el servidor Exchange de Microsoft 2007, el servidor Exchange de Microsoft 2010 y el servidor Exchange de Microsoft 2013.

Consola de administración

Requisitos de hardware:

- CPU con una frecuencia de funcionamiento de 1 GHz o superior. Para un sistema operativo de 64 bits, la frecuencia de CPU mínima es de 1.4 GHz.
- RAM: 512 MB.

- Espacio disponible en disco: 1 GB.

Requisitos de software:

- Sistema operativo de Microsoft Windows (la versión compatible del sistema operativo viene determinada por los requisitos del Servidor de administración), con excepción de los siguientes sistemas.
  - Windows Server 2012 Server Core 64 bits.
  - Windows Server 2012 R2 Server Core 64 bits.
  - Windows Server 2016 Server Core (Opción de instalación) (LTSB) 64 bits.
  - Windows Server 2019 Core 64 bits.
  - Windows Server 2022 Core 64 bits.
- Microsoft Management Console 2.0.
- Microsoft Windows Installer 4.5.
- Microsoft Internet Explorer 10.0 ejecutándose en:
  - Microsoft Windows Server 2008 R2 Service Pack 1.
  - Microsoft Windows Server 2012.
  - Microsoft Windows Server 2012 R2.
  - Microsoft Windows 7 Service Pack 1.
  - Microsoft Windows 8.
  - Microsoft Windows 8.1.
  - Microsoft Windows 10.
- Microsoft Internet Explorer 11.0 ejecutándose en:
  - Microsoft Windows Server 2012 R2.
  - Microsoft Windows Server 2012 R2 Service Pack 1.
  - Microsoft Windows Server 2016.
  - Microsoft Windows Server 2019.
  - Microsoft Windows 7 Service Pack 1.
  - Microsoft Windows 8.1.
  - Microsoft Windows 10.
- Microsoft Edge ejecutándose en Microsoft Windows 10.

Agente de red

Requisitos mínimos de hardware:

- CPU con una frecuencia de funcionamiento de 1 GHz o superior. Para un sistema operativo de 64 bits, la frecuencia de CPU mínima es de 1.4 GHz.
- RAM: 512 MB.
- Espacio disponible en disco: 1 GB.

Se admiten los siguientes sistemas operativos:

- Microsoft Windows Embedded POSReady 2009 con el Service Pack de 32 bits más reciente.
- Microsoft Windows Embedded POSReady 7 de 32 bits / 64 bits.
- Microsoft Windows Embedded Standard 7 con Service Pack 1 de 32 bits / 64 bits.
- Microsoft Windows Embedded 8 Standard de 32 bits / 64 bits.
- Microsoft Windows Embedded 8.1 Industry Pro de 32 bits / 64 bits.
- Microsoft Windows Embedded 8.1 Industry Enterprise de 32 bits / 64 bits.
- Microsoft Windows Embedded 8.1 Industry Update de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 2015 LTSB de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 2016 LTSB de 32 bits / 64 bits.
- Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 bits / ARM.
- Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 bits / ARM.
- Microsoft Windows 10 Enterprise 2019 LTSC de 32 bits / 64 bits.
- Microsoft Windows 10 IoT Enterprise version 1703 de 32 bits / 64 bits.
- Microsoft Windows 10 IoT Enterprise version 1709 de 32 bits / 64 bits.
- Microsoft Windows 10 IoT Enterprise version 1803 de 32 bits / 64 bits.
- Microsoft Windows 10 IoT Enterprise version 1809 de 32 bits / 64 bits.
- Microsoft Windows 10 20H2 IoT Enterprise de 32 bits / 64 bits.
- Microsoft Windows 10 21H2 IoT Enterprise de 32 bits / 64 bits.
- Microsoft Windows 10 IoT Enterprise de 32 bits / 64 bits.
- Microsoft Windows 10 IoT Enterprise version 1909 de 32 bits / 64 bits.
- Microsoft Windows 10 IoT Enterprise LTSC 2021 de 32 bits / 64 bits.

- Microsoft Windows 10 IoT Enterprise version 1607 de 32 bits / 64 bits.
- Microsoft Windows 10 Home RS3 (Actualización de Fall Creators, v1709) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro RS3 (Actualización de Fall Creators, v1709) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro para estaciones de trabajo RS3 (Actualización de Fall Creators, v1709) de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise RS3 (Actualización de Fall Creators, v1709) de 32 bits / 64 bits.
- Microsoft Windows 10 Education RS3 (Actualización de Fall Creators, v1709) de 32 bits / 64 bits.
- Microsoft Windows 10 Home RS4 (Actualización de abril de 2018, 17134) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro RS4 (Actualización de abril de 2018, 17134) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro para estaciones de trabajo RS4 (Actualización de abril de 2018, 17134) de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise RS4 (Actualización de abril de 2018, 17134) de 32 bits / 64 bits.
- Microsoft Windows 10 Education RS4 (Actualización de abril de 2018, 17134) de 32 bits / 64 bits.
- Microsoft Windows 10 Home RS5 (Octubre de 2018) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro RS5 (Octubre de 2018) de 32 bits / 64 bits.
- Microsoft Windows 10 Pro for Workstations RS5 (Octubre de 2018) de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise RS5 (Octubre de 2018) de 32 bits / 64 bits.
- Microsoft Windows 10 Education RS5 (Octubre de 2018) de 32 bits / 64 bits.
- Microsoft Windows 10 Home 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Pro 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Pro for Workstations 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Education 19H1 de 32 bits / 64 bits.
- Microsoft Windows 10 Home 19H2 32 bits / 64 bits.
- Microsoft Windows 10 Pro 19H2 de 32 bits / 64 bits.
- Microsoft Windows 10 Pro for Workstations 19H2 de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 19H2 de 32 bits / 64 bits.
- Microsoft Windows 10 Education 19H2 de 32 bits / 64 bits.
- Microsoft Windows 10 Home 20H1 (actualización de mayo de 2020) de 32 bits / 64 bits.

- Microsoft Windows 10 Pro 20H1 (actualización de mayo de 2020) de 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 20H1 (actualización de mayo de 2020) de 32 bits / 64 bits.
- Microsoft Windows 10 Education 20H1 (actualización de mayo de 2020) de 32 bits / 64 bits.
- Microsoft Windows 10 Home 20H2 (actualización de octubre de 2020) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 20H2 (actualización de octubre de 2020) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 20H2 (actualización de octubre de 2020) 32 bits / 64 bits.
- Microsoft Windows 10 Education 20H2 (actualización de octubre de 2020) 32 bits / 64 bits.
- Microsoft Windows 10 Home 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Education 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Home 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Education 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 11 Home 64 bits.
- Microsoft Windows 11 Pro 64 bits.
- Microsoft Windows 11 Enterprise 64 bits.
- Microsoft Windows 11 Education 64 bits.
- Microsoft Windows 8.1 Pro de 32 bits / 64 bits.
- Microsoft Windows 8.1 Enterprise de 32 bits / 64 bits.
- Microsoft Windows 8 Pro de 32 bits / 64 bits.
- Microsoft Windows 8 Enterprise de 32 bits / 64 bits.
- Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores de 32 bits / 64 bits.
- Microsoft Windows 7 Enterprise/Ultimate con Service Pack 1 y versiones posteriores de 32 bits / 64 bits.
- Microsoft Windows 7 Home Basic/Premium con Service Pack 1 y versiones posteriores de 32 bits / 64 bits.
- Microsoft Windows XP Professional con Service Pack 3 y versiones posteriores de 32 bits.
- Microsoft Windows XP Professional for Embedded Systems Service Pack de 32 bits.

- Windows Small Business Server 2011 Essentials 64 bits.
- Windows Small Business Server 2011 Premium Add-on 64 bits.
- Windows Small Business Server 2011 Standard 64 bits.
- Windows MultiPoint Server 2011 Standard/Premium 64 bits.
- Windows MultiPoint Server 2012 Standard/Premium 64 bits.
- Windows Server 2008 Foundation con Service Pack 2 de 32 bits / 64 bits.
- Windows Server 2008 Service Pack 2 (todas las ediciones) de 32 bits / 64 bits.
- Windows Server 2008 R2 Datacenter Service Pack 1 y versiones posteriores de 64 bits.
- Windows Server 2008 R2 Enterprise Service Pack 1 y versiones posteriores de 64 bits.
- Windows Server 2008 R2 Foundation Service Pack 1 y versiones posteriores de 64 bits.
- Windows Server 2008 R2 Core Mode Service Pack 1 y versiones posteriores de 64 bits.
- Windows Server 2008 R2 Standard Service Pack 1 y versiones posteriores de 64 bits.
- Windows Server 2008 R2 Service Pack 1 (todas las ediciones) 64 bits.
- Windows Server 2012 Server Core 64 bits.
- Windows Server 2012 Datacenter 64 bits.
- Windows Server 2012 Essentials 64 bits.
- Windows Server 2012 Foundation 64 bits.
- Windows Server 2012 Standard 64 bits.
- Windows Server 2012 R2 Server Core 64 bits.
- Windows Server 2012 R2 Datacenter 64 bits.
- Windows Server 2012 R2 Essentials 64 bits.
- Windows Server 2012 R2 Foundation 64 bits.
- Windows Server 2012 R2 Standard 64 bits.
- Windows Server 2016 Datacenter (LTSB) 64 bits.
- Windows Server 2016 Standard (LTSB) 64 bits.
- Windows Server 2016 Server Core (Opción de instalación) (LTSB) 64 bits.
- Windows Server 2019 Standard 64 bits.
- Windows Server 2019 Datacenter 64 bits.

- Windows Server 2019 Core 64 bits.
- Windows Server 2022 Standard 64 bits.
- Windows Server 2022 Datacenter 64 bits.
- Windows Server 2022 Core 64 bits.
- Windows Storage Server 2012 64 bits.
- Windows Storage Server 2012 R2 64 bits.
- Windows Storage Server 2016 64 bits.
- Windows Storage Server 2019 64 bits.
- Debian GNU/Linux 11.x (Bullseye) 32 bits / 64 bits.
- Debian GNU/Linux 10.x (Buster) de 32 bits / 64 bits.
- Debian GNU/Linux 9.x (Stretch) de 32 bits / 64 bits.
- Ubuntu Server 20.04 LTS (Focal Fossa) de 32 bits / 64 bits.
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 bits.
- Ubuntu Server 18.04 LTS (Bionic Beaver) de 32 bits / 64 bits.
- Ubuntu Desktop 20.04 LTS (Focal Fossa) de 32 bits / 64 bits.
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) de 32 bits / 64 bits.
- CentOS 8.x 64 bits.
- CentOS 7.x 64 bits.
- CentOS 7.x ARM 64 bits.
- Red Hat Enterprise Linux Server 8.x 64 bits.
- Red Hat Enterprise Linux Server 7.x 64 bits.
- Red Hat Enterprise Linux Server 6.x de 32 bits / 64 bits.
- SUSE Linux Enterprise Server 12 (todos los Service Packs) 64 bits.
- SUSE Linux Enterprise Server 15 (todos los Service Packs) 64 bits.
- SUSE Linux Enterprise Desktop 15 (todos los Service Packs) 64 bits.
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 bits.
- openSUSE 15 64 bits.
- EulerOS 2.0 SP8 ARM.

- Pardus OS 19.1 64 bits.
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits.
- Astra Linux Special Edition 1.6 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits.
- Astra Linux Common Edition 2.12 64 bits.
- Astra Linux Special Edition 4.7 ARM.
- Alt Server 10 64 bits.
- Alt Server 9.2 64 bits.
- Alt Workstation 10 de 32 bits / 64 bits.
- Alt Workstation 9.2 de 32 bits / 64 bits.
- Alt 8 SP Server (LKNV.11100-01) 64 bits.
- Alt 8 SP Server (LKNV.11100-02) 64 bits.
- Alt 8 SP Server (LKNV.11100-03) 64 bits.
- Alt 8 SP Workstation (LKNV.11100-01) de 32 bits / 64 bits.
- Alt 8 SP Workstation (LKNV.11100-02) de 32 bits / 64 bits
- Alt 8 SP Workstation (LKNV.11100-03) de 32 bits / 64 bits.
- Mageia 4 32 bits.
- Oracle Linux 7 64 bits.
- Oracle Linux 8 64 bits.
- Linux Mint 19.x 32 bits
- Linux Mint 20.x 64 bits
- AlterOS 7.5 y superior 64 bits
- GosLinux IC6 64 bits
- RED OS 7.3 64 bits
- RED OS 7.3 Server 64 bits
- RED OS 7.3 Certified Edition 64 bits
- ROSA Enterprise Linux Server de 64 bits
- ROSA Enterprise Linux Desktop 7.3 de 64 bits
- ROSA COBALT Workstation 7.3 de 64 bits

- ROSA COBALT Server 7.3 de 64 bits.
- Lotos (Linux core versión 4.19.50, DE: MATE) de 64 bits.
- macOS Sierra (10.12).
- macOS High Sierra (10.13).
- macOS Mojave (10.14).
- macOS Catalina (10.15).
- macOS Big Sur (11.x).
- macOS Monterey (12.x).

Para el Agente de red, la arquitectura de Apple Silicon (M1), así como la de Intel, son compatibles.

Se admiten las plataformas de virtualización siguientes:

- VMware vSphere 6.7.
- VMware vSphere 7.0.
- VMware Workstation 16 Pro.
- Microsoft Hyper-V Server 2012 64 bits.
- Microsoft Hyper-V Server 2012 R2 64 bits.
- Microsoft Hyper-V Server 2016 64 bits.
- Microsoft Hyper-V Server 2019 64 bits.
- Microsoft Hyper-V Server 2022 64 bits.
- Citrix XenServer 7.1 LTSR.
- Citrix XenServer 8.x.
- Máquina virtual basada en kernel. Compatible con los siguientes sistemas operativos:
  - Alt 8 SP Server (LKNV.11100-01) 64 bits.
  - Alt Server 10 64 bits.
  - Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits.
  - Debian GNU/Linux 11.x (Bullseye) 32 bits / 64 bits.
  - Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits.
  - RED OS 7.3 64 bits.

- RED OS 7.3 Server 64 bits.
- RED OS 7.3 Certified Edition 64 bits.

En los dispositivos que ejecutan Windows 10 versión RS4 o RS5, puede que Kaspersky Security Center no detecte algunas vulnerabilidades en las carpetas en que esté activada la distinción entre mayúsculas y minúsculas.

En Microsoft Windows XP, el Agente de red podría no realizar algunas operaciones correctamente.

El Agente de red para Linux y el Agente de red para macOS se proporcionan juntos con aplicaciones de seguridad de Kaspersky para estos sistemas operativos.

Lista de aplicaciones y soluciones compatibles con Kaspersky

Kaspersky Security Center admite la implementación y administración centralizadas de todas las aplicaciones y soluciones de Kaspersky que actualmente son compatibles. La siguiente tabla muestra qué aplicaciones y soluciones de Kaspersky son compatibles con la Consola de administración basada en MMC y Kaspersky Security Center 14 Web Console. Para conocer las versiones de las aplicaciones y soluciones, consulte la página web del ciclo de vida del soporte del producto.

Lista de aplicaciones y soluciones de Kaspersky compatibles con Kaspersky Security Center

Nombre de la aplicación o solución de Kaspersky	Compatible con la consola de administración basada en MMC	Compatible con Kaspersky Security Center 14 Web Console
Para estaciones de trabajo		
Kaspersky Endpoint Security para Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security para Linux ARM Edition	✓	✓
Kaspersky Endpoint Security para Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security para Windows	✓	✓
Kaspersky Industrial CyberSecurity		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity para Linux Nodes	✓	—
Kaspersky Industrial CyberSecurity for Networks (no admite despliegue centralizado)	✓	✓
Para dispositivos móviles		
Kaspersky Endpoint Security for Android	✓	✓

Kaspersky Security for iOS	–	✓
Para servidores de archivos		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security para Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Para máquinas virtuales		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	–
Para sistemas de correo y servidores de SharePoint/colaboración (no se admite el despliegue centralizado)		
Kaspersky Security para servidor de correo Linux	✓	–
Kaspersky Secure Mail Gateway	✓	–
Kaspersky Security para servidores Microsoft Exchange	✓	–
Para la detección de ataques dirigidos		
Kaspersky Sandbox	✓	✓
Kaspersky Endpoint Detection and Response Optimum	–	✓
Kaspersky Managed Detection and Response	–	✓
Para dispositivos KasperskyOS		
Kaspersky IoT Secure Gateway	–	✓
Kaspersky Security Management Suite (complemento para Kaspersky Thin Client)	–	✓

Licencias y funciones de Kaspersky Security Center 14

Kaspersky Security Center requiere una licencia para algunas de sus funciones:

La siguiente tabla muestra qué licencia cubre qué funciones de Kaspersky Security Center.

Licencias y funciones de Kaspersky Security Center

Funciones de Kaspersky Security Center	Administración de vulnerabilidades y parches de Kaspersky	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kas E Opt

Evaluación vulnerabilidades	✓	✓	✓	✓	✓	✓	
Administración de parches	✓	–	✓	✓	–	✓	
Control de acceso basado en funciones	✓	✓	✓	✓	✓	✓	
Instalación de sistemas operativos y aplicaciones	✓	–	✓	✓	–	✓	
Administración de dispositivos móviles (es decir, gestión de los dispositivos iOS y Android de los usuarios)	✓	✓	✓	✓	–	–	
Asistente de configuración del entorno de nube para trabajar en entornos de nube como AWS, Microsoft Azure o Google Cloud	–	–	–	–	✓	✓	
Exportación de eventos a sistemas SIEM: Syslog	✓	✓	✓	✓	✓	✓	
Exportación de eventos a sistemas SIEM: QRadar de IBM y ArcSight de Micro Focus	✓	–	✓	✓	–	✓	

Sobre la compatibilidad del Servidor de administración y Kaspersky Security Center 14 Web Console

Le recomendamos que utilice la última versión del Servidor de Administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console. De lo contrario, la funcionalidad de Kaspersky Security Center puede ser limitada.

Puede instalar y actualizar el Servidor de administración de Kaspersky Security Center Administration Server y Kaspersky Security Center 14 Web Console de forma independiente. En este caso, debe asegurarse de que la versión instalada de Kaspersky Security Center 14 Web Console sea compatible con la versión del Servidor de administración al que se conecta:

- Kaspersky Security Center 14 Web Console es compatible con las siguientes versiones de Kaspersky Security Center Administration Server: 14, 13.2 y 13.1.
- Servidor de administración de Kaspersky Security Center 14 es compatible con las siguientes versiones de Kaspersky Security Center Web Console: 14, 13.2 y 13.1.

Acerca de Kaspersky Security Center Cloud Console

El uso de Kaspersky Security Center como una aplicación local significa que instala Kaspersky Security Center, con el Servidor de administración incluido, en un dispositivo local y administra el sistema de seguridad de la red a través de la Consola de administración basada en Microsoft Management Console o de la Web Console de Kaspersky Security Center.

Sin embargo, puede usar Kaspersky Security Center como un servicio en la nube. En este caso, los expertos de Kaspersky instalarán y mantendrán Kaspersky Security Center en el entorno de nube y Kaspersky le dará acceso al Servidor de administración como un servicio. Administrará el sistema de seguridad de la red a través de la Consola de administración basada en la nube llamada Kaspersky Security Center Cloud Console. Esta consola tiene una interfaz similar a la interfaz de la Web Console de Kaspersky Security Center.

La interfaz y la documentación de Kaspersky Security Center Cloud Console están disponibles en los siguientes idiomas:

- Inglés
- Francés
- Alemán
- Italiano
- Portugués (Brasil)
- Ruso
- Español
- Español (Latinoamérica)

Hay más información acerca de Kaspersky Security Center Cloud Console y sus funciones en la documentación de Kaspersky Security Center Cloud Console y en la documentación de Kaspersky Endpoint Security for Business.

Conceptos básicos

Esta sección explica los conceptos básicos relacionados con Kaspersky Security Center.

Servidor de administración

Los componentes de Kaspersky Security Center hacen posible administrar en remoto las aplicaciones Kaspersky instaladas en los dispositivos cliente.

Los dispositivos que tengan instalado el componente Servidor de administración se denominarán *Servidores de administración* (también *Servidores*). Los Servidores de administración se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

El Servidor de administración se instala en un dispositivo como un servicio con el siguiente conjunto de parámetros:

- Con el nombre "Servidor de administración de Kaspersky Security Center".
- Configurar para que se inicie automáticamente cuando se inicie el sistema operativo.
- Con la cuenta **LocalSystem** o la cuenta de usuario seleccionada durante la instalación del Servidor de administración.

El Servidor de administración realiza las siguientes funciones:

- Almacena la estructura de los grupos de administración.
- Almacenamiento de la información acerca de la configuración de los dispositivos cliente.
- Organización de repositorios para los paquetes de distribución de aplicaciones.
- Instalación remota de aplicaciones en dispositivos del cliente y eliminación de aplicaciones.
- Actualiza las bases de datos de la aplicación y los módulos de software de las aplicaciones de Kaspersky.
- Administración de directivas y tareas en los dispositivos cliente.
- Almacenamiento de la información acerca de los eventos que se han producido en los dispositivos cliente.
- Generación de informes sobre el funcionamiento de las aplicaciones Kaspersky.
- Despliega las claves de licencia en dispositivos cliente y almacena la información sobre claves de licencia.
- Reenvía notificaciones sobre el progreso de tareas (por ejemplo, la detección de virus en un dispositivo cliente).

Nombres de administración los Servidores de administración en la interfaz de la aplicación

En la interfaz de la Consola de administración basada en MMC y Kaspersky Security Center 14 Web Console, los Servidores de administración pueden tener los siguientes nombres:

- Nombre del dispositivo del Servidor de administración, por ejemplo: "*nombre_del_dispositivo*" o "Servidor de administración: *nombre_del_dispositivo*".
- Dirección IP del dispositivo del Servidor de administración, por ejemplo: "*Dirección IP*" o "Servidor de administración: *dirección IP*".
- Los Servidores de administración secundarios y los Servidores de administración virtuales tienen nombres personalizados, que usted especifica cuando conecta un Servidor de administración virtual o secundario al Servidor de administración principal.
- Si usa Kaspersky Security Center 14 Web Console instalado en un dispositivo Linux, la aplicación muestra los nombres de los Servidores de administración que especificó como fiables en el archivo de respuesta.

Puede conectarse al Servidor de administración a través de la Consola de administración o de Kaspersky Security Center 14 Web Console.

Jerarquía de Servidores de administración

Los Servidores de administración pueden organizarse en una jerarquía. Cada Servidor de administración puede tener varios Servidores de administración secundarios (conocidos como *Servidores secundarios*) en distintos niveles de anidamiento de la jerarquía. El nivel de anidamiento para los Servidores secundarios no está limitado. Los grupos de administración del Servidor de administración principal incluirán los dispositivos cliente de todos los Servidores de administración secundarios. De esta manera, secciones independientes y aisladas de redes pueden ser administradas por diferentes Servidores de administración que, a su vez, están administrados por el Servidor principal.

Los *Servidores de administración virtual* son un caso particular de Servidores de administración secundarios.

La jerarquía de los Servidores de administración se puede utilizar para hacer lo siguiente:

- Disminuir la carga en el Servidor de administración (comparado con un único Servidor de administración instalado en toda la red).
- Minimizar el tráfico de la Intranet y simplificar el trabajo con las oficinas remotas. No tiene que establecer conexiones entre el Servidor de administración principal y todos los dispositivos de la red, que pueden estar ubicados en diferentes regiones, por ejemplo. Es suficiente instalar un Servidor de administración secundario en cada segmento de red, distribuir los dispositivos entre los grupos de administración de Servidores secundarios y establecer las conexiones entre los Servidores secundarios y el Servidor principal a través de canales de comunicación rápidos.
- Distribuir las responsabilidades entre los administradores de la seguridad antivirus. Todas las posibilidades para la administración centralizada y el control del estado de la seguridad antivirus en las redes corporativas permanecen disponibles.
- Cómo de los proveedores de servicios utilizan Kaspersky Security Center. El proveedor de servicio solo necesita instalar Kaspersky Security Center y Kaspersky Security Center 14 Web Console. Para administrar un gran número de dispositivos cliente de varias organizaciones, un proveedor de servicio puede añadir Servidores de administración virtuales a la jerarquía de Servidores de administración.

Cada dispositivo incluido en la jerarquía de los grupos de administración se puede conectar a un solo Servidor de administración. Debe supervisar independientemente la conexión de dispositivos a los Servidores de administración. Para hacerlo, puede usar la función de búsqueda de dispositivos según atributos de red en los grupos de administración de diferentes servidores.

Servidor de administración virtual

El Servidor de administración virtual (también denominado *servidor virtual*) es un componente de Kaspersky Security Center pensado para administrar protección antivirus de la red de una organización cliente.

El Servidor de administración virtual es un tipo concreto de Servidor de administración secundario y, en comparación con un Servidor de administración físico, tiene las siguientes restricciones:

- El Servidor de administración virtual solo se puede crear en un Servidor de administración principal.

- Durante su funcionamiento, el Servidor de administración Virtual utiliza la base de datos del Servidor de administración principal. Las tareas de copia de seguridad y restauración de datos, así como las tareas de exploración y descarga de actualizaciones, no son compatibles con un Servidor de administración virtual.
- El Servidor virtual no permite la creación de Servidores de administración secundarios (incluidos los Servidores virtuales).

Además, el Servidor de administración virtual tiene las siguientes restricciones:

- En la ventana de propiedades del Servidor de administración virtual el número de secciones es limitado.
- Para llevar a cabo la instalación remota de las aplicaciones de Kaspersky en dispositivos cliente administrados por el Servidor de administración virtual, debe asegurarse que el Agente de red esté instalado en uno de los dispositivos cliente a fin de garantizar la comunicación con el Servidor de administración virtual. La primera vez que se conecta al Servidor de administración virtual, se designa al dispositivo como punto de distribución de manera automática, por lo que funciona como puerta de enlace para la conexión entre el Servidor de administración virtual y los dispositivos cliente.
- Un Servidor virtual solo puede sondear la red a través de puntos de distribución.
- Para reiniciar un Servidor virtual que no funciona correctamente, Kaspersky Security Center reinicia el Servidor de administración principal y todos los Servidores de administración virtuales.

El administrador de un Servidor de administración virtual dispone de todos los privilegios en ese Servidor virtual.

Servidor de dispositivos móviles

Servidor de dispositivos móviles es un componente de Kaspersky Security Center que proporciona acceso a dispositivos móviles y permite su administración a través de la Consola de administración. El Servidor de dispositivos móviles recopila información acerca de dispositivos móviles y almacena sus perfiles.

Existen dos tipos de servidores de dispositivos móviles:

- Servidor de dispositivos móviles de Exchange. Instalado en un dispositivo en el que se ha instalado un servidor Microsoft Exchange, lo que permite recuperar datos del servidor Microsoft Exchange y transmitir datos al Servidor de administración. Este Servidor de dispositivos móviles se utiliza para administrar dispositivos móviles que admiten el protocolo de Exchange ActiveSync.
- Servidor de MDM para iOS. Este servidor de dispositivos móviles se utiliza para administrar dispositivos móviles compatibles con el servicio de Apple Push Notification® (APNs).

Los servidores de dispositivos móviles de Kaspersky Security Center le permiten administrar los siguientes objetos:

- Un dispositivo móvil individual.
- Varios dispositivos móviles.
- Varios dispositivos móviles conectados a un clúster de servidores simultáneamente. Tras establecer la conexión con un clúster de servidores, el servidor de dispositivos móviles instalado en él aparece en la Consola de administración como un único servidor.

Servidor Web

El *Servidor Web* de Kaspersky Security Center (en adelante, *Servidor Web*) es un componente de Kaspersky Security Center que se instala junto con el Servidor de administración. El Servidor web está diseñado para publicar paquetes de instalación independientes, perfiles de MDM de iOS y archivos de una carpeta compartida a través de una red.

Al crear un paquete de instalación independiente, se publica automáticamente en el Servidor Web. El enlace para descargar el paquete independiente se muestra en la lista de paquetes de instalación independiente creados. Si fuera necesario, puede cancelar la publicación del paquete independiente o publicarlo de nuevo en el Servidor Web.

Al crear un perfil de MDM para iOS en el dispositivo móvil del usuario, también se publica automáticamente en el Servidor Web. El perfil publicado se elimina automáticamente del Servidor web tan pronto como se instala correctamente en el dispositivo móvil del usuario.

La carpeta compartida se usa para el almacenamiento de información disponible para todos los usuarios cuyos dispositivos se administran mediante el Servidor de administración. Si un usuario no tiene acceso directo a la carpeta compartida, se le puede proporcionar información de dicha carpeta mediante el Servidor Web.

Para proporcionar a los usuarios información de una carpeta compartida mediante el Servidor Web, el administrador debe crear una subcarpeta denominada "pública" en la carpeta compartida y pegar en ella la información pertinente.

La sintaxis del enlace de transferencia de información es la siguiente:

```
https://<nombre del Servidor Web>:<puerto HTTPS>/public/<objeto>
```

Donde:

- `<Nombre del Servidor Web>` es el nombre del Servidor Web de Kaspersky Security Center.
- `<Puerto HTTPS>` es un puerto HTTPS del Servidor Web definido por el Administrador. Un puerto HTTPS se puede configurar en la sección **Servidor web** de la ventana de propiedades del Servidor de administración. El número de puerto predeterminado es el 8061.
- `<Objeto>` es la subcarpeta o el archivo al que puede acceder el usuario.

El administrador puede enviar el nuevo enlace al usuario de cualquier forma que convenga; por ejemplo, por correo electrónico.

Al hacer clic en el enlace, el usuario puede descargar la información necesaria en un dispositivo local.

Agente de red

La interacción entre el Servidor de administración y los dispositivos se realiza mediante el componente *Agente de red* de Kaspersky Security Center. El Agente de red se debe instalar en todos los dispositivos en los que Kaspersky Security Center se utilice para administrar las aplicaciones de Kaspersky.

El Agente de red se instala en un dispositivo como un servicio con el siguiente conjunto de parámetros:

- Con el nombre "Agente de red de Kaspersky Security Center 14".

- Configurar para que se inicie automáticamente cuando se inicie el sistema operativo.
- Usando la cuenta LocalSystem.

Un dispositivo que tiene instalado el Agente de red se llama *dispositivo administrado* o *dispositivo*.

Puede instalar el Agente de red en Windows, Linux o un dispositivo Mac. Puede obtener el componente de una de las siguientes fuentes:

- Paquete de instalación en el almacenamiento del Servidor de administración (debe tener el Servidor de administración instalado).
- Paquete de instalación ubicado en los servidores web de Kaspersky.

No tiene que instalar el Agente de red en el dispositivo donde instale el Servidor de administración, ya que la versión del servidor del Agente de red se instala automáticamente junto con el Servidor de administración.

El nombre del proceso que inicia el Agente de red es *klnagent.exe*.

El Agente de red sincroniza el dispositivo administrado con el Servidor de administración. Recomendamos que establezca el intervalo de sincronización (también conocido como *heartbeat*) en 15 minutos por cada 10 000 dispositivos administrados.

Grupos de administración

Un *grupo de administración* (de ahora en adelante *grupo*) es un conjunto lógico de dispositivos administrados combinados en función de un rasgo específico para la administración de dispositivos agrupados en una única unidad dentro de Kaspersky Security Center.

Todos los dispositivos administrados dentro de un grupo de administración están configurados para hacer lo siguiente:

- Use la misma configuración de la aplicación (que puede especificar en las directivas de grupo).
- Utilice un modo común de funcionamiento de las aplicaciones, mediante la creación de tareas de grupo con parámetros específicos. Por ejemplo, crear e instalar un paquete de instalación común para actualizar las bases de datos y los módulos de la aplicación, analizar el dispositivo bajo petición y activar la protección en tiempo real.

Un dispositivo administrado puede pertenecer a un solo grupo de administración.

Puede crear jerarquías que tengan cualquier grado de anidamiento para los Servidores de administración los grupos. Un solo nivel de jerarquía puede incluir Servidores de administración secundarios y virtuales, grupos y dispositivos administrados. Puede mover dispositivos de un grupo a otro sin moverlos físicamente. Por ejemplo, si la posición de un trabajador en la empresa cambia de la de contador a desarrollador, puede mover el equipo de este trabajador del grupo de administración de Contadores al grupo de administración de Desarrolladores. A partir de entonces, el equipo recibirá automáticamente la configuración de la aplicación requerida para los desarrolladores.

Dispositivo administrado

Un *dispositivo administrado* es un equipo con Windows, Linux o macOS donde se ha instalado el Agente de red, o un dispositivo móvil con una aplicación de seguridad de Kaspersky instalada. Puede administrar dichos dispositivos creando tareas y directivos para las aplicaciones instaladas en estos dispositivos. También puede recibir informes de dispositivos administrados.

Puede hacer que un dispositivo administrado que no sea móvil funcione como un punto de distribución y como una puerta de enlace de conexión.

Un dispositivo puede estar administrado por un solo Servidor de administración. Un Servidor de administración puede administrar hasta 100 000 dispositivos, incluidos dispositivos móviles.

Dispositivo no asignados

Un *dispositivo no asignado* es un dispositivo en la red que no se ha incluido en ningún grupo de administración. Puede efectuar determinadas acciones en dispositivos no asignados, por ejemplo moverlos a grupos de administración o instalar aplicaciones en ellos.

Cuando se detecta un nuevo dispositivo en su red, este dispositivo va al grupo de administración de dispositivos no asignados. Puede configurar reglas para que los dispositivos se muevan automáticamente a otros grupos de administración una vez que se detecten los dispositivos.

Estación de trabajo del administrador

La *Estación de trabajo del administrador* es un dispositivo en el que se instala la Consola de administración, o que usa para abrir Kaspersky Security Center 14 Web Console. Los administradores pueden utilizar esos dispositivos para una administración centralizada a distancia de las aplicaciones Kaspersky instaladas en los dispositivos cliente.

Después de haber instalado la Consola de administración en su dispositivo, aparecerá el icono que se usa para iniciar la Consola de administración. Búsquelo en **Iniciar** → **Programas** → menú **Kaspersky Security Center**.

No hay restricciones para el número de estaciones de trabajo del administrador. En la red se pueden administrar simultáneamente grupos de administración de varios Servidores de administración desde cualquier estación de trabajo del administrador. Se puede conectar una estación de trabajo del administrador a un Servidor de administración (ya sea físico o virtual) de cualquier nivel de la jerarquía.

Se puede incluir una estación de trabajo del administrador en un grupo de administración como dispositivo cliente.

Dentro de los grupos de administración de cualquier Servidor de administración, el mismo dispositivo puede funcionar como cliente del Servidor de administración, como Servidor de administración o como estación de trabajo del administrador.

Complemento de administración

Las aplicaciones de Kaspersky se administran a través de la Consola de administración utilizando un componente dedicado llamado *complemento de administración*. Cada aplicación de Kaspersky que se puede administrar a través de Kaspersky Security Center incluye un complemento de administración.

Con el complemento de administración de aplicaciones se pueden realizar las siguientes acciones en la Consola de administración:

- Crear y editar las directivas y los parámetros de las aplicaciones, así como los parámetros de las tareas de la aplicación.

- Obtener información acerca de las tareas de la aplicación, los eventos de aplicación, así como las estadísticas del funcionamiento de la aplicación recibidas desde los dispositivos cliente.

Puede descargar complementos de administración desde la Página web del Servicio de soporte técnico de Kaspersky.

Complementos web de administración

Un componente especial, el *complemento web de administración*, se utiliza para la administración remota del software Kaspersky a través de Kaspersky Security Center 14 Web Console. De aquí en adelante, un complemento web de administración se denomina también *complemento de administración*. Un complemento de administración es una interfaz entre Kaspersky Security Center 14 Web Console y una aplicación específica de Kaspersky. Con un complemento de administración, puede configurar tareas y directivas para la aplicación.

Puede descargar complementos web de administración desde la Página web de soporte técnico de Kaspersky.

El complemento de administración proporciona lo siguiente:

- Interfaz para crear y editar tareas y configuraciones de aplicaciones
- Interfaz para crear y editar directivas y perfiles de directivas para la configuración remota y centralizada de las aplicaciones y dispositivos de Kaspersky
- La transmisión de eventos generados por la aplicación
- Funciones de Kaspersky Security Center 14 Web Console para mostrar los datos de los sistemas y los eventos de la aplicación y las estadísticas transmitidas desde dispositivos cliente

Directivas

Una *directiva* es un conjunto de configuraciones de aplicaciones de Kaspersky que se aplican a un grupo de administración y sus subgrupos. Puede instalar varias aplicaciones de Kaspersky en los dispositivos de un grupo de administración. Kaspersky Security Center proporciona una directiva única para cada aplicación de Kaspersky en un grupo de administración. Una directiva tiene uno de los siguientes estados (consulte la tabla a continuación):

El estado de la directiva

Estado	Descripción
Activo	La directiva actual que se aplica al dispositivo. Solo una directiva puede estar activa para una aplicación de Kaspersky en cada grupo de administración. Los dispositivos aplican los valores de configuración de una directiva activa para una aplicación de Kaspersky.
Inactiva	Una directiva que no se aplica actualmente a un dispositivo.
Fuera de la oficina	Si se selecciona esta opción, la directiva se activa cuando un dispositivo sale de la red corporativa.

Las directivas funcionan según las siguientes reglas:

- Se pueden configurar varias directivas con diferentes valores para una única aplicación.
- Solo una directiva puede estar activa para la aplicación actual.

- Puede activar una directiva inactiva cuando ocurre un evento específico. Por ejemplo, puede aplicar una configuración de protección antivirus más estricta durante un brote de virus.

- Una directiva puede tener directivas secundarias.

Generalmente, puede utilizar las directivas como preparación para situaciones de emergencia, como el ataque de un virus. Por ejemplo, si se trata de un ataque a través de unidades flash, puede activar una directiva que bloquee el acceso a las unidades flash. En este caso, la directiva activa actual se vuelve inactiva automáticamente.

Para evitar el mantenimiento de varias directivas, por ejemplo, cuando en diferentes ocasiones se supone el cambio de varias configuraciones únicamente, puede utilizar perfiles de directivas.

Un *perfil de directiva* es un subconjunto con nombre de valores de configuración de directiva que reemplaza los valores de configuración de una directiva. Un perfil de directiva afecta la formación de configuraciones efectivas en un dispositivo administrado. Las *configuraciones efectivas* son un conjunto de configuraciones de directivas, configuraciones de perfiles de directivas y configuraciones de aplicaciones locales que están aplicadas en ese momento en el dispositivo.

Los perfiles de directivas funcionan según las siguientes reglas:

- Un perfil de directiva entra en vigor cuando se produce una condición de activación específica.

- Los perfiles de directivas contienen valores de configuración que difieren de la configuración de la directiva.

- La activación de un perfil de directiva cambia la configuración efectiva del dispositivo administrado.

- Una directiva puede incluir un máximo de 100 perfiles de directivas.

Perfiles de directiva

A veces, puede ser necesario crear varias instancias de una sola directiva para diferentes grupos de administración; también podría desear modificar la configuración de esas directivas centralmente. Estas instancias pueden diferir solo en una o dos configuraciones. Por ejemplo, todos los contadores en una empresa trabajan bajo la misma directiva, pero los contadores sénior tienen permiso para usar unidades flash, mientras que los contadores junior no. En este caso, la aplicación de directivas a los dispositivos solo a través de la jerarquía de grupos de administración puede ser inconveniente.

Para ayudarle a evitar la creación de varias instancias de una sola directiva, Kaspersky Security Center le permite crear *perfiles de directivas*. Los perfiles de directivas son necesarios si desea que los dispositivos dentro de un solo grupo de administración se ejecuten bajo diferentes configuraciones de directivas.

Un perfil de directiva es un subconjunto de parámetros de la directiva denominado. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa en una condición específica denominada la *Condición de activación de perfil.* Los perfiles solo contienen parámetros que se diferencian de la directiva "básica", que está activa en el dispositivo administrado. La activación de un perfil modifica la configuración de la directiva "básica" que inicialmente estaba activa en el dispositivo. La configuración toma los valores especificados en el perfil.

Tareas

Kaspersky Security Center administra las aplicaciones de seguridad de Kaspersky instaladas en dispositivos mediante la creación y ejecución de *tareas*. Las tareas son necesarias para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software, y realizar otras acciones en las aplicaciones.

Las tareas para una aplicación específica solo se pueden crear si el complemento de administración para esa aplicación está instalado.

Las tareas se pueden realizar en el Servidor de administración y en los dispositivos.

Las siguientes tareas se realizan en el Servidor de administración:

- Distribución automática de informes
- Descarga de actualizaciones al repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de bases de datos
- Sincronización de Windows Update
- Creación de un paquete de instalación basado en la imagen del SO de un dispositivo de referencia

Los siguientes tipos de tareas se realizan en dispositivos:

- *Tareas locales*: tareas que se realizan en un dispositivo específico

  Las tareas locales pueden ser modificadas por el administrador usando herramientas de la Consola de administración, o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de la aplicación de seguridad). Si una tarea local ha sido modificada simultáneamente por el administrador y el usuario de un dispositivo administrado, los cambios hechos por el administrador entrarán en vigor, ya que tienen una prioridad más alta.

- *Tareas de grupo*: tareas que se realizan en todos los dispositivos de un grupo específico

  A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Las tareas de grupo también afectan (opcionalmente) los dispositivos que se han conectado a Servidores de administración virtuales y secundarios desplegados en ese grupo o cualquiera de sus subgrupos.

- *Tareas globales*: tareas que se realizan en un conjunto de dispositivos, independientemente de si se incluyen en algún grupo

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede realizar cambios en la configuración de tareas, ver el progreso de las tareas y copiar, exportar, importar y eliminar tareas.

Una tarea se inicia en un dispositivo solo si la aplicación para la que se creó la tarea se está en ejecución.

Los resultados de las tareas se guardan en el registro de eventos de Microsoft Windows y en el registro de eventos de Kaspersky Security Center, tanto de manera central en el Servidor de administración como de manera local en cada dispositivo.

No incluya datos confidenciales en la configuración de la tarea. Por ejemplo, no especifique la contraseña del administrador de dominio.

Cobertura de la tarea

La *cobertura de una tarea* es el conjunto de dispositivos en los que se realiza la tarea. Los tipos de cobertura son los siguientes:

- Para una *tarea local*, la cobertura es el propio dispositivo.
- Para una *tarea del Servidor de administración*, la cobertura es el Servidor de administración.
- Para una *tarea de grupo*, la cobertura es la lista de dispositivos incluidos en el grupo.

Al crear una *tarea global*, puede usar los siguientes métodos para especificar su cobertura:

- Especificar determinados dispositivos manualmente.

  Puede utilizar una dirección IP (o un rango IP), un nombre NetBIOS o un nombre DNS como la dirección del dispositivo.

- Importación de una lista de dispositivos desde un archivo .TXT con las direcciones del dispositivo que se añadirán (cada dirección debe ubicarse en una línea individual).

  Si importa una lista de dispositivos desde un archivo o la crea manualmente, y si los dispositivos se identifican por sus nombres, la lista solo podrá contener dispositivos para los cuales ya se haya introducido información en la base de datos del Servidor de administración. Además, la información debe haberse introducido cuando se conectaron esos dispositivos o durante la detección de dispositivos.

- Especificar selección de dispositivos.

  Con el tiempo, la cobertura de la tarea cambia a medida que el conjunto de dispositivos incluidos en la selección cambia. Puede realizarse una selección de dispositivos sobre la base de atributos del dispositivo, incluido el software instalado en un dispositivo y sobre la base de etiquetas asignadas a dispositivos. La selección de dispositivos es la forma más flexible de especificar la cobertura de una tarea.

  Las tareas para selecciones de dispositivos siempre se ejecutan de forma programada por el Servidor de administración. Estas tareas no se pueden ejecutar en dispositivos que carecen de conexión con el Servidor de administración. Las tareas cuya cobertura se especifica mediante otros métodos se ejecutan directamente en los dispositivos y, por lo tanto, no dependen de la conexión del dispositivo al Servidor de administración.

  Las tareas para selecciones de dispositivos no se ejecutan en la hora local de un dispositivo; en su lugar, se ejecutan en la hora local del Servidor de administración. Las tareas cuya cobertura se especifica mediante otros métodos se ejecutan en la hora local de un dispositivo.

Cómo se relaciona la configuración de la aplicación local con las directivas

Se pueden utilizar directivas para establecer valores idénticos de la configuración de la aplicación para todos los dispositivos de un grupo.

Los valores de los ajustes especificados por una directiva pueden ser redefinidos para dispositivos individuales de un grupo utilizando los ajustes de la aplicación local. Se pueden establecer solo los valores de los parámetros que la directiva permite modificar, es decir, los parámetros desbloqueados.

El valor de un ajuste que una aplicación utiliza en un dispositivo cliente (consulte la figura siguiente) se determina por la posición del candado (🔒) para ese parámetro en la directiva:

- Si la modificación del parámetro está bloqueada, el mismo valor definido en la directiva se utiliza en todos los dispositivos cliente.
- Si el parámetro de modificación está desbloqueado, la aplicación utiliza un valor de configuración local en cada dispositivo cliente en lugar del valor especificado en la directiva. Así, se puede cambiar el parámetro en los parámetros de aplicación locales.

Directiva y parámetros de aplicación locales

Esto significa que cuando una tarea se ejecuta en el dispositivo cliente, la aplicación aplica los parámetros definidos de dos maneras diferentes:

- Por parámetros de tarea y configuración de la aplicación local si el parámetro no está bloqueado contra cambios en la directiva.
- Por directiva de grupo si el parámetro está bloqueado contra cambios.

La configuración de aplicación local se cambia una vez que se aplica por primera vez la directiva, de acuerdo con los parámetros de la directiva.

Punto de distribución

Un *punto de distribución* (anteriormente conocido como agente de actualización) es un dispositivo con el Agente de red instalado que se utiliza para la distribución de actualizaciones, la instalación remota de aplicaciones y la recuperación de información relativa a dispositivos en red. Un punto de distribución puede realizar las siguientes funciones:

- Distribuir las actualizaciones y los paquetes de instalación que se reciben del Servidor de administración a los dispositivos cliente del grupo (incluidos métodos como la multidifusión mediante UDP). Las actualizaciones se pueden recuperar del Servidor de administración o de servidores de actualización de Kaspersky. En el segundo caso, se debe crear una tarea de actualización para el punto de distribución.

Los dispositivos de punto de distribución con macOS no pueden descargar actualizaciones de los servidores de actualización de Kaspersky.

Si uno o más dispositivos incluidos en la cobertura de la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* ejecutan macOS, la tarea se completa con el estado *Fallo*, incluso si se completa correctamente en todos los dispositivos de Windows.

Los puntos de distribución aceleran la distribución de actualizaciones y liberan recursos del Servidor de administración.

- Distribuir directivas y tareas de grupos con la multidifusión mediante UDP.
- Ejercer de puerta de enlace de conexión para el Servidor de administración para los dispositivos del grupo de administración.

  Si no se puede establecer una conexión directa entre los dispositivos administrados del grupo y el Servidor de administración, se puede utilizar el punto de distribución como puerta de enlace de conexión al Servidor de administración para este grupo. En este caso, los dispositivos administrados se conectarán a la puerta de enlace de conexión, que se conectará a su vez al Servidor de administración.

  La presencia de un punto de distribución que ejerce como puerta de enlace de conexión no excluye la opción de conexión directa entre los dispositivos administrados y el Servidor de administración. Si la puerta de enlace de conexión no está disponible, pero técnicamente se puede establecer una conexión directa con el Servidor de administración, los dispositivos administrados se conectarán directamente al servidor.
- Sondear la red para detectar dispositivos nuevos y actualizar la información sobre los existentes. Un punto de distribución puede aplicar los mismos métodos de detección de dispositivos que el Servidor de administración.
- Realizar la instalación remota de aplicaciones de terceros y Kaspersky a través de las herramientas de Microsoft Windows, incluida la instalación en los dispositivos cliente sin el Agente de red.

  Esta función permite transferir de forma remota paquetes de instalación del Agente de red a los dispositivos cliente de las redes a las que el Servidor de administración no tiene acceso directo.
- Actúa como un servidor proxy que participa en Kaspersky Security Network.

  Puede habilitar el proxy de KSN en el lado del punto de distribución para hacer que el dispositivo actúe como proxy de KSN. En este caso, el servicio de Proxy de KSN (ksnproxy) se ejecuta en el dispositivo.

Los archivos se transmiten desde el Servidor de administración a un punto de distribución mediante HTTP o, si está activada la conexión SSL, mediante HTTPS. La utilización del HTTP o HTTPS se traduce en un rendimiento más alto, comparado con SOAP, gracias a la reducción del tráfico.

Los dispositivos que tienen instalado Agente de red se pueden designar como puntos de distribución manualmente (por parte del administrador) o de forma automática (por parte del Servidor de administración). La lista completa de los puntos de distribución para los grupos de administración especificados se muestra en el informe sobre la lista de puntos de distribución.

La cobertura de un punto de distribución es definida por el administrador. La cobertura incluye el grupo de administración asignado y sus subgrupos, de todos los niveles de anidamiento. Si se han asignado varios puntos de distribución a la jerarquía de los grupos de administración, el Agente de red del dispositivo administrado se conecta al punto de distribución más cercano en la jerarquía.

Una ubicación de red también puede estar bajo la cobertura de los puntos de distribución. La ubicación de red se utiliza entonces para la creación manual de un conjunto de dispositivos en los que el punto de distribución distribuirá las actualizaciones. La ubicación de la red solo puede estar determinada para dispositivos que ejecutan un sistema operativo Windows.

Si el Servidor de administración asigna puntos de distribución automáticamente, lo hace por dominios de difusión, no por grupos de administración. Esto tiene lugar si se conocen todos los dominios de difusión. El Agente de red intercambia mensajes con otros Agentes de red de la misma subred; a continuación, envía al Servidor de administración información sobre sí mismo y otros Agentes de red. El Servidor de administración puede utilizar dicha información para agrupar Agentes de red por dominios de difusión. El Servidor de administración conoce los dominios de difusión tras haber sondeado a más del 70 % de los Agentes de red en grupos de administración. El Servidor de administración sondea dominios de difusión cada dos horas. Después de asignar puntos de distribución por dominios de difusión, no se pueden reasignar por grupos de administración.

Si el administrador asigna manualmente puntos de distribución, se pueden asignar a grupos de administración o ubicaciones de red.

Los Agentes de red con el perfil de conexión activo no participan en la detección de dominios de difusión.

Kaspersky Security Center asigna a cada Agente de red una dirección IP de difusión múltiple única que se diferencia del resto de direcciones. Esto permite evitar una sobrecarga de red debida a superposiciones de IP. La función de asignación de dirección única funciona en Kaspersky Security Center 10 Service Pack 3 y versiones posteriores. Las direcciones IP de difusión múltiple que se asignaron en versiones anteriores de la aplicación no se cambiarán.

Si dos o más puntos de distribución se asignan a una sola área de red o un solo grupo de administración, uno de ellos se convierte en el punto de distribución activo y los demás, en puntos de distribución en espera. El punto de distribución activo descarga actualizaciones y paquetes de instalación directamente del Servidor de administración; por su parte, los puntos de distribución en espera solo reciben actualizaciones del punto de distribución activo. En este caso, los archivos se descargan una sola vez del Servidor de administración y después se distribuyen entre los puntos de distribución. Si el punto de distribución activo deja de estar disponible por cualquier motivo, uno de los que están en espera se convierte en punto de distribución activo. El Servidor de administración asigna automáticamente un punto de distribución para que funcione en modo de espera.

El estado del punto de distribución (*Activo*/*En espera*) se muestra con una casilla de verificación en el informe klnagchk.

Un punto de distribución necesita como mínimo 4 GB de espacio libre en disco. Si el espacio libre en disco del punto de distribución es menor a 2 GB, Kaspersky Security Center crea un incidente con el nivel de importancia *Advertencia*. El incidente se publicará en las propiedades del dispositivo, en la sección **Incidentes**.

La ejecución de tareas de instalación remotas en un dispositivo asignado como punto de distribución requiere espacio libre adicional en disco. El volumen de espacio libre en el disco debe superar el tamaño total de todos los paquetes de instalación que se instalarán.

La ejecución de tareas de actualización (parche) y tareas de reparación de la vulnerabilidad en un dispositivo asignado como punto de distribución requiere espacio libre adicional en disco. El volumen de espacio libre en el disco debe ser al menos el doble del tamaño total de todos los parches que se instalarán.

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Puerta de enlace de conexión

Una *puerta de enlace de conexión* es un Agente de red que actúa en un modo especial. Una puerta de enlace de conexión acepta conexiones de otros Agentes de red y las conecta al Servidor de administración a través de su propia conexión con el Servidor. A diferencia de un Agente de red normal, una puerta de enlace de conexión espera las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración.

Una puerta de enlace de conexión puede recibir conexiones de hasta 10 000 dispositivos.

Tiene dos opciones para usar puertas de enlace de conexión:

- Le recomendamos que instale una puerta de enlace de conexión en una zona desmilitarizada (DMZ). Para otros Agentes de red instalados en dispositivos fuera de la oficina, debe configurar especialmente una conexión al Servidor de administración a través de la puerta de enlace de conexión.

  Una puerta de enlace de conexión no modifica ni procesa de ninguna manera los datos que se transmiten desde los Agentes de red al Servidor de administración. Además, no escribe estos datos en ningún búfer y, por lo tanto, no puede aceptar datos de un Agente de red y luego reenviarlos al Servidor de administración. Si el Agente de red intenta conectarse al Servidor de administración a través de la puerta de enlace de conexión, pero la puerta de enlace de la conexión no puede conectarse al Servidor de administración, el Agente de red asume que el Servidor de administración está inaccesible. Todos los datos permanecen en el Agente de red (no en la puerta de enlace de conexión).

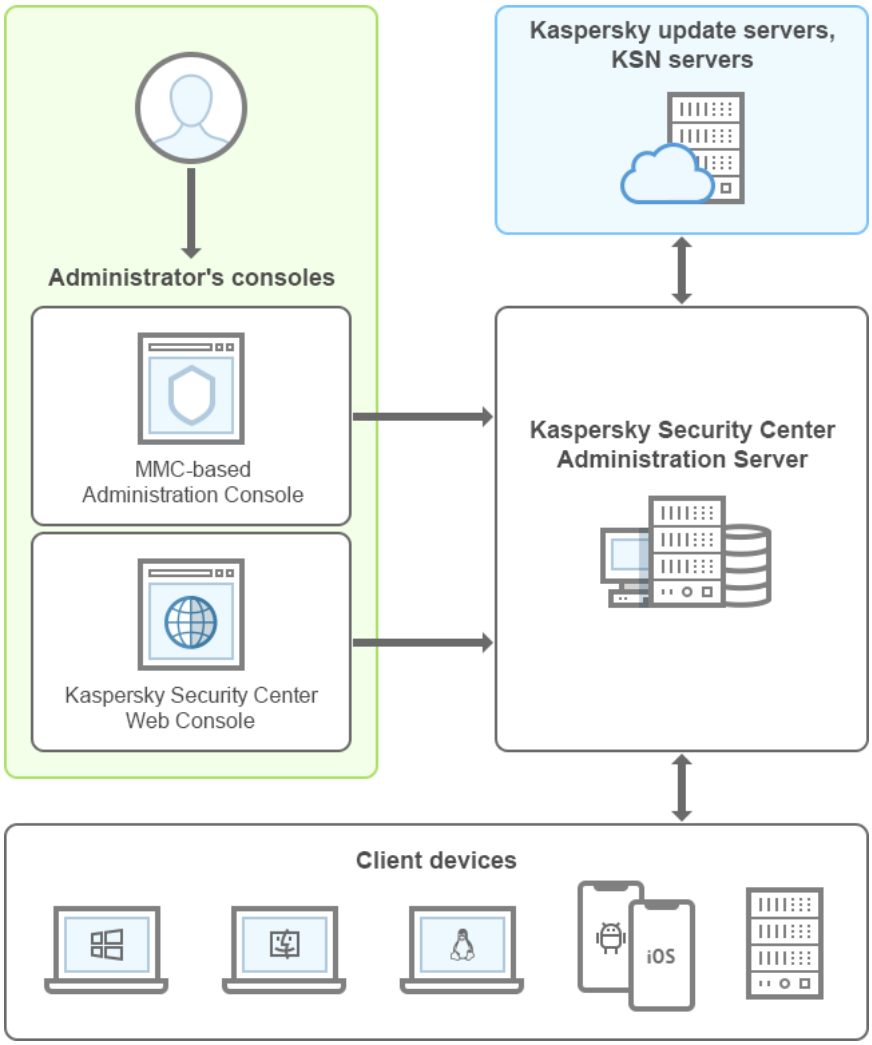
  Una puerta de enlace de conexión no puede conectarse al Servidor de administración a través de otra puerta de enlace de conexión. Significa que el Agente de red no puede ser al mismo tiempo una puerta de enlace de conexión y usar una puerta de enlace de conexión para conectarse al Servidor de administración.

  Todas las puertas de enlace de conexión están incluidas en la lista de puntos de distribución en las propiedades del Servidor de administración.

- También puede utilizar puertas de enlace de conexión dentro de la red. Por ejemplo, los puntos de distribución asignados automáticamente también se convierten en pasarelas de conexión dentro de su propio alcance. Sin embargo, dentro de una red interna, las puertas de enlace de conexión no proporcionan un beneficio considerable. Reducen la cantidad de conexiones de red que recibe el Servidor de administración, pero no reducen el volumen de datos entrantes. Incluso sin puertas de enlace de conexión, todos los dispositivos pueden conectarse al Servidor de administración.

Arquitectura

Esta sección proporciona una descripción de los componentes de Kaspersky Security Center y su interacción.



Arquitectura de Kaspersky Security Center

Kaspersky Security Center consta de los siguientes componentes básicos:

- *Consola de administración* (en adelante la *Consola*). Le proporciona una interfaz del usuario a los servicios de administración del Servidor de administración y el Agente de red. La Consola de administración se implementa en forma de un complemento para Microsoft Management Console (MMC). La Consola de administración permite la conexión al Servidor de administración de forma remota a través de Internet.

- *Kaspersky Security Center Web Console*. Proporciona una interfaz web para crear y mantener el sistema de protección de la red de una organización cliente que es administrada por Kaspersky Security Center.

- *Servidor de administración de Kaspersky Security Center* (también denominado *Servidor*). Centraliza el almacenamiento de la información sobre las aplicaciones instaladas en la red de la organización y sobre cómo administrarlas.

- *Servidores de actualización de Kaspersky*. Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación.

- *Servidores de KSN*. Servidores que contienen una base de datos de Kaspersky con información actualizada constantemente sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network garantiza respuestas más rápidas de las aplicaciones Kaspersky a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos.

- *Dispositivos cliente*. Dispositivos de la empresa cliente protegidos por Kaspersky Security Center. Cada dispositivo que debe protegerse debe tener instalada una de las aplicaciones de seguridad de Kaspersky.

Escenario de instalación principal

Siguiendo este escenario, puede desplegar el Servidor de administración, así como instalar el Agente de red y aplicaciones de seguridad en dispositivos en red. Puede usar este escenario tanto para ver de cerca la aplicación como para la instalación de la aplicación para otros trabajos.

Para obtener información sobre el despliegue de Kaspersky Security Center Cloud Console, consulte la documentación de Kaspersky Security Center Cloud Console.

La instalación de Kaspersky Security Center consta de los siguientes pasos:

1. Tareas preliminares.
2. Instalación de Kaspersky Security Center y una aplicación de seguridad de Kaspersky en el dispositivo del Servidor de administración.
3. Despliegue centralizado de aplicaciones de seguridad de Kaspersky en dispositivos cliente

El despliegue de Kaspersky Security Center en los entornos de nube y el despliegue de Kaspersky Security Center para proveedores de servicios se describen en otras secciones de Ayuda.

Recomendamos que asigne aproximadamente una hora para la instalación del Servidor de administración y un mínimo de un día hábil para la finalización del escenario. También recomendamos que instale una aplicación de seguridad, como Kaspersky Security for Windows Server o Kaspersky Endpoint Security, en el equipo que actuará como Servidor de administración de Kaspersky Security Center.

Una vez completado el escenario, la protección queda desplegada en la red de la organización de la siguiente manera:

- Se instala el DBMS para el Servidor de administración.
- Se instala el Servidor de administración de Kaspersky Security Center.
- Se crearán todas las directivas y las tareas requeridas; se especificarán las configuraciones predeterminadas de las directivas y las tareas.
- Se instalarán las aplicaciones de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) y el Agente de red en los dispositivos administrados.
- Se crearán los grupos de administración (pueden aparecer combinados en una jerarquía).
- Si es necesario, se desplegará la protección de dispositivos móviles.
- Se asignarán los puntos de distribución, si es necesario.

La instalación de Kaspersky Security Center se realiza en etapas:

Tareas preliminares.

1. **Obtención de los archivos necesarios**

   Asegúrese de tener una clave de licencia (código de activación) para Kaspersky Security Center o claves de licencia (códigos de activación) para las aplicaciones de seguridad de Kaspersky.

Desempaquete el archivo que recibió de su proveedor. Este archivo contiene las claves de licencia (archivos KEY), códigos de activación y la lista de aplicaciones de Kaspersky que se pueden activar con cada clave de licencia.

Si primero desea probar Kaspersky Security Center, puede obtener una prueba gratuita de 30 días en el sitio web de Kaspersky.

Para obtener información detallada sobre las licencias de las aplicaciones de seguridad de Kaspersky que no están incluidas en Kaspersky Security Center, puede consultar la documentación de esas aplicaciones.

2. **Selección de una estructura para la protección de una organización**

   Más información sobre los componentes de Kaspersky Security Center. Seleccione la estructura de protección y la configuración de la red que más convenientes resulten para su organización. Según la configuración de red y el rendimiento de los canales de comunicación, debe definir el número de Servidores de administración que se usarán y cómo deben distribuirse entre sus oficinas (en caso de que gestione una red distribuida).

   Para obtener y mantener un rendimiento óptimo en diferentes condiciones operativas, debe tener en cuenta la cantidad de dispositivos en red, la topología de red y el conjunto de funciones de Kaspersky Security Center que necesita (para obtener más información, consulte la Guía de dimensionamiento de Kaspersky Security Center).

   Defina si se utilizará una jerarquía de Servidores de administración en su organización. Para hacer esto, debe evaluar si es posible y oportuno abarcar todos los dispositivos cliente con un solo Servidor de administración o si es necesario construir una jerarquía de Servidores de administración. También es posible que deba construir una jerarquía de Servidores de administración que sea idéntica a la estructura de la organización cuya red quiera proteger.

   Si debe garantizar la protección de dispositivos móviles, realice todas las acciones previamente necesarias para la configuración de un Servidor de dispositivos móviles de Exchange y Servidor de MDM para iOS.

   Asegúrese de que los dispositivos que seleccionó como Servidores de administración, así como aquellos para la instalación de la Consola de administración, cumplan con todos los requisitos de hardware y software.

3. **Preparación para el uso de certificados personalizados**

   Si la infraestructura de clave pública (PKI) de su organización requiere que utilice certificados personalizados emitidos por una autoridad de certificación (CA) específica, prepare esos certificados y asegúrese de que cumplan con todos los requisitos.

4. **Preparación para la obtención de licencias de Kaspersky Security Center**

   Si planea usar una versión de Kaspersky Security Center con Administración de dispositivos móviles, Integración con los sistemas SIEM o Administración de vulnerabilidades y parches, asegúrese de tener un archivo clave o código de activación para la licencia de la aplicación.

5. **Preparación para la obtención de licencias de aplicaciones de seguridad administradas**

   Durante el despliegue de la protección, deberá facilitarle a Kaspersky las claves de licencia activas de las aplicaciones que planea administrar a través de Kaspersky Security Center (consulte la lista de aplicaciones de seguridad administrables). Para obtener información detallada sobre la licencia de cualquier aplicación de seguridad, puede consultar la documentación de esta aplicación.

6. **Selección de la configuración de hardware del Servidor de administración y del DBMS**

   Planifique la configuración de hardware para el DBMS y el Servidor de administración teniendo en cuenta la cantidad de dispositivos en su red.

7. **Selección de un DBMS**

Al seleccionar un DBMS, tenga en cuenta el número de dispositivos administrados que debe abarcar este Servidor de administración. Si su red incluye menos de 10 000 dispositivos y no planea aumentar este número, puede elegir un DBMS gratuito, como SQL Express o MySQL, e instalarlo en el mismo dispositivo que el Servidor de administración. Alternativamente, puede elegir el DBMS MariaDB, que le permite administrar hasta 20 000 dispositivos. Si su red incluye más de 10.000 dispositivos (o si planea ampliar su red hasta esa cantidad de dispositivos), le recomendamos que elija un DBMS SQL de pago y que lo instale en un dispositivo exclusivo. Un DBMS de pago puede funcionar con varios Servidores de administración, pero un DBMS gratuito puede funcionar solo con uno.

Si selecciona SQL Server DBMS, tenga en cuenta que puede migrar los datos almacenados en la base de datos a MySQL, MariaDB o Azure SQL SGBD. Para realizar la migración, haga una copia de seguridad de sus datos y restáurelos en el nuevo DBMS.

8. **Instalación del DBMS y creación de la base de datos**

   Más información sobre las cuentas para trabajar con DBMS e instalar su DBMS. Anote y guarde la configuración de DBMS, ya que los necesitará durante la instalación del Servidor de administración. Esta configuración incluye el nombre del equipo SQL Server, el número de puerto usado para la conexión a SQL Server, el nombre y la contraseña de la cuenta para acceder al equipo de SQL Server.

   De forma predeterminada, el programa de instalación de Kaspersky Security Center crea la base de datos para el almacenamiento de información del Servidor de administración, pero puede optar por dejar de crear esta base de datos y usar otra base de datos. En este caso, asegúrese de que la base de datos se haya creado, de saber cuál es su nombre, y de que la cuenta con la cual el Servidor de administración accederá a esta base de datos tenga la función db_owner para ello.

   Si es necesario, póngase en contacto con su administrador del DBMS para obtener más información.

9. **Configuración de puertos**

   Asegúrese de que todos los puertos necesarios estén abiertos para la interacción entre los componentes de acuerdo con la estructura de seguridad que haya seleccionado.

   Si debe proporcionar acceso a Internet al Servidor de administración, configure los puertos y especifique la configuración de conexión, según la configuración de red.

10. **Comprobación de cuentas**

    Asegúrese de tener todos los derechos de administrador local requeridos para la instalación correcta del Servidor de administración de Kaspersky Security Center y el futuro despliegue de la protección en los dispositivos. Los derechos de administrador local en los dispositivos cliente son necesarios para la instalación del Agente de red en estos dispositivos. Después de instalar el Agente de red, puede usarlo para instalar aplicaciones en dispositivos de forma remota, sin usar la cuenta con los derechos de administrador del dispositivo.

    De forma predeterminada, en el dispositivo seleccionado para la instalación del Servidor de administración, el programa de instalación de Kaspersky Security Center crea tres cuentas locales en las que se ejecutarán el Servidor de administración y los servicios de Kaspersky Security Center:

    - KL-AK-*: Cuenta de servicio del Servidor de administración.
    - KlScSvc: Cuenta para otros servicios desde el conjunto del Servidor de administración.
    - KlPxeUser: Cuenta para el despliegue de sistemas operativos.

    Puede optar por no crear cuentas para los servicios del Servidor de administración y otros servicios. Puede utilizar sus cuentas existentes, por ejemplo cuentas de dominio, si planea instalar el Servidor de administración en un clúster de conmutación por error o si planea utilizar cuentas de dominio en vez de cuentas locales por cualquier otro motivo. En este caso, asegúrese de que las cuentas pensadas para ejecutar el Servidor de administración y los servicios de Kaspersky Security Center se hayan creado, que no tengan privilegios y que tengan todos los permisos requeridos para el acceso al DBMS. (Si planea desplegar más sistemas operativos en dispositivos a través de Kaspersky Security Center, no descarte crear cuentas).

Instalación de Kaspersky Security Center y una aplicación de seguridad de Kaspersky en el dispositivo del Servidor de administración

1. **Instalación del Servidor de administración, la Consola de administración, Kaspersky Security Center 14 Web Console y los complementos de administración para aplicaciones de seguridad**

   Descargue Kaspersky Security Center del sitio web de Kaspersky. Puede descargar el paquete completo, solo Web Console o solo la consola de administración.

   Instale el Servidor de administración en el dispositivo seleccionado (o en varios dispositivos, si planea usar varios Servidores de administración). Puede seleccionar la instalación estándar o personalizada del Servidor de administración. La Consola de administración se instala junto con el Servidor de administración. Se recomienda instalar el Servidor de administración en un servidor dedicado, y no en un controlador de dominio.

   Se recomienda la instalación estándar si desea probar Kaspersky Security Center, por ejemplo, comprobando su funcionamiento en un área pequeña dentro su red. Durante la instalación estándar, solo configura la base de datos. También puede instalar solo el conjunto predeterminado de complementos de administración para las aplicaciones de Kaspersky. También puede utilizar la instalación estándar si ya tiene experiencia de trabajo con Kaspersky Security Center y sabe cómo especificar todas las configuraciones relevantes después de la instalación estándar.

   La instalación personalizada se recomienda si planea modificar la configuración de Kaspersky Security Center, como la ruta a la carpeta compartida, las cuentas y los puertos para la conexión con el Servidor de administración y la configuración de la base de datos. La instalación personalizada le permite especificar qué complementos de administración de Kaspersky instalar. Si es necesario, puede iniciar la instalación personalizada en el modo no interactivo.

   La Consola de administración y la versión de servidor del Agente de red se instalan junto con el Servidor de administración. También puede decidir instalar Kaspersky Security Center 14 Web Console durante la instalación.

   Si lo desea, instala la Consola de administración y/o Kaspersky Security Center 14 Web Console en la estación de trabajo del administrador por separado para administrar el Servidor de administración en la red.

2. **Instalación inicial y obtención de licencias**

   Cuando la instalación del Servidor de administración se completa, en la primera conexión con el Servidor de administración, el Asistente de inicio rápido comienza automáticamente. Realice la configuración inicial del Servidor de administración según los requisitos existentes. Durante la etapa de configuración inicial, el Asistente usa la configuración predeterminada para crear las directivas y las tareas que son necesarias para desplegar la protección. Sin embargo, las configuraciones predeterminadas pueden no ser óptimas para las necesidades de su organización. Si es necesario, puede editar la configuración de directivas y tareas (Configurando la protección en una red de organización cliente, Escenario: Configuración de protección de la red).

   Si planea utilizar funciones que van más allá de la funcionalidad básica, debe obtener una licencia para la aplicación. Puede hacerlo en uno de los pasos del Asistente de inicio rápido.

3. **Comprobación de la instalación del Servidor de administración para un correcto funcionamiento**

   Cuando se completan todos los pasos anteriores, el Servidor de administración queda instalado y listo para su uso.

   Asegúrese de que la Consola de administración se esté ejecutando y de que pueda conectarse al Servidor de administración a través de la Consola de administración. Además, asegúrese de que la descarga de actualizaciones en el repositorio del Servidor de administración esté disponible en la tarea del Servidor de administración (en la carpeta **Tareas** del árbol de la consola), así como la directiva de Kaspersky Endpoint Security (en la carpeta **Directivas** del árbol de la consola).

   Cuando haya terminado la comprobación, continúe con los siguientes pasos.

Despliegue centralizado de aplicaciones de seguridad de Kaspersky en dispositivos cliente

1. **Detección de dispositivos en red**

Este paso forma parte del Asistente de inicio rápido. También puede iniciar la Detección de dispositivos manualmente. Kaspersky Security Center recibe las direcciones y los nombres de todos los dispositivos detectados en la red. A continuación, puede usar Kaspersky Security Center para instalar aplicaciones y software de Kaspersky desde otros proveedores en los dispositivos detectados. Cada cierto tiempo, Kaspersky Security Center inicia una detección de dispositivos, lo que significa que si aparece alguna instancia nueva en la red, se detectará automáticamente.

2. **Instalación del Agente de red y de aplicaciones de seguridad en dispositivos en red**

   El despliegue de la protección (Configuración de un sistema de protección en la red de la organización cliente, Escenario: Configuración de protección de la red) en la red de una organización implica la instalación del Agente de red y de aplicaciones de seguridad (por ejemplo, Kaspersky Endpoint Security) en dispositivos que el Servidor de administración ha detectado durante la detección de dispositivos.

   Las aplicaciones de seguridad protegen los dispositivos frente a virus u otros programas que suponen una amenaza. El Agente de red garantiza la comunicación entre el dispositivo y el Servidor de administración. Los ajustes del Agente de red se configuran automáticamente de forma predeterminada.

   Si lo desea, puede instalar el Agente de red en modo silencioso con un archivo de respuesta o sin un archivo de respuesta.

   Antes de iniciar la instalación del Agente de red y las aplicaciones de seguridad en los dispositivos de la red, asegúrese de que pueda acceder a estos dispositivos (es decir, que estén encendidos). Usted puede instalar el Agente de red en máquinas virtuales y en dispositivos físicos.

   Las aplicaciones de seguridad y el Agente de red se pueden instalar de forma remota o local.

   Instalación remota: mediante el Asistente de despliegue de la protección, puede instalar de forma remota las aplicaciones de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) y el Agente de red en aquellos dispositivos que el Servidor de administración haya detectado en la red de la organización. Normalmente, la tarea de instalación remota despliega correctamente la protección en la mayoría de los dispositivos de la red. Sin embargo, puede devolver un error en algunos dispositivos si, por ejemplo, un dispositivo está apagado o no se puede abrir por algún otro motivo. En este caso, recomendamos que conecte al dispositivo manualmente y use la instalación local.

   Instalación local: se utiliza en dispositivos de la red en los cuales la protección no se podía desplegar usando la tarea de instalación remota. Para instalar la protección en dichos equipos, cree un paquete de instalación independiente que pueda ejecutar de forma local en esos dispositivos.

   La instalación del Agente de red en dispositivos con sistemas operativos Linux y macOS se describe en la documentación de Kaspersky Endpoint Security for Linux y Kaspersky Endpoint Security for Mac, respectivamente. (Aunque los dispositivos con los sistemas operativos Linux y macOS se consideran menos vulnerables que los dispositivos con Windows, recomendamos que aun así instale aplicaciones de seguridad en ellos).

   Después de la instalación, compruebe que la aplicación de seguridad esté instalada en los dispositivos administrados. Ejecute un informe de la versión de software de Kaspersky y vea sus resultados.

3. **Despliegue de claves de licencia en dispositivos cliente**

   Despliegue claves de licencia en los dispositivos cliente para activar las aplicaciones de seguridad administradas en esos dispositivos.

4. **Configuración de protección de dispositivos móviles**

   Este paso forma parte del Asistente de inicio rápido.

   Si desea administrar dispositivos móviles de empresas, siga los pasos necesarios para preparar y desplegar la Administración de dispositivos móviles.

5. **Creación de una estructura de grupo de administración**

En algunos casos, para desplegar la protección en dispositivos en red de la forma más cómoda puede ser necesario dividir el conjunto completo de dispositivos en grupos de administración, tomando en cuenta la estructura de la organización. Puede crear reglas de movimiento para distribuir dispositivos entre grupos o puede distribuir dispositivos manualmente. Puede asignar tareas de grupo para grupos de administración, definir la cobertura de las directivas y asignar puntos de distribución.

Asegúrese de que todos los dispositivos administrados se hayan asignado correctamente a los grupos de administración apropiados, y de que ya no haya dispositivos no asignados en la red.

6 **Asignando los puntos de distribución**

Kaspersky Security Center asigna automáticamente puntos de distribución a los grupos de administración, pero también puede asignarlos manualmente, si es necesario. En redes grandes, recomendamos que use puntos de distribución para reducir la carga sobre el Servidor de administración y las redes que tengan una estructura distribuida para proporcionar al Servidor de administración acceso a los dispositivos (o grupos de dispositivos) conectados mediante canales de baja velocidad. Puede utilizar dispositivos que ejecutan Linux como puntos de distribución, así como dispositivos que ejecutan Windows.

Puertos utilizados por Kaspersky Security Center

Las siguientes tablas muestran los puertos predeterminados que deben estar abiertos en los Servidores de administración y en los dispositivos cliente (consulte la siguiente tabla). Si lo desea, puede cambiar los números de puerto predeterminados.

Las siguientes tablas muestran los puertos predeterminados que deben estar abiertos en los Servidores de administración y en los dispositivos cliente (consulte la siguiente tabla). Sin embargo, si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL-Server y el servidor MariaDB, o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

Puertos que deben estar abiertos en el Servidor de administración

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
8060	klcsweb	TCP	Transmisión de paquetes de instalación publicados a dispositivos cliente	Publicación de paquetes de instalación. Puede cambiar el número de puerto predeterminado en la sección **Servidor web** de la ventana de propiedades del Servidor de administración en la Consola de administración o en Kaspersky Security Center 14 Web Console.
8061	klcsweb	TCP (TLS)	Transmisión de paquetes de instalación publicados a dispositivos cliente	Publicación de paquetes de instalación.

				Puede cambiar el número de puerto predeterminado en la sección **Servidor web** de la ventana de propiedades del Servidor de administración en la Consola de administración o en Kaspersky Security Center 14 Web Console.
13000	klserver	TCP (TLS)	Recepción de conexiones de Agentes de red y Servidores de administración secundarios; también se usa en Servidores de administración secundarios para recibir conexiones del Servidor de administración principal (por ejemplo, si el Servidor de administración secundarios está en la DMZ)	Administración de dispositivos cliente y Servidores de administración secundarios. Puede cambiar el número del puerto predeterminado para recibir conexiones de los Agentes de red al configurar los puertos de conexión; puede cambiar el número del puerto predeterminado para recibir conexiones de los Servidores de administración secundarios al crear una jerarquía de Servidores de administración en la Consola de administración o en Kaspersky Security Center 14 Web Console.
13000	klserver	UDP	Recepción de información sobre dispositivos que se apagaron desde Agentes de red	Administración de dispositivos cliente. Puede cambiar el número de puerto predeterminado en la configuración de la directiva del Agente de red en la Consola de administración o en Kaspersky Security Center 14 Web Console.
13291	klserver	TCP (TLS)	Configuración de conexiones de la Consola de administración al Servidor de administración	Gestión del Servidor de administración. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración en la Consola de administración.
13299	klserver	TCP (TLS)	Recibiendo conexiones desde Kaspersky Security Center 14 Web Console al Servidor de administración; recibiendo conexiones al Servidor de administración sobre OpenAPI	Kaspersky Security Center 14 Web Console, OpenAPI. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración (en la sección secundaria **Puertos de conexión** en la Sección **general**) en la Consola de administración, o al crear una jerarquía de Servidores de administración en la Consola de administración o en Kaspersky Security Center 14 Web Console.
14000	klserver	TCP	Recepción de conexiones de Agentes de red	Administración de dispositivos cliente.

				Puede cambiar el número de puerto predeterminado al configurar puertos de conexión durante la instalación de Kaspersky Security Center o al conectar manualmente un dispositivo cliente al Servidor de administración.
13111 (solo si el servicio de Proxy de KSN se ejecuta en el dispositivo)	ksnproxy	TCP	Recepción de solicitudes de dispositivos administrados al Servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración.
15111 (solo si el servicio de Proxy de KSN se ejecuta en el dispositivo)	ksnproxy	UDP	Recepción de solicitudes de dispositivos administrados al Servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración.
17000	klactprx	TCP (TLS)	Recepción de conexiones para la activación de la aplicación de dispositivos administrados (excepto para dispositivos móviles)	Servidor proxy de activación utilizado por dispositivos no móviles para activar aplicaciones de Kaspersky con códigos de activación. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración.
17100 (solo si administra dispositivos móviles)	klactprx	TCP (TLS)	Recepción de conexiones para la activación de aplicaciones de dispositivos móviles	Activación del Servidor proxy para dispositivos móviles. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración.
19170	klserver	HTTPS (TLS)	Uso de la utilidad klsctunnel para tunelizar conexiones a dispositivos administrados	Conexión remota a dispositivos administrados mediante Kaspersky Security Center 14 Web Console. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración (en la sección secundaria **Puertos adicionales** en la Sección **general**) en la Consola de administración únicamente.
13292 (solo si administra dispositivos móviles)	klserver	TCP (TLS)	Recepción de conexiones de dispositivos móviles	Administración de dispositivos móviles. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del Servidor de administración en la consola de administración o en Kaspersky Security Center 14 Web Console.
13294 (solo si administra	klserver	TCP (TLS)	Recepción de conexiones de dispositivos con protección de UEFI	Administración de dispositivos cliente con protección de UEFI.

dispositivos móviles)				Puede cambiar el número de puerto predeterminado al conectar dispositivos móviles, o más tarde en la ventana de propiedades del Servidor de administración (en la sección secundaria **Puertos adicionales** en la Sección general) en la Consola de administración o en Kaspersky Security Center 14 Web Console.

La siguiente tabla muestra el puerto que debe estar abierto en el servidor de MDM para iOS (solo si administra dispositivos móviles).

Puerto utilizado por del servidor de MDM para iOS d Kaspersky Security Center

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
443	kliosmdmservicesrv	TCP (TLS)	Recepción de conexiones de dispositivos móviles con iOS	Administración de dispositivos móviles. Puede cambiar el número de puerto predeterminado al instalar el servidor de MDM para iOS.

La siguiente tabla muestra el puerto que debe estar abierto en Kaspersky Security Center Web Console Server. Puede ser el mismo dispositivo donde está instalado el Servidor de administración o un dispositivo diferente.

Puerto utilizado por Kaspersky Security Center Web Console Server

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
8080	Node.js: JavaScript del lado del servidor	TCP (TLS)	Recibiendo conexiones del navegador web a Kaspersky Security Center 14 Web Console	Kaspersky Security Center 14 Web Console. Puede cambiar el número de puerto predeterminado al instalar Kaspersky Security Center 14 Web Console en un dispositivo con Windows o en una plataforma Linux. Si instala Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto que no sea 8080, ya que el sistema operativo usa el puerto 8080.

La siguiente tabla muestra el puerto que debe estar abierto en los dispositivos administrados donde está instalado el Agente de red.

Puertos utilizados por el Agente de red

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
15000	klnagent	UDP	Señales de gestión del Servidor de administración a los Agentes de red	Administración de dispositivos cliente.

				Puede cambiar el número de puerto predeterminado en la configuración de la directiva del Agente de red en la Consola de administración o en Kaspersky Security Center 14 Web Console.
15000	klnagent	Transmisión UDP	Obtención de datos sobre otros Agentes de red dentro del mismo dominio de transmisión (los datos se envían al Servidor de administración)	Entrega de actualizaciones y paquetes de instalación.

La siguiente tabla muestra los puertos que deben estar abiertos en un dispositivo administrado que tenga el Agente de red instalado actuando como un punto de distribución.

Puertos utilizados por el Agente de red que funciona como punto de distribución

Número de puerto	Nombre del proceso que abre el puerto	Protocolo	Objetivo del puerto	Cobertura
13000	klnagent	TCP (TLS)	Recepción de conexiones de Agentes de red	Administración de dispositivos cliente, entrega de actualizaciones y paquetes de instalación Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center 14 Web Console.
13111 (solo si el servicio de Proxy de KSN se ejecuta en el dispositivo)	ksnproxy	TCP	Recepción de solicitudes de dispositivos administrados al Servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center 14 Web Console.
15001	klnagent	UDP	Multidifusión para Agentes de red	Entrega de actualizaciones y paquetes de instalación. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center 14 Web Console.
15111 (solo si el servicio de Proxy de KSN se ejecuta en el dispositivo)	ksnproxy	UDP	Recepción de solicitudes de dispositivos administrados al Servidor proxy de KSN	Servidor proxy de KSN. Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center 14 Web Console.
13295 (solo si utiliza el punto de distribución	klnagent	TCP (TLS)	Envío de notificaciones push a los	Servidor push.

como servidor push)			dispositivos administrados	Puede cambiar el número de puerto predeterminado en la ventana de propiedades del punto de distribución en la Consola de administración o en Kaspersky Security Center 14 Web Console.

Certificados para trabajar con Kaspersky Security Center

Esta sección contiene información sobre los certificados de Kaspersky Security Center y describe cómo emitir un certificado personalizado para el Servidor de administración.

Acerca de los certificados de Kaspersky Security Center

Kaspersky Security Center utiliza los siguientes tipos de certificados para permitir una interacción segura entre los componentes de la aplicación:

- Certificado del Servidor de administración
- Certificado móvil
- Certificado del Servidor de MDM para iOS
- Certificado de Kaspersky Security Center Web Server
- Certificado de Kaspersky Security Center 14 Web Console

De forma predeterminada, Kaspersky Security Center utiliza certificados autofirmados (es decir, emitidos por el propio Kaspersky Security Center), pero puede reemplazarlos por certificados personalizados para cumplir mejor con los requisitos de la red de su organización y cumplir con los estándares de seguridad. Una vez que el Servidor de administración verifica si un certificado personalizado cumple con todos los requisitos aplicables, este certificado asume el mismo alcance funcional que un certificado autofirmado. La única diferencia es que un certificado personalizado no se vuelve a emitir automáticamente al expirar. Puede reemplazar certificados autofirmados por personalizados mediante la utilidad klsetsrvcert o mediante la sección de propiedades del Servidor de administración en la Consola de administración, según el tipo de certificado. Cuando usa la utilidad klsetsrvcert, debe especificar un tipo de certificado usando uno de los siguientes valores:

- C: Certificado común para los puertos 13000 y 13291.
- CR: Certificado de reserva común para los puertos 13000 y 13291.
- M: Certificado móvil para el puerto 13292.
- MR: Certificado móvil de reserva para el puerto 13292.
- MCA: Autoridad de certificación móvil para certificados de usuario generados automáticamente.

No necesita descargar la utilidad klsetsrvcert. Está incluida en el kit de distribución de Kaspersky Security Center. La utilidad no es compatible con versiones anteriores de Kaspersky Security Center.

Certificados del Servidor de administración

Se requiere un certificado del Servidor de administración para la autenticación del Servidor de administración, así como para la interacción segura entre el Servidor de administración y el Agente de red en los dispositivos administrados. Cuando conecta la Consola de administración al Servidor de administración por primera vez, se le solicita que confirme el uso del certificado del Servidor de administración vigente. Dicha confirmación también se requiere cada vez que se reemplaza el certificado del Servidor de administración, después de cada reinstalación del Servidor de administración y cuando se conecta un Servidor de administración secundario al Servidor de administración principal. Este certificado se llama común ("C").

Además, existe un certificado de reserva común ("CR"). Kaspersky Security Center genera automáticamente este certificado 90 días antes del vencimiento del certificado común. El certificado de reserva común se utiliza más tarde para sustituir el certificado del Servidor de administración. Cuando el certificado común está a punto de caducar, el certificado de reserva común se utiliza para mantener la conexión con las instancias del Agente de red instaladas en los dispositivos administrados. Con este propósito, el certificado de reserva común se convierte automáticamente en el nuevo certificado común 24 horas antes de que expire el antiguo certificado común.

También puede realizar una copia de seguridad del certificado del Servidor de administración por separado de otras configuraciones del Servidor de administración para mover el Servidor de administración de un dispositivo a otro sin pérdida de datos.

Certificados móviles

Se requiere un certificado móvil ("M") para la autenticación del Servidor de administración en dispositivos móviles. El uso del certificado móvil se configura en el paso dedicado del Asistente de inicio rápido.

Además, existe un certificado de reserva móvil ("MR"), que se utiliza para reemplazar sin problemas el certificado móvil. Cuando el certificado móvil está a punto de caducar, el certificado de reserva móvil se utiliza para mantener la conexión con las instancias del Agente de red instaladas en los dispositivos móviles administrados. Con este propósito, el certificado de reserva móvil se convierte automáticamente en el nuevo certificado móvil 24 horas antes de que expire el antiguo certificado móvil.

Si el escenario de conexión requiere el uso de un certificado de cliente en dispositivos móviles (conexión que implica autenticación SSL bidireccional), genere esos certificados por medio de la autoridad de certificación para certificados de usuario generados automáticamente ("MCA"). Además, el Asistente de inicio rápido le permite comenzar a utilizar certificados de cliente personalizados emitidos por una autoridad de certificación diferente, mientras que la integración con la Infraestructura de clave pública (PKI) del dominio de su organización le permite emitir certificados de cliente por medio de la autoridad de certificación de su dominio.

Certificado del Servidor de MDM para iOS

Se requiere un certificado de servidor de MDM para iOS para la autenticación del Servidor de administración en dispositivos móviles que ejecutan el sistema operativo iOS. La interacción con estos dispositivos se realiza a través del protocolo de administración de dispositivos móviles (MDM) de Apple que no involucra ningún Agente de red. En su lugar, instala en cada dispositivo un perfil especial de MDM para iOS, que contiene un certificado de cliente, para garantizar la autenticación SSL bidireccional.

Además, el Asistente de inicio rápido le permite comenzar a utilizar certificados de cliente personalizados emitidos por una autoridad de certificación diferente, mientras que la integración con la Infraestructura de clave pública (PKI) del dominio de su organización le permite emitir certificados de cliente por medio de la autoridad de certificación de su dominio.

Los certificados de cliente se transmiten a dispositivos iOS cuando descarga esos perfiles de MDM de iOS. Cada certificado de cliente de Servidor de MDM para iOS es único. Todos los certificados de cliente de Servidor de MDM para iOS se generan mediante la autoridad de certificación para certificados de usuario generados automáticamente ("MCA").

Certificado de Kaspersky Security Center Web Server

Kaspersky Security Center Web Server (en adelante, Web Server), un componente del Kaspersky Security Center Administration Server, utiliza un tipo de certificado especial. Este certificado es necesario para publicar los paquetes de instalación del Agente de red que posteriormente se descargan en los dispositivos administrados, así como para publicar perfiles de MDM de iOS, aplicaciones de iOS y los paquetes de instalación de Kaspersky Security for Mobile. Para ello, Servidor Web puede utilizar varios certificados.

Si la compatibilidad con dispositivos móviles está desactivada, Servidor Web utiliza uno de los siguientes certificados, en orden de prioridad:

1. Certificado de Servidor Web personalizado que especificó manualmente mediante la Consola de administración
2. Certificado del Servidor de administración común ("C")

Si la compatibilidad con dispositivos móviles está activada, Servidor Web utiliza uno de los siguientes certificados, en orden de prioridad:

1. Certificado de Servidor Web personalizado que especificó manualmente mediante la Consola de administración
2. Certificado móvil personalizado
3. Certificado móvil autofirmado ("M")
4. Certificado del Servidor de administración común ("C")

Certificado de Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console Server tiene su propio certificado (en adelante, también denominado certificado del servidor de Web Console y de Web Console), que se requiere para la autenticación de Kaspersky Security Center 14 Web Console. Cuando abre Kaspersky Security Center 14 Web Console, el Servidor de Web Console se conecta al Servidor de administración. A su vez, el Servidor de administración solicita las credenciales de usuario y el certificado de la Web Console para verificar la autenticidad.

Cuando abre Kaspersky Security Center 14 Web Console, el navegador le informa que la conexión a Kaspersky Security Center 14 Web Console no es privada y que el certificado de Web Console no es válido. Esta advertencia aparece porque el certificado de la Web Console está autofirmado y fue generado automáticamente por Kaspersky Security Center. Para eliminar esta advertencia, puede realizar una de las acciones siguientes:

- Reemplace el certificado de Web Console por uno personalizado (opción recomendada). Cree un certificado que sea de confianza en su infraestructura y que cumpla con los requisitos de los certificados personalizados.
- Añada el certificado de Web Console a la lista de certificados de navegador de confianza. Le recomendamos que utilice esta opción solo si no puede crear un certificado personalizado.

Acerca del Certificado del Servidor de administración

Se realizan dos operaciones según el *Certificado del servidor de administración:* Autenticación del Servidor de administración durante la conexión por Consola de administración e intercambio de datos con dispositivos. El certificado también se usa para la autenticación cuando los Servidores de administración principales están conectados a Servidores de administración secundarios.

Certificado emitido por Kaspersky

El certificado del Servidor de administración se crea automáticamente durante la instalación del componente del Servidor de administración y se guarda en la carpeta ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

El certificado del Servidor de administración es válido por cinco años, si se lo emitió antes del 1 de septiembre de 2020. De lo contrario, el plazo de validez del certificado se limita a 397 días. El Servidor de administración genera un nuevo certificado como certificado de reserva 90 días antes de la fecha de caducidad del certificado actual. Posteriormente, el nuevo certificado reemplazará automáticamente el certificado actual un día antes de la fecha de caducidad. Todos los Agentes de red en los dispositivos cliente se vuelven a configurar automáticamente para autenticar el Servidor de administración con el nuevo certificado.

Si especifica un período de validez superior a 397 días para el certificado del Servidor de administración, el navegador devuelve un error.

Certificados personalizados

Si es necesario, puede asignar un certificado personalizado para el Servidor de administración. Por ejemplo, esto puede ser necesario para una mejor integración con la PKI existente de su empresa o para la configuración personalizada de los campos de certificado. Al reemplazar el certificado, todos los Agentes de red que estaban conectados anteriormente al Servidor de administración a través de SSL perderán su conexión y devolverán el "error de autenticación del Servidor de administración". Para eliminar este error, tendrá que restaurar la conexión después del reemplazo del certificado.

Si se pierde el certificado del Servidor de administración, para recuperarlo debe volver a instalar el componente Servidor de administración y restaurar los datos.

Requisitos para los certificados personalizados utilizados en Kaspersky Security Center

La siguiente tabla muestra los requisitos para los certificados personalizados especificados para diferentes componentes de Kaspersky Security Center.

Requisitos para los certificados de Kaspersky Security Center

Tipo de certificado	Requisitos	Comentarios
Certificado común, certificado de	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto	El parámetro Extended Key Usage es opcional.

reserva común ("C", "CR")	• Restricción de longitud de ruta: Ninguna Uso de la clave: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Uso extendido de claves (opcional): autenticación de servidor, autenticación de cliente.	El valor de la restricción de longitud de ruta puede ser un número entero diferente de "Ninguna", pero no menos de 1.
Certificado móvil, Certificado de reserva móvil ("M", "MR")	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto • Restricción de longitud de ruta: Ninguna Uso de la clave: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Extended Key Usage (opcional): autenticación de servidor.	El parámetro Extended Key Usage es opcional. El valor de restricción de longitud de ruta puede ser un número entero diferente de "Ninguna" si el certificado común tiene un valor de restricción de longitud de ruta no menor que "1".
CA de certificado para certificados de usuario generados automáticamente ("MCA")	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto • Restricción de longitud de ruta: Ninguna Uso de la clave: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Uso extendido de claves (opcional): autenticación de servidor, autenticación de cliente.	El parámetro Extended Key Usage es opcional. El valor de restricción de longitud de ruta puede ser diferente de "Ninguna", si el certificado común tiene un valor de restricción de longitud de ruta no menor que 1.
Certificado del	Extended Key Usage: autenticación de	No aplica.

Servidor web	servidor. El contenedor PKCS # 12 / PEM desde el que se especifica el certificado incluye toda la cadena de claves públicas. El nombre alternativo del sujeto (SAN) del certificado está presente; es decir, el valor del campo `subjectAltName` es válido. El certificado cumple con los requisitos efectivos que los navegadores imponen a los certificados de servidor, así como con los requisitos básicos actuales del CA/Browser Forum.	
Certificado de Kaspersky Security Center Web Console	El contenedor PEM desde el que se especifica el certificado incluye la cadena completa de claves públicas. El nombre alternativo del sujeto (SAN) del certificado está presente; es decir, el valor del campo `subjectAltName` es válido. El certificado cumple con los requisitos efectivos que los navegadores imponen a los certificados de servidor, así como con los requisitos básicos actuales del CA/Browser Forum.	Los certificados cifrados no son compatibles con Kaspersky Security Center Web Console.

Escenario: especificación del certificado del Servidor de administración personalizado

Puede asignar el certificado del Servidor de administración personalizado, por ejemplo, para una mejor integración con la infraestructura de clave pública (PKI) existente de su empresa o para la configuración personalizada de los campos del certificado. Es útil reemplazar el certificado inmediatamente después de la instalación del Servidor de administración y antes de que el Asistente de inicio rápido se complete.

Si especifica un período de validez superior a 397 días para el certificado del Servidor de administración, el navegador devuelve un error.

Requisitos previos

El nuevo certificado debe crearse en el formato PKCS#12 (por ejemplo, mediante la PKI de la organización) y debe ser emitido por una autoridad de certificación (CA) de confianza. Además, el nuevo certificado debe incluir toda la cadena de confianza y una clave privada, que debe almacenarse en el archivo con la extensión pfx o p12. Para el nuevo certificado, se deben cumplir los requisitos enumerados en la siguiente tabla.

Requisitos para los certificados del Servidor de administración

Tipo de certificado	Requisitos
Certificado común, certificado de reserva común ("C", "CR")	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto

	• Restricción de longitud de ruta: Ninguna El valor de la restricción de longitud de ruta puede ser un número entero diferente de “Ninguna”, pero no menos de 1. Uso de la clave: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Uso extendido de claves (EKU): autenticación de servidor y autenticación de cliente. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del servidor y del cliente deben especificarse en el EKU.
Certificado móvil, certificado de reserva móvil (“M”, “MR”)	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto • Restricción de longitud de ruta: Ninguna El valor de restricción de longitud de ruta puede ser un número entero diferente de “Ninguna” si el certificado común tiene un valor de restricción de longitud de ruta no menor que “1”. Uso de la clave: • Firma digital • Firma de certificados • Cifrado de claves • Firma de CRL Extended Key Usage (EKU): autenticación de servidor. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del servidor deben especificarse en el EKU.
CA de certificado para certificados de usuario generados automáticamente ("MCA")	Longitud mínima de la clave: 2048. Restricciones básicas: • CA: cierto • Restricción de longitud de ruta: Ninguna El valor de restricción de longitud de ruta puede ser un número entero diferente de “Ninguna” si el certificado común tiene un valor de restricción de longitud de ruta no menor que “1”. Uso de la clave: • Firma digital • Firma de certificados

	• Cifrado de claves • Firma de CRL Extended Key Usage (EKU): autenticación del cliente. El EKU es opcional, pero si su certificado lo contiene, los datos de autenticación del cliente deben especificarse en el EKU.

Los certificados emitidos por una CA pública no tienen el permiso de firma de certificados. Para utilizar dichos certificados, asegúrese de haber instalado la versión 13, o una posterior, del Agente de red en los puntos de distribución o las puertas de enlace de conexión de su red. De lo contrario, no podrá utilizar certificados sin el permiso de firma.

Etapas

La especificación del certificado del Servidor de administración se realiza por etapas:

1. **Sustitución del certificado del Servidor de administración**

   Para ello, use la línea de comandos utilidad klsetsrvcert.

2. **Especificación de un nuevo certificado y restauración de la conexión de los Agentes de red con el Servidor de administración**

   Al reemplazar el certificado, todos los Agentes de red que estaban conectados anteriormente al Servidor de administración a través de SSL pierden su conexión y devuelven el "error de autenticación del Servidor de administración". Para especificar el nuevo certificado y restaurar la conexión, use la línea de comandos utilidad klmover.

Resultados

Cuando termina el escenario, el certificado del Servidor de administración se reemplaza y el servidor es autenticado por los Agentes de red en los dispositivos administrados.

Reemplazo del certificado del Servidor de administración mediante la utilidad klsetsrvcert

Para reemplazar el certificado del Servidor de administración:

Desde la línea de comandos, ejecute la siguiente utilidad:

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

No necesita descargar la utilidad klsetsrvcert. Está incluida en el kit de distribución de Kaspersky Security Center. No es compatible con versiones anteriores de Kaspersky Security Center.

La descripción de los parámetros de la utilidad klsetsrvcert se presenta en la siguiente tabla.

Valores de los parámetros de la utilidad klsetsrvcert

Parámetro	Valor
`-t <type>`	Tipo de certificado para reemplazar. Posibles valores del parámetro `<type>`: • `C`: Reemplace el certificado para los puertos 13000 y 13291. • `CR`: Reemplace el certificado de reserva común para los puertos 13000 y 13291. • `M`: Reemplace el certificado para dispositivos móviles en el puerto 13292. • `MR`: Reemplace el certificado de reserva para dispositivos móviles para el puerto 13292. • `MCA`: CA de cliente móvil para certificados de usuario autogenerados.
`-f <time>`	Programación de cambio del certificado, en formato "DD-MM-AAAA hh:mm" (para los puertos 13000 y 13291). Utilice este parámetro si desea reemplazar el certificado común o de reserva común antes de que caduque. Especifique la hora en que los dispositivos administrados deben sincronizarse con el Servidor de administración en un nuevo certificado.
`-i <inputfile>`	Contenedor con el certificado y una clave privada con formato PKCS#12 (archivo con la extensión .p12 o .pfx).
`-p <password>`	Contraseña usada para la protección del contenedor p12. El certificado y una clave privada se almacenan en el contenedor, por lo tanto, se requiere la contraseña para descifrar el archivo con el contenedor.
`-o <chkopt>`	Parámetros de validación del certificado (separados por punto y coma). Para usar un certificado personalizado sin permiso de firma, especifique `-o NoCA` en la utilidad klsetsrvcert. Esto es útil para los certificados emitidos por una CA pública.
`-g <dnsname>`	Un nuevo certificado se creará para el nombre de DNS especificado.
`-r <calistfile>`	Lista de autoridades de certificación raíz de confianza, formato PEM.
`-l <logfile>`	Archivo de salida de resultados. De forma predeterminada, la salida se redirige al flujo de salida estándar.

Por ejemplo, para especificar el certificado del Servidor de administración personalizado, use el siguiente comando:

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

Después de reemplazar el certificado, todos los Agentes de red conectados al Servidor de administración a través de SSL pierden su conexión. Para restaurarlo, use la línea de comandos utilidad klmover.

Conexión de los Agentes de red al Servidor de administración mediante la utilidad klmover

Después de reemplazar el certificado del Servidor de administración mediante la línea de comandos utilidad klsetsrvcert, debe establecer la conexión SSL entre los Agentes de red y el Servidor de administración porque la conexión está interrumpida.

Para especificar el nuevo certificado del Servidor de administración y restaurar la conexión, haga lo siguiente:

Desde la línea de comandos, ejecute la siguiente utilidad:

```
klmover [-address <dirección del servidor>] [-pn <número de puerto>] [-ps <número de puerto SSL>] [-nossl] [-cert <ruta al archivo de certificado>]
```

Esta utilidad se copia automáticamente en la carpeta de instalación del Agente de red, cuando el Agente de red está instalado en un dispositivo cliente.

La descripción de los parámetros de la utilidad klmover se presenta en la siguiente tabla.

Valores de los parámetros de la utilidad klmover

Parámetro	Valor
`-address <dirección del servidor>`	Dirección del Servidor de administración para la conexión. Puede especificar una dirección IP, el nombre NetBIOS o el nombre DNS.
`-pn <número de puerto>`	Número del puerto por el que se establecerá la conexión no cifrada al Servidor de administración. El número de puerto predeterminado es el 14000.
`-ps <número de puerto SSL>`	Número del puerto SSL por el que se establecerá la conexión cifrada al Servidor de administración, con protocolo SSL. El número de puerto predeterminado es el 13000.
`-nossl`	Usar conexión no cifrada al Servidor de administración. Si la clave no está en uso, el Agente de red se conecta al Servidor de administración mediante el protocolo cifrado SSL.
`-cert <ruta al archivo de certificado>`	Utilizar el archivo de certificado especificado para la autenticación del acceso al Servidor de administración.

Volver a emitir el certificado de servidor web

El certificado de Servidor web que se utiliza en Kaspersky Security Center es necesario para publicar paquetes de instalación del Agente de red que posteriormente descarga en dispositivos administrados, así como para publicar perfiles de MDM de iOS, aplicaciones de iOS y paquetes de instalación de Kaspersky Endpoint Security for Mobile. Dependiendo de la configuración actual de la aplicación, pueden funcionar varios certificados como certificado de servidor web (para obtener más detalles, consulte Acerca de los certificados de Kaspersky Security Center).

Es posible que deba volver a emitir el certificado de Servidor web para cumplir con los requisitos de seguridad específicos de su organización o para mantener la conexión continua de sus dispositivos administrados antes de comenzar a actualizar la aplicación. Kaspersky Security Center ofrece dos formas de volver a emitir el certificado de Servidor web; la elección entre los dos métodos depende de si tiene dispositivos móviles conectados y administrados a través del protocolo móvil (es decir, mediante el uso del certificado móvil).

Si nunca ha especificado su propio certificado personalizado como certificado del Servidor web en la sección **Servidor web** de la ventana de propiedades del Servidor de administración, el certificado móvil actúa como el certificado del Servidor web. En este caso, la reemisión del certificado del Servidor web se realiza mediante la reemisión del propio protocolo móvil.

Para volver a emitir el certificado de Servidor web cuando no tiene dispositivos móviles administrados a través del protocolo móvil:

1. En el árbol de la consola, haga clic con el botón derecho en el nombre del Servidor de administración correspondiente y, en el menú contextual, seleccione **Propiedades**.

2. En la ventana de propiedades del Servidor de administración que se abre, en el panel izquierdo seleccione la sección **Configuración de la conexión del Servidor de administración**.

3. En la lista de subsecciones, seleccione la subsección **Certificados**.

4. Si planea continuar usando el certificado emitido por Kaspersky Security Center, haga lo siguiente:

   a. En el panel derecho, en el grupo de configuraciones de **Autenticación del Servidor de administración por dispositivos móviles**, seleccione la opción **Certificado emitido a través del Servidor de administración** y haga clic en el botón **Reemitir**.

   b. En la ventana **Volver a emitir certificado** que se abre, en el grupo de configuraciones **Dirección de conexión** y **Plazo de activación** seleccione las opciones relevantes y haga clic en **Aceptar**.

   c. En la ventana de confirmación, haga clic en **Sí**.

   Alternativamente, si planea usar su propio certificado personalizado, haga lo siguiente:

   a. Compruebe si su certificado personalizado cumple los requisitos de Kaspersky Security Center y los requisitos de certificados de confianza de Apple. Si es necesario, modifique el certificado.

   b. Seleccione la opción **Otro certificado**, y haga clic en el botón **Examinar**.

   c. En la ventana **Certificado** que se abre, en el campo **Tipo de certificado** seleccione el tipo de su certificado y luego especifique la ubicación y la configuración del certificado:

      - Si ha seleccionado **Contenedor PKCS #12**, haga clic en el botón **Examinar** al lado del campo **Archivo de certificado** y especifique el archivo de certificado en su disco duro. Si el archivo de certificado está protegido con contraseña, ingrese la contraseña en el campo **Contraseña (si es aplicable)**.

      - Si ha seleccionado **Certificado X.509**, haga clic en el botón **Examinar** al lado del campo **Clave privada (.prk, .pem)** y especifique la clave privada en su disco duro. Si la clave privada está protegida con contraseña, ingrese la contraseña en el campo **Contraseña (si es aplicable)**. Luego haga clic en el botón **Examinar** al lado del campo **Clave pública (.cer)** y especifique la clave privada en su disco duro.

   d. En la ventana **Certificado**, haga clic en **Aceptar**.

   e. En la ventana de confirmación, haga clic en **Sí**.

   El certificado móvil se vuelve a emitir para utilizarlo como certificado de Servidor web.

Para volver a emitir el certificado de Servidor web cuando tiene dispositivos móviles administrados a través del protocolo móvil:

1. Genere su certificado personalizado y prepárelo para usarse en Kaspersky Security Center. Compruebe si su certificado personalizado cumple los requisitos de Kaspersky Security Center y los requisitos de certificados de confianza de Apple. Si es necesario, modifique el certificado.

   Puede utilizar la utilidad kliossrvcertgen.exe para la generación de certificados.

2. En el árbol de la consola, haga clic con el botón derecho en el nombre del Servidor de administración correspondiente y, en el menú contextual, seleccione **Propiedades**.

3. En la ventana de propiedades del Servidor de administración que se abre, en el panel izquierdo seleccione la sección **Servidor web**.

4. En el menú **A través de HTTPS**, seleccione la opción **Especificar otro certificado**.

5. En el menú **A través de HTTPS**, haga clic en el botón **Modificar**.

6. En la ventana emergente **Certificado**, en el campo **Tipo de certificado** seleccione el tipo de su certificado:

   - Si ha seleccionado **Contenedor PKCS #12**, haga clic en el botón **Examinar** al lado del campo **Archivo de certificado** y especifique el archivo de certificado en su disco duro. Si el archivo de certificado está protegido con contraseña, ingrese la contraseña en el campo **Contraseña (si es aplicable)**.

   - Si ha seleccionado **Certificado X.509**, haga clic en el botón **Examinar** al lado del campo **Clave privada (.prk, .pem)** y especifique la clave privada en su disco duro. Si la clave privada está protegida con contraseña, ingrese la contraseña en el campo **Contraseña (si es aplicable)**. Luego haga clic en el botón **Examinar** al lado del campo **Clave pública (.cer)** y especifique la clave privada en su disco duro.

7. En la ventana **Certificado**, haga clic en **Aceptar**.

8. Si es necesario, en la ventana de propiedades del Servidor de administración, en el campo **Puerto HTTPS del servidor web** cambie el número del puerto HTTPS para Servidor web. Haga clic en **Aceptar**.

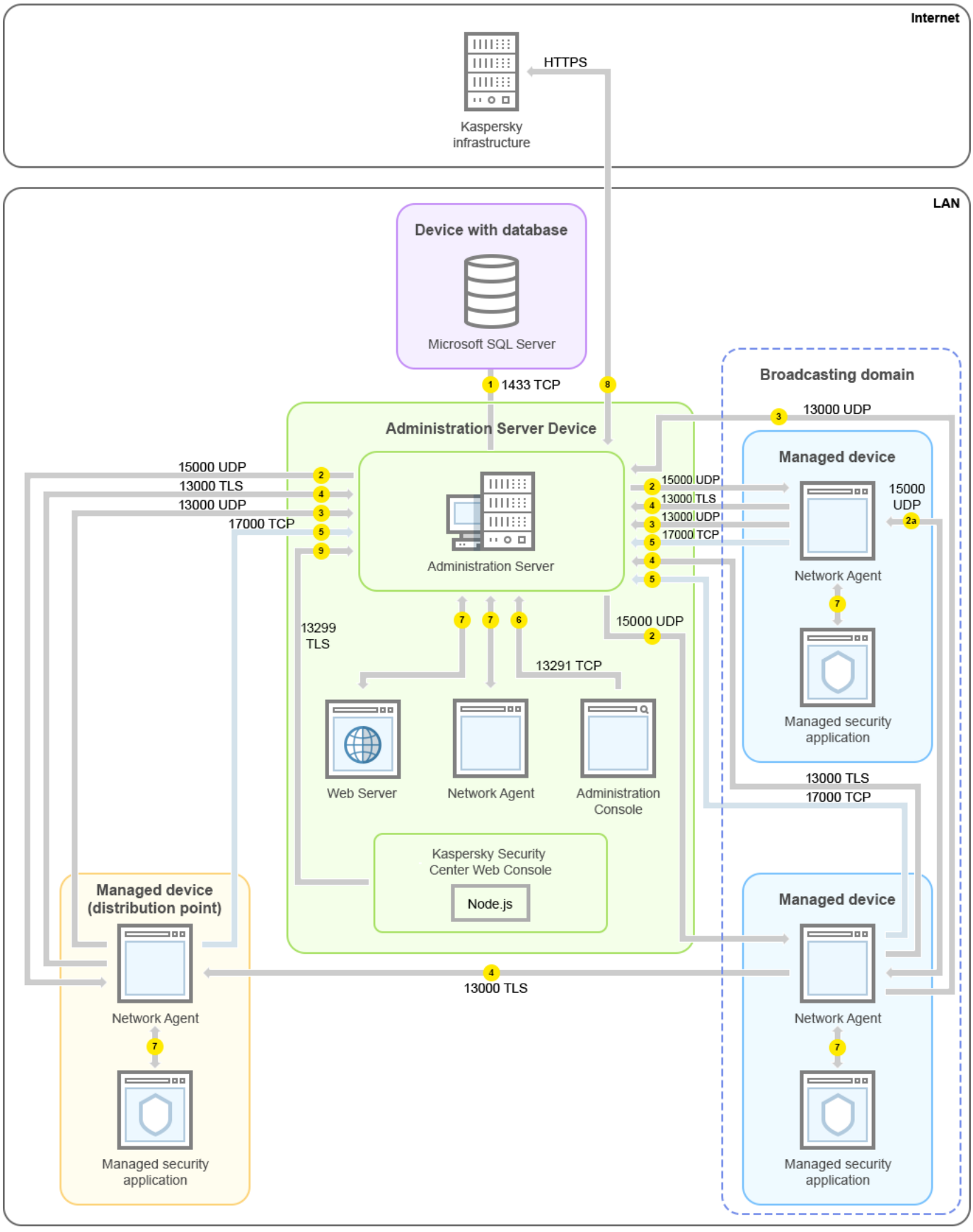
   Se volverá a emitir el certificado del Servidor web.

Esquemas para tráfico de datos y uso de puertos

Esta sección proporciona esquemas para el tráfico de datos entre los componentes de Kaspersky Security Center, las aplicaciones de seguridad administradas y los servidores externos de varias configuraciones. Los esquemas se proporcionan con los números para los puertos que deben estar disponibles en los dispositivos locales.

Servidor de administración y dispositivos administrados en LAN

La siguiente figura muestra el tráfico de datos si Kaspersky Security Center se despliega solo en la red de área local (LAN).



Servidor de administración y dispositivos administrados en una red de área local (LAN)

La figura muestra cómo los diferentes dispositivos administrados se conectan al Servidor de administración de diferentes maneras: directamente o a través de un punto de distribución. Los puntos de distribución reducen la carga en el Servidor de administración durante la distribución de actualizaciones y optimizan el tráfico de red. Sin embargo, los puntos de distribución solo son necesarios si el número de dispositivos administrados es lo suficientemente grande. Si el número de dispositivos administrados es pequeño, todos los dispositivos administrados pueden recibir actualizaciones del Servidor de administración directamente.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. Se proporcionan el número del puerto y el nombre del protocolo utilizado para la transferencia de datos. Cada flecha tiene una etiqueta de número y los detalles sobre el tráfico de datos correspondiente son los siguientes:

1. El Servidor de administración envía datos a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL-Server y el servidor MariaDB, o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Las solicitudes de comunicación provenientes del Servidor de administración se transfieren a todos los dispositivos administrados no móviles a través del puerto UDP 15000.

   Los Agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

3. La información sobre el apagado de los dispositivos administrados se transfiere desde el Agente de red al Servidor de administración a través del puerto UDP 13000.

4. El Servidor de administración recibe conexiones de los Agentes de red y de los Servidores de administración secundarios a través del puerto SSL 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir una conexión de Agentes de red a través del puerto no SSL 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.

   > El punto de distribución se llamaba "Agente de actualización" en versiones anteriores de Kaspersky Security Center.

5. Los dispositivos administrados (excepto dispositivos móviles) solicitan la activación a través del puerto TCP 17000. Esto no es necesario si el dispositivo tiene su propio acceso a Internet; en este caso, el dispositivo envía los datos directamente a los servidores de Kaspersky en Internet.

6. La Consola de administración basada en MMC transfiere datos al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en un dispositivo diferente).

7. Las aplicaciones en un solo dispositivo intercambian tráfico local (ya sea en el Servidor de administración o en un dispositivo administrado). Los puertos externos no tienen que abrirse.

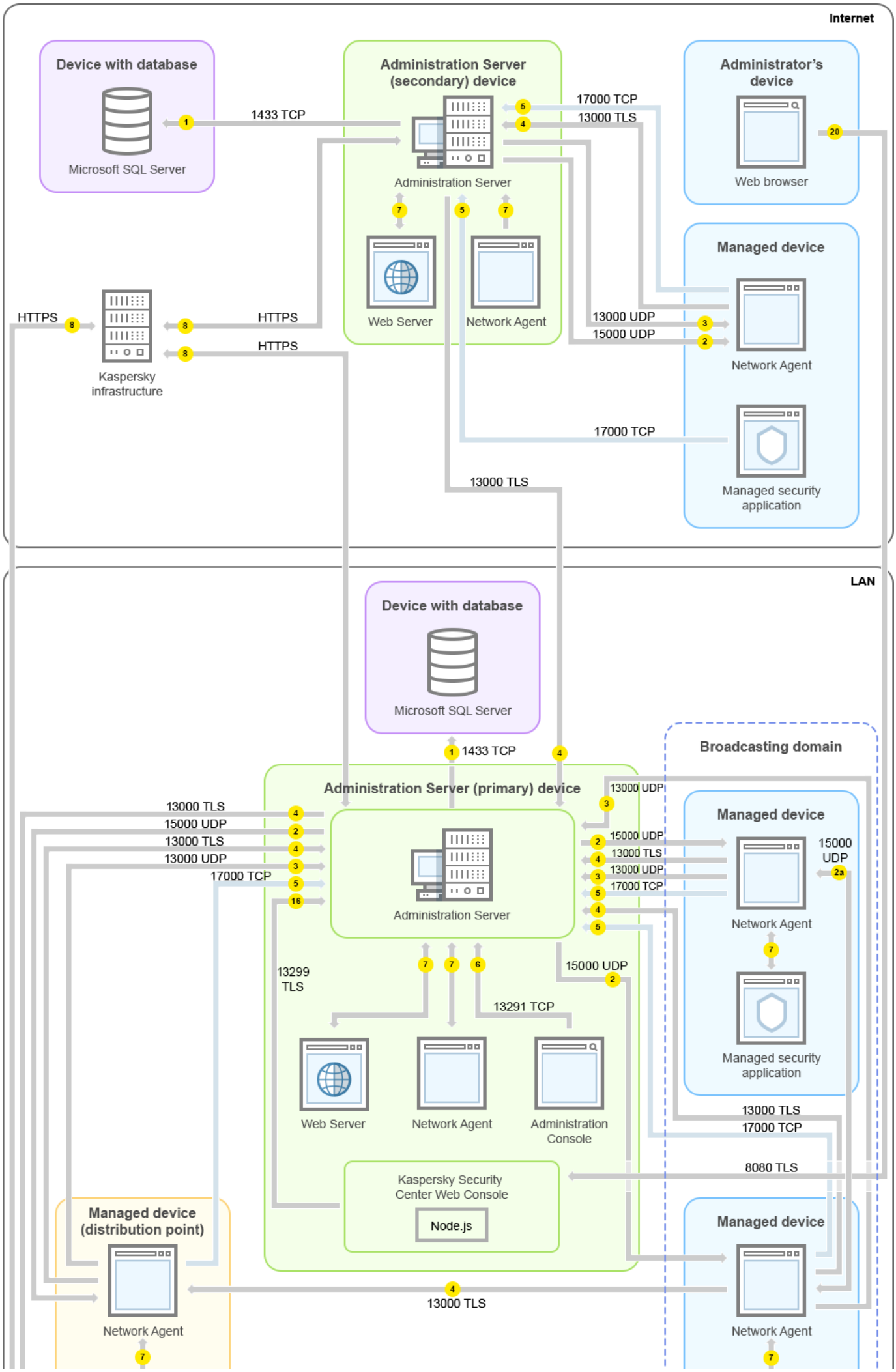
8. Los datos enviados del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos enviados de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

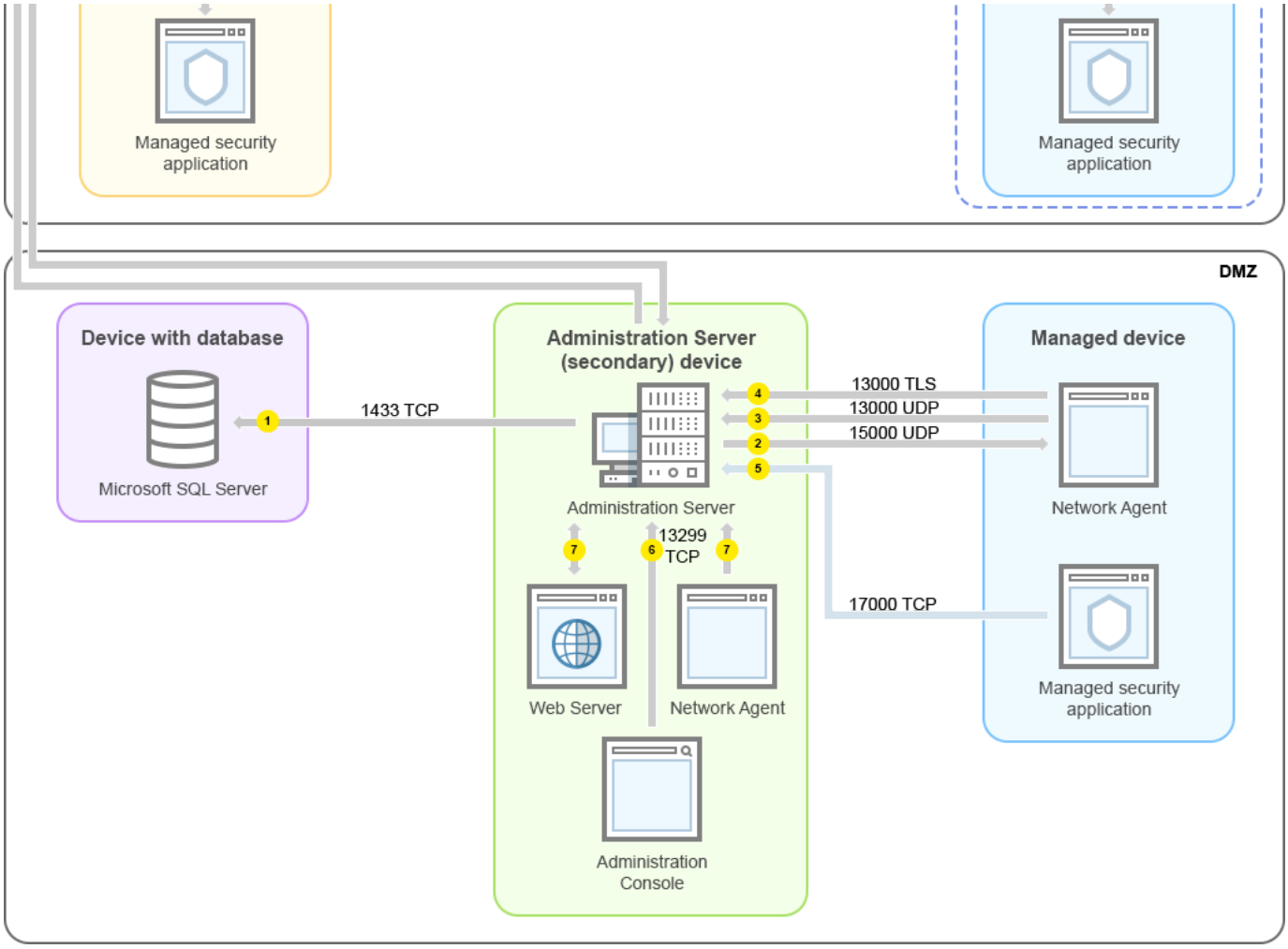
   Si no desea que su Servidor de administración tenga acceso a Internet, debe administrar estos datos de forma manual.

9. Servidor de Kaspersky Security Center Web Console envía datos al Servidor de administración, que puede estar instalado en el mismo dispositivo o en un dispositivo diferente, a través del puerto 13299 TLS.

Servidor de administración principal en LAN y dos Servidores de administración secundarios

La siguiente figura muestra la jerarquía de los Servidores de administración: el Servidor de administración principal está en una red de área local (LAN). Un Servidor de administración secundario está en la zona desmilitarizada (DMZ); otro Servidor de administración secundario está en Internet.


Internet
Device with database
Microsoft SQL Server
1433 TCP
Administration Server (secondary) device
Administration Server
Web Server
Network Agent
17000 TCP
13000 TLS
Administrator's device
Web browser
Managed device
Network Agent
13000 UDP
15000 UDP
17000 TCP
Managed security application
13000 TLS
HTTPS
Kaspersky infrastructure
LAN
Device with database
Microsoft SQL Server
1433 TCP
Broadcasting domain
Administration Server (primary) device
Administration Server
13000 TLS
15000 UDP
13000 TLS
13000 UDP
17000 TCP
13000 UDP
15000 UDP
13000 TLS
13000 UDP
17000 TCP
Managed device
Network Agent
15000 UDP
Managed security application
13299 TLS
15000 UDP
13291 TCP
Web Server
Network Agent
Administration Console
13000 TLS
17000 TCP
8080 TLS
Kaspersky Security Center Web Console
Node.js
Managed device (distribution point)
Network Agent
13000 TLS
Managed device
Network Agent



Jerarquía de Servidores de administración: Servidor de administración principal y dos Servidores de administración secundarios

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. Se proporcionan el número del puerto y el nombre del protocolo utilizado para la transferencia de datos. Cada flecha tiene una etiqueta de número y los detalles sobre el tráfico de datos correspondiente son los siguientes:

1. El Servidor de administración envía datos a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL-Server y el servidor MariaDB, o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Las solicitudes de comunicación provenientes del Servidor de administración se transfieren a todos los dispositivos administrados no móviles a través del puerto UDP 15000.

   Los Agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

3. La información sobre el apagado de los dispositivos administrados se transfiere desde el Agente de red al Servidor de administración a través del puerto UDP 13000.

4. El Servidor de administración recibe conexiones de los Agentes de red y de los Servidores de administración secundarios a través del puerto SSL 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir una conexión de Agentes de red a través del puerto no SSL 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.

El punto de distribución se llamaba "Agente de actualización" en versiones anteriores de Kaspersky Security Center.

5. Los dispositivos administrados (excepto dispositivos móviles) solicitan la activación a través del puerto TCP 17000. Esto no es necesario si el dispositivo tiene su propio acceso a Internet; en este caso, el dispositivo envía los datos directamente a los servidores de Kaspersky en Internet.

6. La Consola de administración basada en MMC transfiere datos al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en un dispositivo diferente).

7. Las aplicaciones en un solo dispositivo intercambian tráfico local (ya sea en el Servidor de administración o en un dispositivo administrado). Los puertos externos no tienen que abrirse.

8. Los datos enviados del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos enviados de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

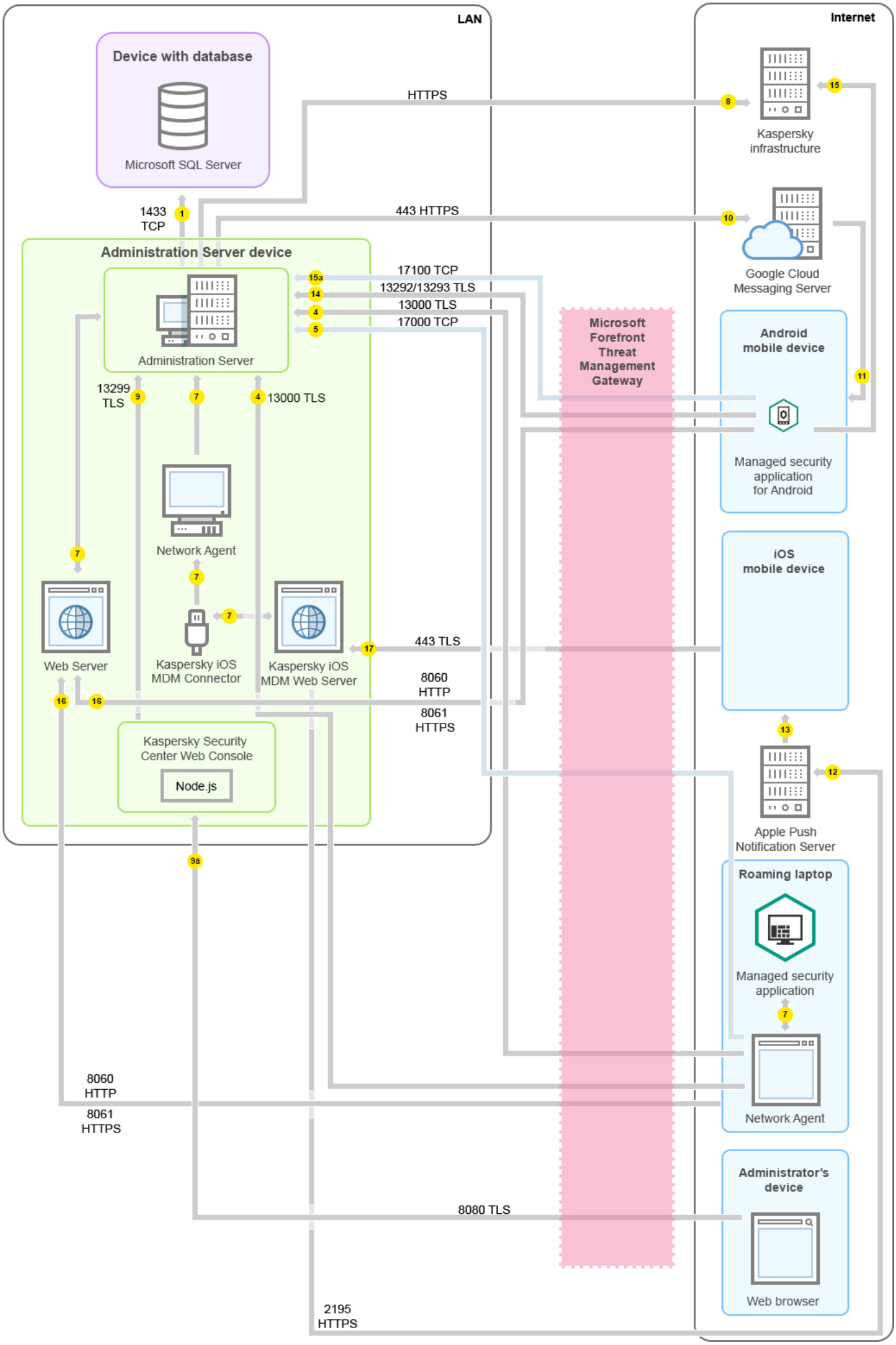
   Si no desea que su Servidor de administración tenga acceso a Internet, debe administrar estos datos de forma manual.

9. Servidor de Kaspersky Security Center 14 Web Console envía datos al Servidor de administración, que puede estar instalado en el mismo dispositivo o en un dispositivo diferente, a través del puerto 13299 TLS.

   9a. Los datos del navegador, que se instalan en un dispositivo separado del administrador, se transfieren al Servidor de Kaspersky Security Center 14 Web Console a través del puerto TLS 8080. Kaspersky Security Center 14 Web Console se puede instalar en el Servidor de administración o en otro dispositivo.

Servidor de administración en LAN, dispositivos administrados en internet; TMG está en uso

La siguiente figura muestra el tráfico de datos si el Servidor de administración está en una red de área local (LAN), y los dispositivos administrados, incluidos los dispositivos móviles, están en Internet. En esta figura, *Microsoft Forefront Threat Management Gateway* (TMG) está en uso. Sin embargo, si desea utilizar un firewall corporativo puede usar una aplicación diferente; consulte la documentación de la aplicación de su elección para más detalles.


LAN
Internet
Device with database
Microsoft SQL Server
HTTPS
Kaspersky infrastructure
1433 TCP
443 HTTPS
Google Cloud Messaging Server
Administration Server device
17100 TCP
13292/13293 TLS
13000 TLS
17000 TCP
Administration Server
Microsoft Forefront Threat Management Gateway
Android mobile device
13299 TLS
13000 TLS
Managed security application for Android
Network Agent
iOS mobile device
Web Server
Kaspersky iOS MDM Connector
Kaspersky iOS MDM Web Server
443 TLS
8060 HTTP
8061 HTTPS
Kaspersky Security Center Web Console
Node.js
Apple Push Notification Server
Roaming laptop
Managed security application
8060 HTTP
8061 HTTPS
Network Agent
Administrator's device
8080 TLS
Web browser
2195 HTTPS

Se recomienda este esquema de despliegue si no desea que los dispositivos móviles se conecten directamente al Servidor de administración y no desea asignar una puerta de enlace de conexión en la DMZ.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. Se proporcionan el número del puerto y el nombre del protocolo utilizado para la transferencia de datos. Cada flecha tiene una etiqueta de número y los detalles sobre el tráfico de datos correspondiente son los siguientes:

1. El Servidor de administración envía datos a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL-Server y el servidor MariaDB, o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Las solicitudes de comunicación provenientes del Servidor de administración se transfieren a todos los dispositivos administrados no móviles a través del puerto UDP 15000.

   Los Agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

3. La información sobre el apagado de los dispositivos administrados se transfiere desde el Agente de red al Servidor de administración a través del puerto UDP 13000.

4. El Servidor de administración recibe conexiones de los Agentes de red y de los Servidores de administración secundarios a través del puerto SSL 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir una conexión de Agentes de red a través del puerto no SSL 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.

   > El punto de distribución se llamaba "Agente de actualización" en versiones anteriores de Kaspersky Security Center.

5. Los dispositivos administrados (excepto dispositivos móviles) solicitan la activación a través del puerto TCP 17000. Esto no es necesario si el dispositivo tiene su propio acceso a Internet; en este caso, el dispositivo envía los datos directamente a los servidores de Kaspersky en Internet.

6. La Consola de administración basada en MMC transfiere datos al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en un dispositivo diferente).

7. Las aplicaciones en un solo dispositivo intercambian tráfico local (ya sea en el Servidor de administración o en un dispositivo administrado). Los puertos externos no tienen que abrirse.

8. Los datos enviados del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos enviados de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no desea que su Servidor de administración tenga acceso a Internet, debe administrar estos datos de forma manual.

9. Servidor de Kaspersky Security Center 14 Web Console envía datos al Servidor de administración, que puede estar instalado en el mismo dispositivo o en un dispositivo diferente, a través del puerto 13299 TLS.

9a. Los datos del navegador, que se instalan en un dispositivo separado del administrador, se transfieren al Servidor de Kaspersky Security Center 14 Web Console a través del puerto TLS 8080. Kaspersky Security Center 14 Web Console se puede instalar en el Servidor de administración o en otro dispositivo.

10. Solo para dispositivos móviles Android: los datos del Servidor de administración se transfieren a los servidores de Google. Esta conexión se utiliza para notificar a los dispositivos móviles de Android de que se tienen que conectar al Servidor de administración. Luego se envían notificaciones push a los dispositivos móviles.

11. Solo para dispositivos móviles Android: notificaciones push desde los servidores de Google se envían al dispositivo móvil. Esta conexión se utiliza para notificar a los dispositivos móviles de que se tienen que conectar al Servidor de administración.

12. Solo para dispositivos móviles iOS: los datos del Servidor de MDM para iOS se transfieren a los servidores de Apple Push Notification. Luego se envían notificaciones push a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. Esta conexión se utiliza para notificar a los dispositivos móviles iOS de que se tienen que conectar al Servidor de administración.

14. Solo para dispositivos móviles: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través del puerto 13292/13293 TLS, directamente o a través de un Microsoft Forefront Threat Management Gateway (TMG).

15. Solo para dispositivos móviles: los datos del dispositivo móvil se transfieren a la infraestructura de Kaspersky.

    15a. Si un dispositivo móvil no tiene acceso a Internet, los datos se transfieren al Servidor de administración a través del puerto 17100, y el Servidor de administración los envía a la infraestructura de Kaspersky; sin embargo, este escenario se aplica muy raramente.

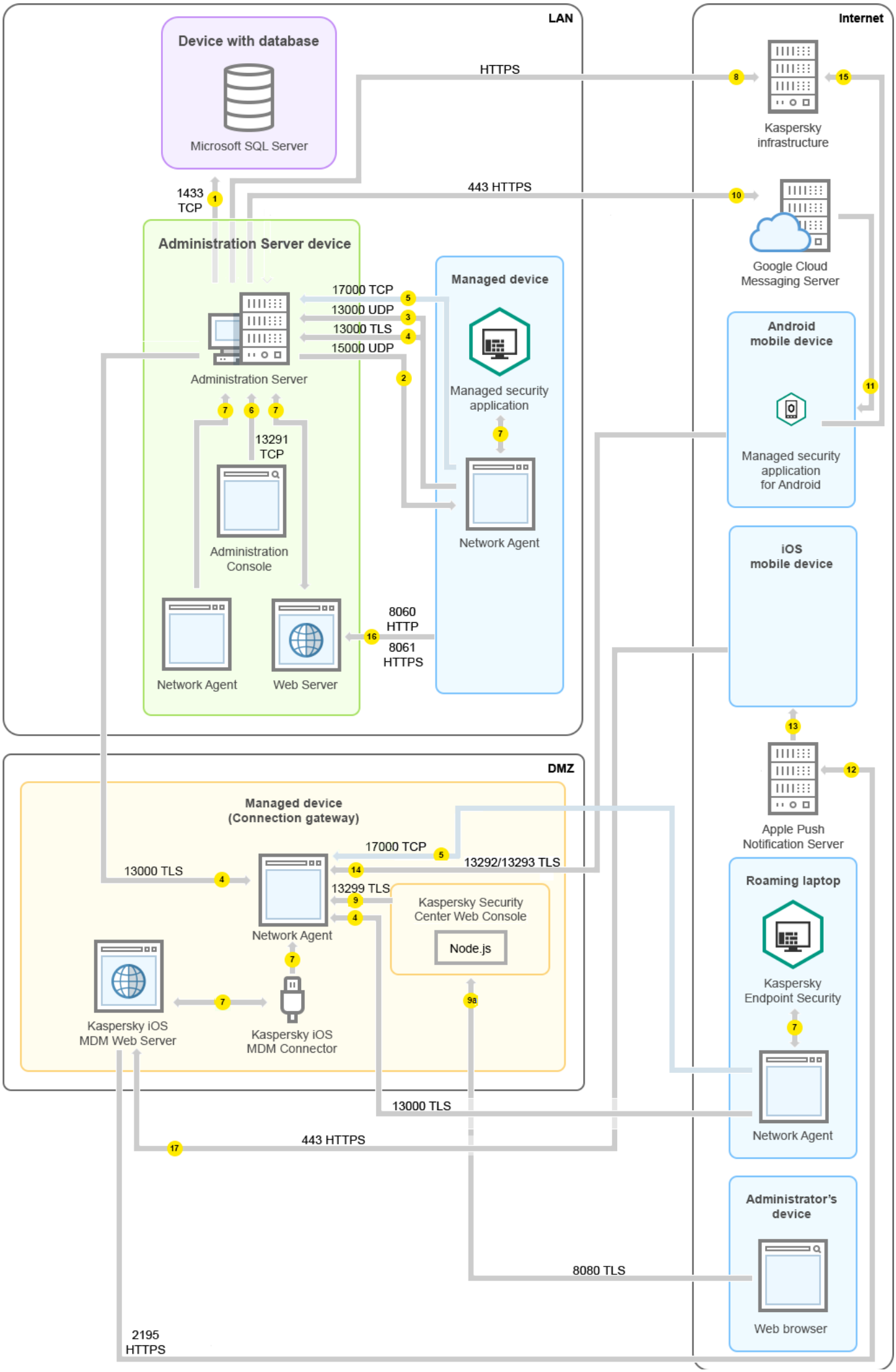
16. Las solicitudes de paquetes de dispositivos administrados, incluidos los dispositivos móviles, se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

17. Solo para dispositivos móviles iOS: los datos del dispositivo móvil se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

Servidor de administración en LAN, dispositivos administrados en internet; la puerta de enlace de conexión está en uso

La siguiente figura muestra el tráfico de datos si el Servidor de administración está en una red de área local (LAN) y los dispositivos administrados, incluidos los dispositivos móviles, están en Internet. Una puerta de enlace de conexión está en uso.

Se recomienda este esquema de despliegue si no desea que los dispositivos móviles se conecten directamente al Servidor de administración y no desee usar un Microsoft Forefront Threat Management Gateway (TMG) o un firewall corporativo.


LAN
Internet
Device with database
Microsoft SQL Server
HTTPS
Kaspersky infrastructure
1433 TCP
443 HTTPS
Google Cloud Messaging Server
Administration Server device
Managed device
17000 TCP
13000 UDP
13000 TLS
15000 UDP
Administration Server
Managed security application
Android mobile device
Managed security application for Android
13291 TCP
Administration Console
Network Agent
iOS mobile device
8060 HTTP
8061 HTTPS
Network Agent
Web Server
DMZ
Managed device (Connection gateway)
17000 TCP
13292/13293 TLS
13000 TLS
13299 TLS
Kaspersky Security Center Web Console
Node.js
Network Agent
Apple Push Notification Server
Roaming laptop
Kaspersky Endpoint Security
Kaspersky iOS MDM Web Server
Kaspersky iOS MDM Connector
13000 TLS
Network Agent
443 HTTPS
Administrator's device
8080 TLS
Web browser
2195 HTTPS

En esta figura, los dispositivos administrados están conectados al Servidor de administración a través de una puerta de enlace de conexión que se encuentra en DMZ. Ningún TMG o firewall corporativo está en uso.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. Se proporcionan el número del puerto y el nombre del protocolo utilizado para la transferencia de datos. Cada flecha tiene una etiqueta de número y los detalles sobre el tráfico de datos correspondiente son los siguientes:

1. El Servidor de administración envía datos a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL-Server y el servidor MariaDB, o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Las solicitudes de comunicación provenientes del Servidor de administración se transfieren a todos los dispositivos administrados no móviles a través del puerto UDP 15000.

   Los Agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

3. La información sobre el apagado de los dispositivos administrados se transfiere desde el Agente de red al Servidor de administración a través del puerto UDP 13000.

4. El Servidor de administración recibe conexiones de los Agentes de red y de los Servidores de administración secundarios a través del puerto SSL 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir una conexión de Agentes de red a través del puerto no SSL 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.

   > El punto de distribución se llamaba "Agente de actualización" en versiones anteriores de Kaspersky Security Center.

5. Los dispositivos administrados (excepto dispositivos móviles) solicitan la activación a través del puerto TCP 17000. Esto no es necesario si el dispositivo tiene su propio acceso a Internet; en este caso, el dispositivo envía los datos directamente a los servidores de Kaspersky en Internet.

6. La Consola de administración basada en MMC transfiere datos al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en un dispositivo diferente).

7. Las aplicaciones en un solo dispositivo intercambian tráfico local (ya sea en el Servidor de administración o en un dispositivo administrado). Los puertos externos no tienen que abrirse.

8. Los datos enviados del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos enviados de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no desea que su Servidor de administración tenga acceso a Internet, debe administrar estos datos de forma manual.

9. Servidor de Kaspersky Security Center 14 Web Console envía datos al Servidor de administración, que puede estar instalado en el mismo dispositivo o en un dispositivo diferente, a través del puerto 13299 TLS.

9a. Los datos del navegador, que se instalan en un dispositivo separado del administrador, se transfieren al Servidor de Kaspersky Security Center 14 Web Console a través del puerto TLS 8080. Kaspersky Security Center 14 Web Console se puede instalar en el Servidor de administración o en otro dispositivo.

10. Solo para dispositivos móviles Android: los datos del Servidor de administración se transfieren a los servidores de Google. Esta conexión se utiliza para notificar a los dispositivos móviles de Android de que se tienen que conectar al Servidor de administración. Luego se envían notificaciones push a los dispositivos móviles.

11. Solo para dispositivos móviles Android: notificaciones push desde los servidores de Google se envían al dispositivo móvil. Esta conexión se utiliza para notificar a los dispositivos móviles de que se tienen que conectar al Servidor de administración.

12. Solo para dispositivos móviles iOS: los datos del Servidor de MDM para iOS se transfieren a los servidores de Apple Push Notification. Luego se envían notificaciones push a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. Esta conexión se utiliza para notificar a los dispositivos móviles iOS de que se tienen que conectar al Servidor de administración.

14. Solo para dispositivos móviles: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través del puerto 13292/13293 TLS, directamente o a través de un Microsoft Forefront Threat Management Gateway (TMG).

15. Solo para dispositivos móviles: los datos del dispositivo móvil se transfieren a la infraestructura de Kaspersky.

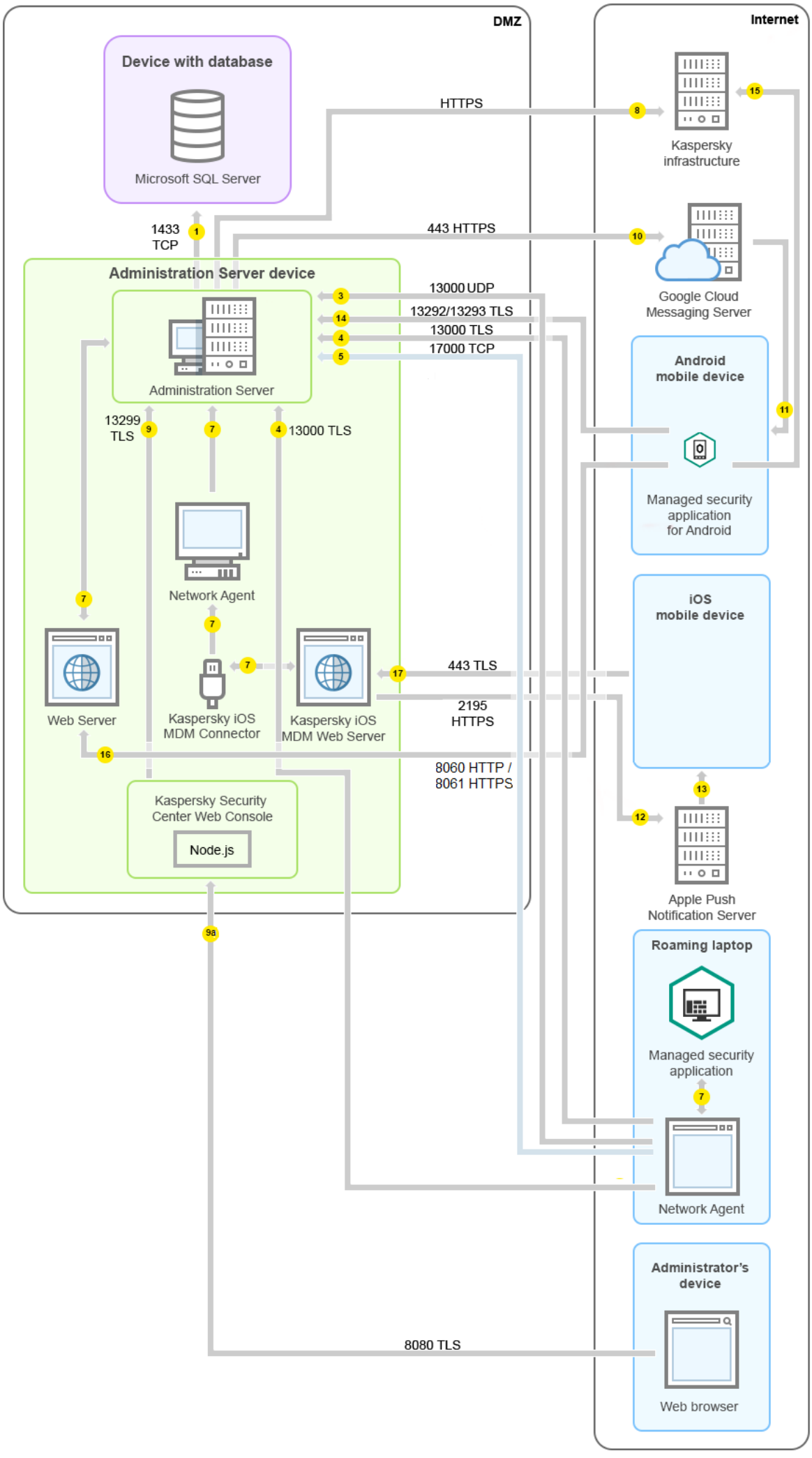
    15a. Si un dispositivo móvil no tiene acceso a Internet, los datos se transfieren al Servidor de administración a través del puerto 17100, y el Servidor de administración los envía a la infraestructura de Kaspersky; sin embargo, este escenario se aplica muy raramente.

16. Las solicitudes de paquetes de dispositivos administrados, incluidos los dispositivos móviles, se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

17. Solo para dispositivos móviles iOS: los datos del dispositivo móvil se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

Servidor de administración en DMZ, dispositivos administrados en Internet

La siguiente figura muestra el tráfico de datos si el Servidor de administración está en la zona desmilitarizada (DMZ) y los dispositivos administrados, incluidos los dispositivos móviles, están en Internet.


DMZ
Internet
Device with database
Microsoft SQL Server
HTTPS
Kaspersky infrastructure
1433 TCP
443 HTTPS
Google Cloud Messaging Server
Administration Server device
13000 UDP
13292/13293 TLS
13000 TLS
17000 TCP
Administration Server
Android mobile device
Managed security application for Android
13299 TLS
13000 TLS
Network Agent
iOS mobile device
Web Server
Kaspersky iOS MDM Connector
Kaspersky iOS MDM Web Server
443 TLS
2195 HTTPS
8060 HTTP / 8061 HTTPS
Kaspersky Security Center Web Console
Node.js
Apple Push Notification Server
Roaming laptop
Managed security application
Network Agent
Administrator's device
8080 TLS
Web browser

En esta figura, ninguna puerta de enlace de conexión está en uso: los dispositivos móviles se conectan directamente al Servidor de administración.

Las flechas indican el inicio del tráfico: cada flecha apunta desde un dispositivo que inicia la conexión al dispositivo que "responde" a la llamada. Se proporcionan el número del puerto y el nombre del protocolo utilizado para la transferencia de datos. Cada flecha tiene una etiqueta de número y los detalles sobre el tráfico de datos correspondiente son los siguientes:

1. El Servidor de administración envía datos a la base de datos. Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL-Server y el servidor MariaDB, o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

2. Las solicitudes de comunicación provenientes del Servidor de administración se transfieren a todos los dispositivos administrados no móviles a través del puerto UDP 15000.

   Los Agentes de red se envían solicitudes entre sí dentro de un dominio de transmisión. Luego, los datos se envían al Servidor de administración y se utilizan para definir los límites del dominio de transmisión y para la asignación automática de puntos de distribución (si esta opción está activada).

3. La información sobre el apagado de los dispositivos administrados se transfiere desde el Agente de red al Servidor de administración a través del puerto UDP 13000.

4. El Servidor de administración recibe conexiones de los Agentes de red y de los Servidores de administración secundarios a través del puerto SSL 13000.

   Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir una conexión de Agentes de red a través del puerto no SSL 14000. Kaspersky Security Center también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.

   > El punto de distribución se llamaba "Agente de actualización" en versiones anteriores de Kaspersky Security Center.

   4a. Una puerta de enlace de conexión en DMZ también recibe la conexión del Servidor de administración a través del puerto SSL 13000. Debido a que una puerta de enlace de conexión en DMZ no puede alcanzar los puertos del Servidor de administración, el Servidor de administración crea y mantiene una conexión de señal permanente con una puerta de enlace de conexión. La conexión de señal no se utiliza para transferir datos; solo se utiliza para enviar una invitación a interactuar en la red. Cuando la puerta de enlace de conexión necesita conectarse al servidor, notifica al servidor a través de esta conexión de señal y luego el servidor crea la conexión necesaria para la transferencia de datos.

   Los dispositivos fuera de la oficina también se conectan a la puerta de enlace de conexión a través del puerto SSL 13000.

5. Los dispositivos administrados (excepto dispositivos móviles) solicitan la activación a través del puerto TCP 17000. Esto no es necesario si el dispositivo tiene su propio acceso a Internet; en este caso, el dispositivo envía los datos directamente a los servidores de Kaspersky en Internet.

6. La Consola de administración basada en MMC transfiere datos al Servidor de administración a través del puerto 13291. (La Consola de administración se puede instalar en el mismo dispositivo o en un dispositivo diferente).

7. Las aplicaciones en un solo dispositivo intercambian tráfico local (ya sea en el Servidor de administración o en un dispositivo administrado). Los puertos externos no tienen que abrirse.

8. Los datos enviados del Servidor de administración a los servidores de Kaspersky (como los datos de KSN o la información sobre licencias) y los datos enviados de los servidores de Kaspersky al Servidor de administración (como las actualizaciones de aplicaciones y las actualizaciones de bases de datos antivirus) se transfieren mediante el protocolo HTTPS.

   Si no desea que su Servidor de administración tenga acceso a Internet, debe administrar estos datos de forma manual.

9. Servidor de Kaspersky Security Center 14 Web Console envía datos al Servidor de administración, que puede estar instalado en el mismo dispositivo o en un dispositivo diferente, a través del puerto 13299 TLS.

   9a. Los datos del navegador, que se instalan en un dispositivo separado del administrador, se transfieren al Servidor de Kaspersky Security Center 14 Web Console a través del puerto TLS 8080. Kaspersky Security Center 14 Web Console se puede instalar en el Servidor de administración o en otro dispositivo.

10. Solo para dispositivos móviles Android: los datos del Servidor de administración se transfieren a los servidores de Google. Esta conexión se utiliza para notificar a los dispositivos móviles de Android de que se tienen que conectar al Servidor de administración. Luego se envían notificaciones push a los dispositivos móviles.

11. Solo para dispositivos móviles Android: notificaciones push desde los servidores de Google se envían al dispositivo móvil. Esta conexión se utiliza para notificar a los dispositivos móviles de que se tienen que conectar al Servidor de administración.

12. Solo para dispositivos móviles iOS: los datos del Servidor de MDM para iOS se transfieren a los servidores de Apple Push Notification. Luego se envían notificaciones push a los dispositivos móviles.

13. Solo para dispositivos móviles iOS: las notificaciones push se envían desde los servidores de Apple al dispositivo móvil. Esta conexión se utiliza para notificar a los dispositivos móviles iOS de que se tienen que conectar al Servidor de administración.

14. Solo para dispositivos móviles: los datos de la aplicación administrada se transfieren al Servidor de administración (o a la puerta de enlace de conexión) a través del puerto 13292/13293 TLS, directamente o a través de un Microsoft Forefront Threat Management Gateway (TMG).

15. Solo para dispositivos móviles: los datos del dispositivo móvil se transfieren a la infraestructura de Kaspersky.

    15a. Si un dispositivo móvil no tiene acceso a Internet, los datos se transfieren al Servidor de administración a través del puerto 17100, y el Servidor de administración los envía a la infraestructura de Kaspersky; sin embargo, este escenario se aplica muy raramente.

16. Las solicitudes de paquetes de dispositivos administrados, incluidos los dispositivos móviles, se transfieren al Servidor web, que se encuentra en el mismo dispositivo que el Servidor de administración.

17. Solo para dispositivos móviles iOS: los datos del dispositivo móvil se transfieren a través del puerto TLS 443 al servidor de MDM para iOS, que se encuentra en el mismo dispositivo que el Servidor de administración o en la puerta de enlace de conexión.

Interacción de los componentes y aplicaciones de seguridad de Kaspersky Security Center: más información

Esta sección proporciona los esquemas para la interacción de componentes de Kaspersky Security Center y aplicaciones de seguridad administradas. Los esquemas proporcionan los números de los puertos que deben estar disponibles y los nombres de los procesos que abren esos puertos.

Convenciones utilizadas en esquemas de interacción

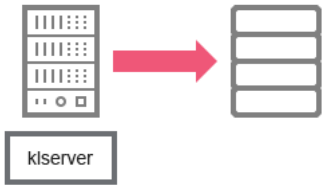
La siguiente tabla proporciona las convenciones usadas en los esquemas.

Convenciones del documento

Icono	Significado
	Servidor de administración
	Servidor de administración secundario
	DBMS
	Dispositivo cliente (que tiene un Agente de red y una aplicación de la familia Kaspersky Endpoint Security instalada o tiene una aplicación de seguridad diferente instalada que Kaspersky Security Center puede administrar)
	Puerta de enlace de conexión
	Punto de distribución
	Dispositivo cliente móvil que tiene Kaspersky Security for Mobile
	Navegador en el dispositivo del usuario
	Proceso que se ejecuta en el dispositivo y abre un puerto
	Puerto y su número
	Tráfico TCP (la dirección de la flecha muestra la dirección del flujo del tráfico)
	Tráfico UDP (la dirección de la flecha muestra la dirección del flujo del tráfico)
	Invocación de COM
	Transporte de DBMS
	Límite de DMZ

Servidor de administración y DBMS

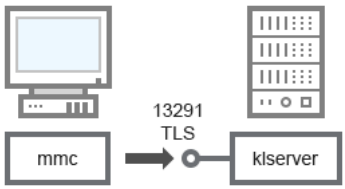
Los datos del Servidor de administración se introducen en la base de datos de SQL Server, MySQL o MariaDB.



Servidor de administración y DBMS

Si instala el Servidor de administración y la base de datos en dispositivos diferentes, debe asegurarse de que los puertos necesarios estén disponibles en el dispositivo donde se encuentra la base de datos (por ejemplo, el puerto 3306 para MySQL-Server y el servidor MariaDB, o el puerto 1433 para Microsoft SQL Server). Consulte la documentación del DBMS para obtener la información necesaria.

Servidor de administración y Consola de administración



Servidor de administración y Consola de administración

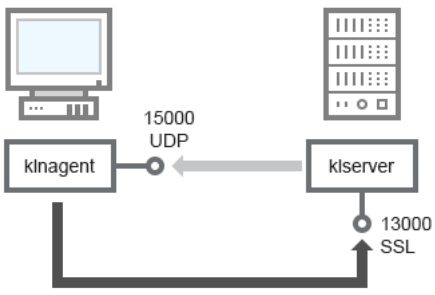
Para entender mejor el esquema, consulte la siguiente tabla.

Servidor de administración y Consola de administración (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS	Objetivo del puerto
Servidor de administración	13291	klserver	TCP	Sí	Recepción de conexiones desde la Consola de administración

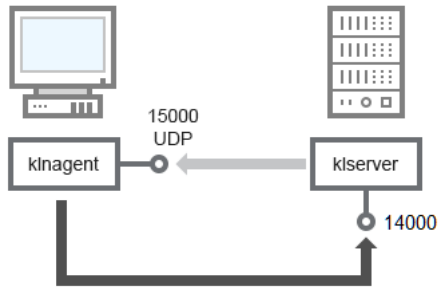
Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad

El Servidor de administración recibe la conexión de los Agentes de red a través del puerto SSL 13000 (vea la siguiente figura).



Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad, conexión mediante el puerto 13000 (recomendado)

Si usó una versión anterior de Kaspersky Security Center, el Servidor de administración de su red puede recibir conexiones de Agentes de red a través del puerto no SSL 14000 (vea la siguiente figura). Kaspersky Security Center 14 también admite la conexión de Agentes de red a través del puerto 14000, aunque se recomienda utilizar el puerto SSL 13000.



Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad, conexión mediante el puerto 14000 (menos seguridad)

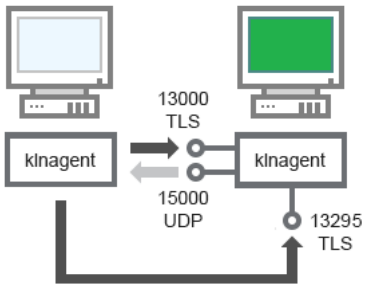
Para tener una visión más clara de los esquemas, consulte la siguiente tabla.

Servidor de administración y dispositivo cliente: administración de la aplicación de seguridad (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS (solo para TCP)	Objetivo del puerto
Agente de red	15000	klnagent	UDP	Null	Multidifusión para Agentes de red
Servidor de administración	13000	klserver	TCP	Sí	Recepción de conexiones de Agentes de red
Servidor de administración	14000	klserver	TCP	No	Recepción de conexiones de Agentes de red

Actualización del software en un dispositivo cliente a través de un punto de distribución

El dispositivo cliente se conecta al punto de distribución mediante el puerto 13000 y, si utiliza el punto de distribución como servidor push, también mediante el puerto 13295. La multidifusión del punto de distribución para Agentes de red se realiza mediante un puerto 15000 (consulte la imagen siguiente).



Actualización del software en un dispositivo cliente a través de un punto de distribución

Para entender mejor el esquema, consulte la siguiente tabla.

Actualización del software a través de un punto de distribución (tráfico)

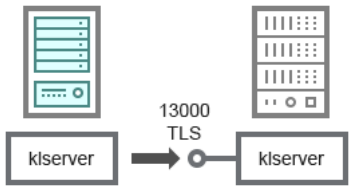
Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS (solo para TCP)	Objetivo del puerto
Agente de red	15000	klnagent	UDP	Null	Multidifusión para Agentes de red
Punto de distribución	13000	klnagent	TCP	Sí	Recepción de conexiones de Agentes de red
Punto de distribución	13295	klnagent	TCP	Sí	Envío de notificaciones push al Agente de red

Jerarquía de Servidores de administración: Servidor de administración principal y Servidor de administración secundario

El esquema (vea la siguiente figura) muestra cómo usar el puerto 13000 para asegurar la interacción entre los Servidores de administración combinados en una jerarquía.

Cuando combine dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13291 esté accesible en ambos Servidores de administración. La Consola de administración se conecta al Servidor de administración a través del puerto 13291.

Posteriormente, cuando los Servidores de administración se combinen en una jerarquía, podrá administrarlos mediante la Consola de administración conectada al Servidor de administración principal. Por lo tanto, el único requisito previo es la accesibilidad del puerto 13291 del Servidor de administración principal.



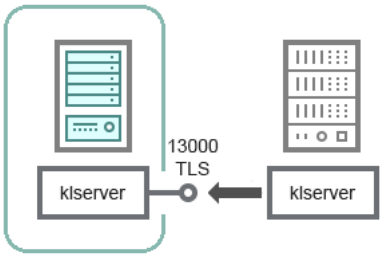
Jerarquía de Servidores de administración: Servidor de administración principal y Servidor de administración secundario

Para entender mejor el esquema, consulte la siguiente tabla.

Jerarquía de Servidores de administración (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS	Objetivo del puerto
Servidor de administración principal	13000	klserver	TCP	Sí	Recepción de conexiones desde Servidores de administración secundarios

Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ



Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ

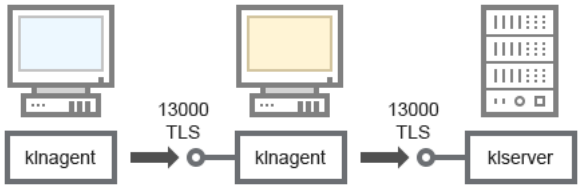
El esquema muestra una jerarquía de Servidores de administración en la que el Servidor de administración secundario localizado en la DMZ recibe una conexión del Servidor de administración principal (consulte la siguiente tabla para tener una visión más clara del esquema). Cuando combine dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13291 esté accesible en ambos Servidores de administración. La Consola de administración se conecta al Servidor de administración a través del puerto 13291.

Posteriormente, cuando los Servidores de administración se combinen en una jerarquía, podrá administrarlos mediante la Consola de administración conectada al Servidor de administración principal. Por lo tanto, el único requisito previo es la accesibilidad del puerto 13291 del Servidor de administración principal.

Jerarquía de Servidores de administración con un Servidor de administración secundario en DMZ (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS	Objetivo del puerto
Servidor de administración secundario	13000	klserver	TCP	Sí	Recepción de conexiones desde el Servidor de administración principal

Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente



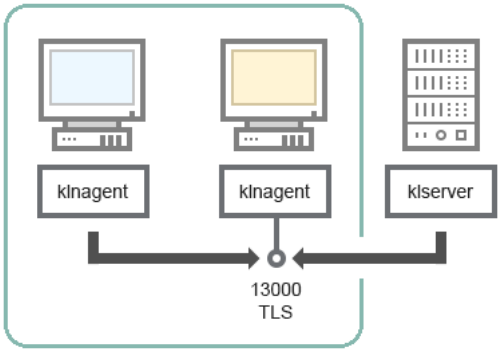
Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente

Para entender mejor el esquema, consulte la siguiente tabla.

Servidor de administración, una puerta de enlace de conexión en un segmento de red y un dispositivo cliente (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS	Objetivo del puerto
Servidor de administración	13000	klserver	TCP	Sí	Recepción de conexiones de Agentes de red
Agente de red	13000	klnagent	TCP	Sí	Recepción de conexiones de Agentes de red

Servidor de administración y dos dispositivos en DMZ: una puerta de enlace de conexión y un dispositivo cliente



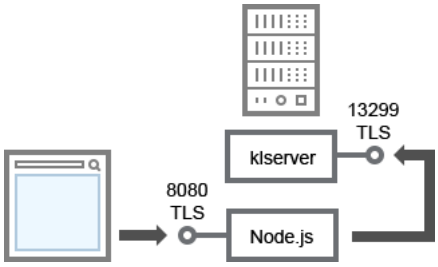
Servidor de administración con una puerta de enlace de conexión y un dispositivo cliente en DMZ

Para entender mejor el esquema, consulte la siguiente tabla.

Servidor de administración con una puerta de enlace de conexión en un segmento de red y un dispositivo cliente (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS	Objetivo del puerto
Agente de red	13000	klnagent	TCP	Sí	Recepción de conexiones de Agentes de red

Servidor de administración y Kaspersky Security Center 14 Web Console



Servidor de administración y Kaspersky Security Center 14 Web Console

Para entender mejor el esquema, consulte la siguiente tabla.

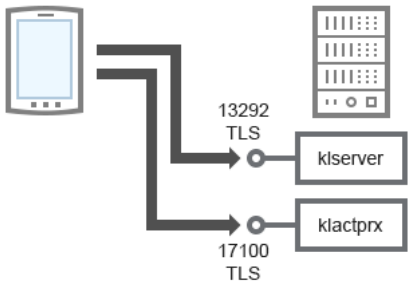
Servidor de administración y Kaspersky Security Center 14 Web Console (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS	Objetivo del puerto
Servidor de administración	13299	klserver	TCP	Sí	Recepción de conexiones desde la Kaspersky Security Center 14 Web Console al Servidor de administración a través de OpenAPI
Servidor o Servidor de administración de Kaspersky	8080	Node.js: JavaScript	TCP	Sí	Recibiendo conexiones de Kaspersky Security Center 14

Security Center 14 Web Console		del lado del servidor			Web Console

Kaspersky Security Center 14 Web Console se puede instalar en el Servidor de administración o en otro dispositivo.

Activación y administración de la aplicación de seguridad en un dispositivo móvil



Activación y administración de la aplicación de seguridad en un dispositivo móvil

Para entender mejor el esquema, consulte la siguiente tabla.

Activación y administración de la aplicación de seguridad en un dispositivo móvil (tráfico)

Dispositivo	Número de puerto	Nombre del proceso que abre el puerto	Protocolo	TLS	Objetivo del puerto
Servidor de administración	13292	klserver	TCP	Sí	Configuración de conexiones de la Consola de administración al Servidor de administración
Servidor de administración	17100	klserver	TCP	Sí	Recepción de conexiones para la activación de aplicaciones de dispositivos móviles

Mejores prácticas de despliegue

Kaspersky Security Center es una aplicación distribuida. Kaspersky Security Center incluye las aplicaciones siguientes:

- Servidor de administración: componente principal, diseñado para administrar dispositivos de una organización y almacenar datos en DBMS.
- Consola de administración: herramienta básica para el administrador. La Consola de administración se envía junto con el Servidor de administración, pero también puede instalarse individualmente en uno o varios dispositivos ejecutados por el administrador.
- Agente de red: diseñado para administrar la aplicación de seguridad instalada en un dispositivo, así como para recibir información sobre ese dispositivo y transferir esta información al Servidor de administración. Los Agentes de red se instalan en los dispositivos de una organización.

El despliegue de Kaspersky Security Center en una red de la organización se realiza del siguiente modo:

- Instalación del Servidor de administración.
- Instalación de la Consola de administración en el dispositivo del administrador.
- Instalación del Agente de red y la aplicación de seguridad en los dispositivos de la empresa.

Preparación para despliegue

Esta sección describe los pasos que debe seguir antes de desplegar Kaspersky Security Center.

Planificación del despliegue de Kaspersky Security Center

Esta sección proporciona la información sobre las opciones más convenientes para el despliegue de los componentes de Kaspersky Security Center en la red de una organización, según los siguientes criterios:

- Número total de dispositivos.
- Las unidades (oficinas locales, filiales) que están separadas organizativa o geográficamente.
- Las redes independientes conectadas por canales estrechos.
- La necesidad de acceso a Internet para el Servidor de administración.

Esquemas típicos de despliegue del sistema de protección

Esta sección describe los esquemas estándar de despliegue de sistemas de protección en una red corporativa mediante Kaspersky Security Center.

El sistema debe estar protegido contra cualquier tipos de acceso no autorizado. Le recomendamos instalar todas las actualizaciones de seguridad disponibles para su sistema operativo antes de instalar la aplicación en su dispositivo y proteger físicamente los Servidores de administración y los puntos de distribución.

Puede usar Kaspersky Security Center para desplegar un sistema de protección en la red corporativa si recurre a los siguientes esquemas de despliegue:

- Despliegue del sistema de protección por medio de Kaspersky Security Center, con uno de los siguientes métodos:
  - Mediante la Consola de administración
  - Mediante Kaspersky Security Center 14 Web Console

  Las aplicaciones Kaspersky se instalan automáticamente en los dispositivos cliente, que, a su vez, se conectan automáticamente al Servidor de administración mediante Kaspersky Security Center.

  El esquema básico de despliegue es el despliegue del sistema de protección a través de Consola de administración. El uso de Kaspersky Security Center 14 Web Console permite iniciar la instalación de las aplicaciones de Kaspersky desde un navegador.

- Despliegue manual del sistema de protección mediante paquetes de instalación independientes generados por Kaspersky Security Center.

  La instalación de aplicaciones de Kaspersky en los dispositivos cliente y en la estación de trabajo del administrador se realiza de forma manual; los parámetros para la conexión de los dispositivos cliente al Servidor de administración se especifican al instalar el Agente de red.

  Se recomienda utilizar este método de despliegue en caso de que sea imposible usar una instalación remota.

Kaspersky Security Center también permite desplegar el sistema de protección con las directivas de grupo de Microsoft Active Directory®.

Información acerca de la planificación del despliegue de Kaspersky Security Center en la red de una organización

Un Servidor de administración puede admitir un máximo de 100.000 dispositivos. Si el número total de dispositivos en una red de la organización supera los 100.000, deben desplegarse varios Servidores de administración en esa red y combinarse en una jerarquía para una administración centralizada cómoda.

Si una organización incluye oficinas locales remotas a gran escala (filiales) en sus propios administradores, es útil desplegar Servidores de administración en esas oficinas. De otra forma, esas oficinas se deben ver como redes separadas conectadas por canales de bajo rendimiento, consulte la sección "Configuración estándar: pocas oficinas a gran escala ejecutadas por sus propios administradores".

Al usar redes separadas conectadas a canales estrechos, puede ahorrarse tráfico al asignar uno o varios Agentes de red para que funcionen como puntos de distribución (consulte la tabla de cálculo del número de puntos de distribución). En este caso, todos los dispositivos en una red separada reciben actualizaciones desde tales centros de actualización locales. Los puntos de distribución reales pueden descargar actualizaciones ambos desde el Servidor de administración (escenario predeterminado) y desde servidores de Kaspersky en Internet (consulte la sección "Configuración estándar: varias pequeñas oficinas remotas").

La sección «Configuraciones estándar de Kaspersky Security Center» proporciona descripciones detalladas de las configuraciones estándar de Kaspersky Security Center. Al planear el despliegue, seleccione la configuración estándar más conveniente, según la estructura de la empresa.

En la etapa de la planificación del despliegue, debe considerarse la asignación del certificado especial X.509 al Servidor de administración. La asignación del certificado X.509 al Servidor de administración puede ser útil en los siguientes casos (lista parcial):

- Inspección del tráfico de la capa de sockets seguros (SSL) mediante un proxy de cancelación de SSL o mediante el uso de un proxy inverso.
- Integración con la infraestructura de claves públicas (PKI) de una empresa.
- Especificación de valores obligatorios en campos del certificado.
- Suministro de la fuerza de cifrado requerida de un certificado.

Selección de una estructura para la protección de una empresa

La selección de una estructura para la protección de una organización se define según los siguientes factores:

- Topología de la red de la organización.

- Estructura de organización.
- Número de empleados responsables de la protección de la red y asignación de sus responsabilidades.
- Recursos de hardware que se pueden asignar a componentes de administración de protección.
- Rendimiento de los canales de comunicación que se pueden asignar para mantener los componentes de protección en la red organizativa.
- Plazos para la ejecución de operaciones administrativas críticas en la red de la organización. Las operaciones administrativas críticas incluyen, por ejemplo, la distribución de bases de datos antivirus y la modificación de la directivas para dispositivos cliente.

Al seleccionar una estructura de protección, primero se deberían estimar los recursos de la red y de hardware disponibles para el funcionamiento de un sistema de protección centralizado.

Para analizar la infraestructura de red y hardware, es aconsejable seguir el proceso descrito a continuación:

1. Defina la configuración siguiente de la red en la que se desplegará la protección:
   - Número de segmentos de red.
   - Velocidad de los canales de comunicación entre segmentos individuales de la red.
   - Número de dispositivos administrados en cada uno de los segmentos de la red.
   - Rendimiento de cada canal de distribución que puede asignarse para mantener el funcionamiento de la protección.
2. Determine el tiempo máximo permitido para la ejecución de las operaciones administrativas clave para todos los dispositivos administrados.
3. Analice la información de los pasos 1 y 2, así como datos de pruebas de carga del sistema de administración. De acuerdo con el análisis, responda a las preguntas siguientes:
   - ¿Es posible prestar servicio a todos los clientes con un solo Servidor de administración o se requiere una jerarquía de Servidores de administración?
   - ¿Qué configuración de hardware de Servidores de administración se requiere para tratar con todos los clientes dentro de los plazos especificados en el paso 2?
   - ¿Es necesario utilizar los puntos de distribución para reducir la carga en los canales de comunicación?

Tras obtener las respuestas a las preguntas del paso 3, puede compilar un conjunto de estructuras permitidas de la protección de la organización.

En la red de la organización, puede utilizar una de las estructuras de protección estándar siguientes:

- Un Servidor de administración. Todos los dispositivos cliente están conectados a un solo Servidor de administración. El Servidor de administración funciona como punto de distribución.
- Un Servidor de administración con puntos de distribución. Todos los dispositivos cliente están conectados a un solo Servidor de administración. Algunos de los dispositivos cliente en red funcionan como puntos de distribución.
- Jerarquía de Servidores de administración. Para cada uno de los segmentos de la red, se asigna un Servidor de administración individual, que pasa a formar parte de una jerarquía general de Servidores de administración. El

Servidor de administración principal funciona como punto de distribución.

- Jerarquía de Servidores de administración con puntos de distribución. Para cada uno de los segmentos de la red, se asigna un Servidor de administración individual, que pasa a formar parte de una jerarquía general de Servidores de administración. Algunos de los dispositivos cliente en red funcionan como puntos de distribución.

Configuraciones estándar de Kaspersky Security Center

Esta sección describe las siguientes configuraciones estándares que se usan para el despliegue de componentes de Kaspersky Security Center en una red de la organización:

- Oficina única
- Pocas oficinas a gran escala, que están geográficamente separadas y son ejecutadas por sus propios administradores
- Pequeñas oficinas varias, que están geográficamente separadas

Configuración estándar: oficina única

Uno o varios Servidores de administración pueden desplegarse en la red de la organización. El número Servidores de administración puede seleccionarse según el hardware disponible o según el número total de dispositivos administrados.

Un Servidor de administración puede admitir hasta 100 000 dispositivos. Debe considerar la posibilidad de aumentar el número de dispositivos administrados en el futuro próximo: puede ser útil conectar un número ligeramente menor de dispositivos a un único Servidor de administración.

Los Servidores de administración pueden desplegarse ya sea en la intranet o en la DMZ, según si se requiere el acceso a Internet para los Servidores de administración.

Si se utilizan varios servidores, se recomienda que los combine en una jerarquía. La utilización de una jerarquía de Servidores de administración le permite evitar directivas y tareas duplicadas y gestionar el conjunto entero de dispositivos administrados como si estuvieran administrados por un Servidor de administración único (es decir, buscar dispositivos, crear selecciones de dispositivos y crear informes).

Configuración estándar: pocas oficinas a gran escala ejecutadas por sus propios administradores

Si la organización tiene unas pocas oficinas grandes geográficamente separadas, debe considerar la opción de desplegar Servidores de administración en cada una de ellas. Se pueden desplegar uno o varios Servidores de administración por oficina, según la cantidad de dispositivos cliente y el hardware disponibles. En este caso, cada una de las oficinas puede verse como una "Configuración estándar: oficina única". Para facilitar la administración, le recomendamos que combine todos los Servidores de administración en una jerarquía (de ser posible, de varios niveles).

Si algunos empleados se mueven entre oficinas con sus dispositivos (equipos portátiles), debe crearse una regla para cambiar el Agente de red entre Servidores de administración en la directiva del Agente de red.

Configuración estándar: varias pequeñas oficinas remotas

Esta configuración estándar es útil para una oficina central y muchas oficinas remotas pequeñas que pueden comunicarse con la oficina central por Internet. Cada una de las oficinas remotas puede localizarse detrás de la Traducción de la Dirección de red (NAT), es decir, no puede establecerse ninguna conexión entre dos oficinas remotas, dado que están aisladas.

Debe desplegarse un Servidor de administración en la oficina central y deben asignarse uno o varios puntos de distribución al resto de las oficinas. Si las oficinas están vinculadas a través de Internet, puede ser útil crear una tarea de *Descargar actualizaciones a los repositorios de puntos de distribución* para los puntos de distribución, de modo que descarguen actualizaciones directamente desde los servidores de Kaspersky, una carpeta local o en red, no desde el Servidor de administración.

Si algunos dispositivos en una oficina remota no tienen acceso directo al Servidor de administración (por ejemplo, el acceso al Servidor de administración se proporciona mediante Internet pero algunos dispositivos no tienen acceso a Internet), los puntos de distribución deben cambiarse al modo de Puerta de enlace de conexión. En este caso, los Agentes de red en los dispositivos en la oficina remota se conectarán, para mayor sincronización, al Servidor de administración, pero mediante la puerta de enlace, no de manera directa.

Dado que lo más probable es que el Servidor de administración no pueda sondear la red de la oficina remota, puede ser útil trasladar esta función a un punto de distribución.

El Servidor de administración no podrá enviar notificaciones al puerto UDP 15000 a dispositivos administrados ubicados detrás de la NAT en la oficina remota. Para resolver este problema, puede activar el modo de conexión continua con el Servidor de administración en las propiedades de los dispositivos que funcionan como puntos de distribución (casilla de verificación **No desconectar del Servidor de administración**). Este modo está disponible si el número total de puntos de distribución no supera los 300.

Cómo seleccionar una DBMS para el Servidor de administración

Al seleccionar el sistema de gestión de bases de datos (DBMS) para que lo utilice un Servidor de administración, debe tomar en cuenta el número de dispositivos abarcados por el Servidor de administración.

SQL Server Express Edition tiene limitaciones en el volumen de memoria que se utiliza, el número de núcleos de la CPU que se utilizan y el tamaño máximo de la base de datos. Por lo tanto, no puede usar SQL Server Express Edition si su Servidor de administración abarca más de 10 000 dispositivos o si se utiliza el Control de aplicaciones en dispositivos administrados.

Si el Servidor de administración abarca más de 10.000 dispositivos, le recomendamos que use versiones de SQL Server con menos limitaciones, p. ej.: SQL Server Workgroup Edition, SQL Server® Web Edition, SQL Server Standard Edition o SQL Server Enterprise Edition.

Si el Servidor de administración tiene a su cargo 50 000 dispositivos (o menos), y si no se usa el Control de aplicaciones en dispositivos administrados, también puede usar MySQL 8.0.20 y versiones posteriores.

Si el Servidor de administración tiene a su cargo 20 000 dispositivos (o menos), y si no se usa el Control de aplicaciones en los dispositivos administrados, puede usar el servidor MariaDB 10.3 como DBMS.

Si el Servidor de administración tiene a su cargo 10 000 dispositivos (o menos), y si no se usa el Control de aplicaciones en dispositivos administrados, también puede usar MySQL 5.5, 5.6 o 5.7 como DBMS.

Las versiones de MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 y 5.5.5 ya no son compatibles.

Si está utilizando SQL Server 2019 como DBMS y no tiene el parche acumulativo CU12 o posterior, debe realizar lo siguiente después de instalar Kaspersky Security Center:

1. Conéctese a SQL Server con SQL Management Studio.
2. Ejecute los siguientes comandos (si eligió un nombre diferente para la base de datos, use ese nombre en lugar de KAV):

```
USE KAV
```

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

3. Reinicie el servicio SQL Server 2019.

De lo contrario, el uso de SQL Server 2019 puede generar errores, como "There is insufficient system memory in resource pool 'internal' to run this query".

Selección de un DBMS

Al instalar el Servidor de administración, puede seleccionar el DBMS que usará el Servidor de administración. Al seleccionar el sistema de gestión de bases de datos (DBMS) para que lo utilice un Servidor de administración, debe tomar en cuenta el número de dispositivos abarcados por el Servidor de administración.

La siguiente tabla enumera las opciones de DBMS válidas, así como las restricciones en su uso.

Restricciones en DBMS

DBMS	Restricciones
SQL Server Express Edition 2012 o posterior	No se recomienda si tiene la intención de ejecutar un único Servidor de administración para más de 10 000 dispositivos o usar Control de aplicaciones.
Edición de SQL Server local, no Express, 2012 o posterior	Sin limitaciones.
Edición de SQL Server remota, no Express, 2012 o posterior	Solo es válido si ambos dispositivos están en el mismo dominio Windows®; si los dominios difieren, se debe establecer una relación de confianza bidireccional entre ellos.
Local o remota MySQL 5.5, 5.6 o 5.7 (Las versiones de MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 y 5.5.5 ya no son compatibles)	No se recomienda si tiene la intención de ejecutar un único Servidor de administración para más de 10 000 dispositivos o usar Control de aplicaciones.
MySQL 8.0.20 o versión posterior local o remoto	No se recomienda si tiene la intención de ejecutar un único Servidor de administración para más de 50 000 dispositivos o usar Control de aplicaciones.
Servidor MariaDB 10.3 local o remoto	No se recomienda si tiene la intención de ejecutar un único Servidor de administración para más de 20 000 dispositivos o usar el Control de aplicaciones.

Si está utilizando SQL Server 2019 como DBMS y no tiene el parche acumulativo CU12 o posterior, debe realizar lo siguiente después de instalar Kaspersky Security Center:

1. Conéctese a SQL Server con SQL Management Studio.

2. Ejecute los siguientes comandos (si eligió un nombre diferente para la base de datos, use ese nombre en lugar de KAV):

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

3. Reinicie el servicio SQL Server 2019.

De lo contrario, el uso de SQL Server 2019 puede generar errores, como "There is insufficient system memory in resource pool 'internal' to run this query".

Se prohíbe estrictamente el uso concurrente de SQL Server Express Edition DBMS por el Servidor de administración y otra aplicación.

Administración de dispositivos móviles con Kaspersky Endpoint Security for Android

Los dispositivos móviles con Kaspersky Endpoint Security for Android™ instalado (en adelante, denominados dispositivos KES) se administran por medio del Servidor de administración. Kaspersky Security Center 10 Service Pack 1, así como versiones anteriores, admite las siguientes funciones para administrar dispositivos KES:

- Manipulación de dispositivos móviles como dispositivos cliente:
  - Pertenencia a grupos de administración
  - Supervisión, por ejemplo, ver estados, eventos e informes
  - Modificación de la configuración local y asignación de directivas para Kaspersky Endpoint Security for Android
- Envío de comandos en modo centralizado
- Instalación de paquetes de aplicaciones móviles remotamente

El Servidor de administración gestiona los dispositivos KES mediante TLS, puerto TCP 13292.

Suministro de acceso a Internet al Servidor de administración

Los casos siguientes requieren acceso a Internet del Servidor de administración:

- Actualización con regularidad de las bases de datos, los módulos de software y las aplicaciones de Kaspersky
- Actualización de software de terceros

  De forma predeterminada, el Servidor de administración no requiere conexión a Internet para instalar actualizaciones de software de Microsoft en los dispositivos administrados. Por ejemplo, los dispositivos administrados pueden descargar las actualizaciones de software de Microsoft directamente desde los servidores de Microsoft Update o desde Windows Server con Microsoft Windows Server Update Services (WSUS) implementado en la red de su organización. El Servidor de administración debe estar conectado a Internet en los siguientes casos:
  - Al usar el Servidor de administración como servidor WSUS
  - Para instalar actualizaciones de software de terceros que no sean software de Microsoft
- Arreglar vulnerabilidades de software de terceros

  Se requiere conexión a Internet para que el Servidor de administración realice las siguientes tareas:
  - Para hacer una lista de reparaciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente la lista.

    - Para reparar vulnerabilidades en software de terceros que no sea el software de Microsoft.

- Administración de dispositivos (equipos portátiles) de usuarios fuera de la oficina.
- Administración de dispositivos en oficinas remotas.
- Interacción con Servidores de administración principales o secundarios ubicados en oficinas remotas
- Administración de dispositivos móviles.

Esta sección describe las formas habituales de proporcionar acceso al Servidor de administración mediante Internet. Cada una de la concentración de casos en el Acceso a Internet que proporciona al Servidor de administración puede requerir un certificado dedicado para el Servidor de administración.

Acceso a Internet: Servidor de administración en una red local

Si el Servidor de administración está ubicado dentro de la intranet de una organización, puede hacer que el puerto TCP 13000 del Servidor de administración sea accesible desde fuera mediante el redireccionamiento de puertos. Si se requiere la administración de dispositivos móviles, puede hacer accesible el puerto 13292 TCP.

Acceso a Internet: Servidor de administración en una DMZ

Si el Servidor de administración está ubicado en la DMZ de la red de la organización, no tiene acceso a la intranet de la organización. Por lo tanto, se aplican las siguientes limitaciones:

- El Servidor de administración no puede detectar nuevos dispositivos.
- El Servidor de administración no puede realizar el despliegue inicial del Agente de red mediante la instalación forzada en dispositivos en la intranet de la organización.

Esto solo se aplica a la configuración inicial del Agente de red. Las demás actualizaciones a versiones nuevas del Agente de red o la instalación de la aplicación de seguridad, sin embargo, pueden ser realizadas por el Servidor de administración. Al mismo tiempo, el despliegue inicial de Agentes de red puede ser realizado por otros medios, por ejemplo, mediante directivas de grupo de Microsoft® Active Directory®.

- El Servidor de administración no puede enviar notificaciones a dispositivos administrados mediante el puerto UDP 15000, lo que no es crítico para el funcionamiento de Kaspersky Security Center.
- El Servidor de administración no puede sondear Active Directory. Sin embargo, los resultados del Sondeo de Active Directory no se requieren en la mayoría de las situaciones.

Si las limitaciones indicadas anteriormente se ven como críticas, pueden eliminarse usando puntos de distribución ubicados dentro de la red de la organización:

- Para realizar el despliegue inicial en dispositivos sin Agente de red, primero se instala el Agente de red en uno de los dispositivos y, luego, se le asigna el estado de punto de distribución. Por lo tanto, la configuración inicial del Agente de red en otros dispositivos será realizada por el Servidor de administración mediante este punto de distribución.
- Para detectar nuevos dispositivos en la intranet de la organización y sondear Active Directory, debe permitir los métodos relevantes de detección de dispositivos en uno de los puntos de distribución.

Para garantizar el envío correcto de notificaciones al puerto UDP 15000 en dispositivos administrados ubicados dentro de la intranet de la organización, debe abarcar la red completa de puntos de distribución. En las propiedades de los puntos de distribución asignados, seleccione la casilla de verificación **No desconectar del Servidor de administración**. Como resultado, el Servidor de administración establecerá una conexión continua con los puntos de distribución y estos podrán enviar notificaciones al puerto UDP 15.000 en dispositivos dentro de la red interna de la organización (puede ser una red IPv4 o IPv6).

Acceso a Internet: Agente de red como puerta de enlace de conexión en DMZ

El Servidor de administración puede estar ubicado en la red interna de la organización; en la DMZ de esa red puede haber un dispositivo con el Agente de red ejecutándose como puerta de enlace de conexión con conectividad inversa (el Servidor de administración establece una conexión con el Agente de red). En este caso, deben cumplirse las condiciones siguientes para garantizar el acceso a Internet:

- El Agente de red debe estar instalado en el dispositivo que está en la DMZ. Cuando instale el Agente de red, en la ventana del Asistente de instalación **Puerta de enlace de conexión**, seleccione **Usar el Agente de red como puerta de enlace de conexión en DMZ**.
- El dispositivo con la puerta de enlace de conexión instalada debe estar agregado como punto de distribución. Cuando agrega la puerta de enlace de conexión, en la ventana **Agregar un punto de distribución** seleccione la opción **Seleccionar → Añadir puerta de enlace de conexión en DMZ por dirección**.
- Para usar una conexión a Internet para conectar ordenadores de escritorio externos al Servidor de administración, se debe corregir el paquete de instalación del Agente de red. En las propiedades del paquete de instalación creado, seleccione la opción **Avanzado →Conectar con el Servidor de administración usando una puerta de enlace de conexión** y luego especifique la puerta de enlace de conexión recién creada.

Para la Puerta de enlace de conexión en la DMZ, el Servidor de administración crea un certificado firmado con el certificado del Servidor de administración. Si el administrador decide asignar un certificado personalizado al Servidor de administración, debe hacerlo antes de que se cree una Puerta de enlace de conexión en la DMZ.

Si algunos empleados usan equipos portátiles que pueden conectarse al Servidor de administración desde la red local o mediante Internet, puede ser útil crear una regla de cambio para el Agente de red en la directiva del Agente de red.

Acerca de los puntos de distribución

Los dispositivos que tengan instalado el Agente de red pueden utilizarse como punto de distribución. En este modo, el Agente de red puede realizar las siguientes funciones:

- Distribuir actualizaciones (que pueden recuperarse del Servidor de administración o de servidores de actualización de Kaspersky). En este último caso, debe crearse la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* para el dispositivo que sirve como punto de distribución:
  - Instalar software (incluido el despliegue inicial de Agentes de red) en otros dispositivos.
  - Sondear la red para detectar dispositivos nuevos y actualizar la información sobre los existentes. Un punto de distribución puede aplicar los mismos métodos de detección de dispositivos que el Servidor de administración.

El despliegue de puntos de distribución en la red de una organización cumple los siguientes objetivos:

- Reduce la carga en el Servidor de administración.
- Optimiza el tráfico.

- Proporciona al Servidor de administración acceso a dispositivos en puntos poco accesibles de la red de la organización. La disponibilidad de un punto de distribución en la red detrás de la NAT (con relación al Servidor de administración) permite que el Servidor de administración realice las siguientes acciones:
  - Envíe notificaciones a dispositivos mediante UDP en la red IPv4 o IPv6.
  - Sondee la red IPv4 o IPv6.
  - Realice el despliegue inicial.
  - Actúe como un servidor push.

Se asigna un punto de distribución para un grupo de administración. En este caso, la cobertura del punto de distribución incluye todos los dispositivos dentro del grupo de administración y todos sus subgrupos. Sin embargo, el dispositivo que funciona como el punto de distribución no puede incluirse en el grupo de administración al cual se ha asignado.

Puede realizar una función de punto de distribución como una puerta de enlace de conexión. En este caso, los dispositivos en la cobertura del punto de distribución se conectarán al Servidor de administración a través de la puerta de enlace, no directamente. Este modo puede ser útil en situaciones que no permitan establecer una conexión directa entre el Servidor de administración y los dispositivos administrados.

Cálculo del número y la configuración de los puntos de distribución

Cuantos más dispositivos cliente contenga una red, más puntos de distribución requerirá. Le recomendamos que no desactive la asignación automática de puntos de distribución. Cuando la asignación automática de puntos de distribución está activada, el Servidor de administración asigna puntos de distribución si el número de dispositivos cliente es elevado y define su configuración.

La utilización de puntos de distribución exclusivamente asignados

Si planea usar ciertos dispositivos específicos como puntos de distribución (es decir, servidores asignados exclusivamente), puede optar por no usar la asignación automática de puntos de distribución. En este caso, compruebe que los dispositivos a los que planea hacer puntos de distribución tengan el volumen suficiente de espacio libre en disco, que no se apaguen con frecuencia y que tengan el modo de suspensión desactivado.

Número de puntos de distribución asignados exclusivamente en una red que contiene un único segmento de red, en función del número de dispositivos en red

Número de dispositivos cliente en el segmento de la red	Número de puntos de distribución
Menos de 300	0 (no asigne puntos de distribución)
Más de 300	Aceptable: (N/10,000 + 1), recomendado: (N/5000 + 2), donde N es el número de dispositivos conectados a una red

Número de puntos de distribución asignados exclusivamente en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

Número de dispositivos cliente por segmento de la red	Número de puntos de distribución
Menos de 10	0 (no asigne puntos de distribución)
10-100	1
Más de 100	Aceptable: (N/10,000 + 1), recomendado: (N/5000 + 2), donde N es el número de dispositivos conectados a una red

Uso de dispositivos cliente estándar (estaciones de trabajo) como puntos de distribución

Si planea usar dispositivos cliente estándar (es decir, estaciones de trabajo) como puntos de distribución, le recomendamos que asigne puntos de distribución como se muestra en las siguientes tablas para evitar una carga excesiva en los canales de comunicación y el Servidor de administración:

Número de estaciones de trabajo que funcionan como puntos de distribución en una red que contiene un único segmento de red, en función del número de dispositivos en red

Número de dispositivos cliente en el segmento de la red	Número de puntos de distribución
Menos de 300	0 (no asigne puntos de distribución)
Más de 300	(N/300 + 1), donde N es el número de dispositivos en red, pero debe haber al menos tres puntos de distribución

Número de estaciones de trabajo que funcionan como puntos de distribución en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

Número de dispositivos cliente por segmento de la red	Número de puntos de distribución
Menos de 10	0 (no asigne puntos de distribución)
10-30	1
31-300	2
Más de 300	(N/300 + 1), donde N es el número de dispositivos en red, pero debe haber al menos tres puntos de distribución

Si un punto de distribución se apaga (o no está disponible por algún otro motivo), los dispositivos administrados en su cobertura pueden acceder al Servidor de administración para obtener actualizaciones.

Jerarquía de Servidores de administración

Un MSP puede ejecutar varios Servidores de administración. Puede resultar incómodo administrar varios Servidores de administración independientes, por lo tanto, se puede aplicar una jerarquía. Una configuración de "principal/secundario" para dos Servidores de administración proporciona las siguientes opciones:

- Un Servidor de administración secundario hereda directivas y tareas del Servidor de administración principal, lo que evita la copia de la configuración.
- Las selecciones de dispositivos en el Servidor de administración principal pueden incluir dispositivos de Servidores de administración secundarios.
- Los informes sobre el Servidor de administración principal pueden contener datos (incluida información detallada) de Servidores de administración secundarios.

Servidores de administración virtual

Sobre la base de un Servidor de administración físico, se pueden crear varios Servidores de administración virtuales, que serán similares a los Servidores de administración secundarios. Comparado con el modelo de acceso discrecional, que se basa en listas de control de acceso (ACL), el modelo del Servidor de administración virtual es más funcional y proporciona un mayor nivel de aislamiento. Además de una estructura dedicada de grupos de administración para dispositivos asignados con directivas y tareas, cada Servidor de administración virtual tiene su propio grupo de dispositivos no asignados, sus propios conjuntos de informes, dispositivos y eventos seleccionados, paquetes de instalación, reglas móviles, etc. La cobertura funcional de los Servidores de administración virtuales puede ser utilizada tanto por proveedores de servicios (xSP) para maximizar el aislamiento de clientes, como por organizaciones a gran escala con flujos de trabajo sofisticados y numerosos administradores.

Los Servidores de administración virtuales son muy similares a los Servidores de administración secundarios, pero con las distinciones siguientes:

- Un Servidor de administración virtual carece de la configuración más global y sus propios puertos TCP.
- Un Servidor de administración virtual no tiene Servidores de administración secundarios.
- Un Servidor de administración virtual no tiene otros Servidores de administración virtuales.
- Un Servidor de administración físico ve dispositivos, grupos, eventos y objetos en dispositivos administrados (elementos en Cuarentena, registro de aplicaciones, etc.) de todos sus Servidores de administración virtuales.
- Un Servidor de administración virtual solo puede analizar la red con puntos de distribución conectados.

Información sobre limitaciones de Kaspersky Security Center

La siguiente tabla muestra las limitaciones de la versión actual de Kaspersky Security Center.

Limitaciones de Kaspersky Security Center

Tipo de limitación	Valor
Número máximo de dispositivos administrados por Servidor de administración	100000
Número máximo de dispositivos con la opción **No desconectar del Servidor de administración** de verificación seleccionada	300
Número máximo de grupos de administración	10000
Número máximo de eventos para almacenar	45000000
Número máximo de directivas	2000
Número máximo de tareas	2000
Número total máximo de objetos de Active Directory (unidades organizativas [OU] y cuentas de usuarios, dispositivos y grupos de seguridad)	1000000
Número máximo de perfiles en una directiva	100
Número máximo de Servidores de administración secundarios en un único Servidor de administración principal	500
Número máximo de Servidores de administración virtuales	500
Número máximo de dispositivos que un único punto de distribución puede abarcar (los puntos de distribución pueden abarcar únicamente dispositivos no móviles)	10000
Número máximo de dispositivos que pueden usar una única puerta de enlace de conexión	10 000, incluyendo dispositivos móviles

Número máximo de dispositivos móviles por Servidor de administración	100 000 menos el número de dispositivos fijos administrados

Carga de red

Esta sección contiene información sobre el volumen del tráfico de red que se intercambia entre los dispositivos cliente y el Servidor de administración durante situaciones administrativas clave.

La principal carga en la red se ocasiona debido a las siguientes situaciones administrativas en curso:

- Despliegue inicial de la protección antivirus.
- Actualización inicial de la bases de datos antivirus.
- Sincronización de un dispositivo cliente con el Servidor de administración.
- Actualizaciones periódica de las bases de datos antivirus.
- Procesamiento de eventos de dispositivos cliente por el Servidor de administración.

Despliegue inicial de la protección antivirus

Esta sección proporciona información sobre volúmenes de tráfico después de la instalación del Agente de red 14 y Kaspersky Endpoint Security para Windows en el dispositivo cliente (consulte la siguiente tabla).

El Agente de red se instala mediante una instalación forzada, cuando los archivos requeridos para la instalación se copian por el Servidor de administración a una carpeta compartida en el dispositivo cliente. Tras la instalación, el Agente de red recupera el paquete de distribución de Kaspersky Endpoint Security para Windows con la conexión al Servidor de administración.

Tráfico

Escenario	Instalación del Agente de red para un solo dispositivo cliente	Instalación de Kaspersky Endpoint Security para Windows en un solo dispositivo cliente (con las bases de datos actualizadas)	Instalación simultánea del Agente de red y de Kaspersky Endpoint Security para Windows
Tráfico del dispositivo cliente al Servidor de administración, en KB	1638,4	7843,84	9707,52
Tráfico del Servidor de administración al dispositivo cliente, en KB	69990,4	259317,76	329318,4
Tráfico total (para un solo dispositivo cliente), en KB	71628,8	267161,6	339025,92

Después de que el Agente de red se instala en dispositivos cliente, se puede asignar uno de los dispositivos en el grupo de administración para que funcione como punto de distribución. Se utiliza para la distribución de los paquetes de instalación. En este caso, el volumen de tráfico durante el despliegue inicial de la protección antivirus variará considerablemente según si utiliza la multidifusión IP.

Si se utiliza multidifusión del IP, los paquetes de instalación se envían una vez a todos los dispositivos en ejecución en el grupo de administración. De este modo, el tráfico total es N veces menor, donde N es el número total de dispositivos en ejecución en el grupo de administración. Si la multidifusión IP no se utiliza, el tráfico total es idéntico al tráfico que se calcula cuando los paquetes de distribución se descargan desde el Servidor de administración. Sin embargo, el origen del paquete será el punto de distribución, no el Servidor de administración.

Actualización inicial de la bases de datos antivirus

Las tasas de tráfico durante la actualización inicial de las bases de datos antivirus (al iniciar la tarea de actualización de las bases de datos por primera vez en un dispositivo cliente) son las siguientes:

- Tráfico del dispositivo cliente al Servidor de administración: 1,8 MB
- Tráfico del Servidor de administración al dispositivo cliente: 113 MB
- Tráfico total (para un solo dispositivo cliente): 114 MB

Los datos pueden variar levemente en función de la versión actual de la base de datos antivirus.

Sincronización de un cliente con el Servidor de administración

Esta situación describe el estado del sistema de administración cuando se produce una sincronización de datos intensiva entre un dispositivo cliente y el Servidor de administración. Los dispositivos cliente se conectan al Servidor de administración con el intervalo definido por el administrador. El Servidor de administración compara el estado de los datos de un dispositivo cliente con el del Servidor, registra la información en la base de datos sobre la última conexión del dispositivo cliente y sincroniza datos.

Esta sección contiene información sobre los valores del tráfico para las situaciones básicas de administración al conectar con un cliente del Servidor de administración (consulte la siguiente tabla). Los datos de la tabla pueden variar levemente en función de la versión actual de la base de datos antivirus.

Tráfico

Escenario	Tráfico de dispositivos cliente al Servidor de administración, en KB	Tráfico del Servidor de administración al dispositivos cliente, en KB	Tráfico total (para un solo dispositivo cliente), en KB
Sincronización inicial antes de la actualización de las bases de datos en un dispositivo cliente	699,44	568,42	1267,86
Sincronización inicial después de la actualización de las bases de datos en un dispositivo cliente	735,8	4474,88	5210,68
Sincronización sin cambios en un dispositivo cliente y el Servidor de administración	11,99	6,73	18,72
Sincronización después de cambiar el valor de un parámetro en una directiva de grupo	9,79	11,39	21,18
Sincronización después de cambiar el valor de un parámetro en una tarea de grupo	11,27	11,72	22,99

Sincronización forzada sin cambios en un dispositivo cliente	77,59	99,45	177,04

El volumen del tráfico general varía considerablemente dependiendo de si se utiliza la opción de multidifusión IP en los grupos de administración. Si se está usando la multidifusión IP, el volumen de tráfico total disminuye aproximadamente N veces para el grupo, donde N significa el número total de dispositivos incluidos en el grupo de administración.

El volumen de tráfico de la sincronización inicial antes y después de actualizar las bases de datos se especifica en los siguientes casos:

- Instalar un Agente de red y una aplicación de seguridad en un dispositivo cliente.
- Mover un dispositivo cliente a un grupo de administración.
- Aplicar una directiva y tareas que se han creado para el grupo de forma predeterminada, a un dispositivo cliente.

La tabla especifica tasas de tráfico en caso de cambios en una de las configuraciones de protección que se incluyen en la configuración de directivas de Kaspersky Endpoint Security. Los datos de otros parámetros de la directiva pueden diferir de aquellos mostrados en la tabla.

Actualización adicional de bases de datos antivirus

Las tasas de tráfico en caso de una actualización incremental de bases de datos antivirus 20 horas después de la actualización anterior son las siguientes:

- Tráfico del dispositivo cliente al Servidor de administración: 169 KB
- Tráfico del Servidor de administración al dispositivo cliente: 16 MB
- Tráfico total (para un solo dispositivo cliente): 16,3 MB

Los datos de la tabla pueden variar levemente en función de la versión actual de la base de datos antivirus.

El volumen del tráfico varía considerablemente dependiendo de si se utiliza la opción de multidifusión IP en los grupos de administración. Si se está usando la multidifusión IP, el volumen de tráfico total disminuye aproximadamente N veces para el grupo, donde N significa el número total de dispositivos incluidos en el grupo de administración.

Procesamiento de eventos de clientes por el Servidor de administración

Esta sección proporciona información sobre los valores de volumen de tráfico cuando un dispositivo cliente encuentra un evento de "Virus detectado", que se envía al Servidor de administración y se registra en la base de datos (consulte la siguiente tabla).

Tráfico

Escenario	Transferencia de datos al Servidor de administración cuando ocurre un evento de "Virus detectado"	Transferencia de datos al Servidor de administración cuando ocurren nueve eventos de "Virus detectado"
Tráfico del dispositivo cliente al Servidor de administración, en KB	49,66	64,05
Tráfico del Servidor de administración al dispositivo cliente, en KB	28,64	31,97

Tráfico total (para un solo dispositivo cliente), en KB	78,3	96,02

Los datos de la tabla pueden variar ligeramente dependiendo de la versión actual de la aplicación antivirus y de los eventos que se definen en su directiva para el registro en la base de datos del Servidor de administración.

Tráfico en 24 horas

Esta sección contiene información sobre tasas de tráfico durante 24 horas de la actividad del sistema de administración en una condición "tranquila", cuando ni los dispositivos cliente ni el Servidor de administración realizan cambios en los datos (ver la tabla a continuación).

Los datos presentados en la tabla describen la condición de la red después de la instalación estándar de Kaspersky Security Center y la finalización del Asistente de inicio rápido. La frecuencia de sincronización del dispositivo cliente con el Servidor de administración fue de 20 minutos; las actualizaciones se descargaron en el repositorio del Servidor de administración una cada hora.

Tasas de tráfico por 24 horas en estado inactivo

Flujo de tráfico	Valor
Tráfico del dispositivo cliente al Servidor de administración, en KB	3235,84
Tráfico del Servidor de administración al dispositivo cliente, en KB	64378,88
Tráfico total (para un solo dispositivo cliente), en KB	67614,72

Preparación para la administración de dispositivos móviles

Esta sección también contiene la siguiente información:

- Acerca del Servidor de dispositivos móviles de Exchange destinado a la administración de dispositivos móviles a través del protocolo Exchange ActiveSync.
- Acerca del Servidor de MDM para iOS destinado a la administración de dispositivos iOS mediante la instalación de perfiles dedicados de MDM para iOS en ellos.
- Acerca de la administración de dispositivos móviles que tienen instalado Kaspersky Endpoint Security for Android.

Servidor de dispositivos móviles de Exchange

Un Servidor de dispositivos móviles de Exchange le permite administrar dispositivos móviles conectados a un Servidor de administración usando el protocolo de Exchange ActiveSync (dispositivos EAS).

Cómo desplegar un Servidor de dispositivos móviles de Exchange

Si se desplegaron varios servidores de Microsoft Exchange dentro de una matriz de Servidor de acceso de cliente en la organización, se debe instalar un Servidor de dispositivos móviles de Exchange en cada uno de los servidores en esa matriz. La opción **Modo de clúster** debe estar activada en el Asistente de instalación del Servidor de dispositivos móviles de Exchange. En este caso, el conjunto de instancias del Servidor de dispositivos móviles de Exchange instalado en servidores en la matriz se denomina el clúster de Servidores de dispositivos móviles de Exchange.

Si no se desplegó ninguna matriz de servidor de acceso de cliente de servidores de Microsoft Exchange en la organización, debe instalarse un Servidor de dispositivos móviles de Exchange en un servidor Microsoft Exchange que tenga acceso de cliente. En este caso, la opción **Modo estándar** debe estar activada en el Asistente de instalación del Servidor de dispositivos móviles de Exchange.

Junto con el Servidor de dispositivos móviles de Exchange, el Agente de red debe instalarse en el dispositivo; ayuda a integrar el Servidor de dispositivos móviles de Exchange con Kaspersky Security Center.

La cobertura del análisis predeterminada del Servidor de dispositivos móviles de Exchange es el dominio de Active Directory actual en el cual se instaló. El despliegue de un Servidor de dispositivos móviles de Exchange en un servidor con Microsoft Exchange Server (versiones 2010, 2013) instalado permite que la extensión de la cobertura del análisis incluya todo el bosque de dominio en el Servidor de dispositivos móviles de Exchange (consulte la sección "Configuración de la cobertura del análisis"). La información solicitada durante un análisis incluye cuentas de usuarios del servidor Microsoft Exchange, directivas de Exchange ActiveSync y dispositivos móviles de los usuarios conectados a Microsoft Exchange Server sobre el protocolo de Exchange ActiveSync.

No es posible instalar varias instancias del Servidor de dispositivos móviles de Exchange dentro de un solo dominio si se ejecutan en **Modo estándar** administrados por un único Servidor de administración.

Dentro de un único bosque de dominio de Active Directory, no pueden instalarse varias instancias de un Servidor de dispositivos móviles de Exchange (o varios clústeres de Servidores de dispositivos móviles de Exchange), ya sea si se ejecutan en **Modo estándar** con la cobertura del análisis ampliada que incluye todo el bosque del dominio y si están conectados a un único Servidor de administración.

Derechos necesarios para el despliegue de un Servidor de dispositivos móviles de Exchange

El despliegue de un servidor Exchange de dispositivos móviles en Microsoft Exchange Server (2010, 2013) requiere derechos del administrador del dominio y la función de administración de la organización. El despliegue de un servidor Exchange de dispositivos móviles en Microsoft Exchange Server (2007) requiere derechos del administrador del dominio y pertenencia al grupo de seguridad de administradores de la organización Exchange.

Cuenta de servicio de Exchange ActiveSync

Cuando se instala un Servidor de dispositivos móviles de Exchange, se crea una cuenta automáticamente en Active Directory:

- En Microsoft Exchange Server (2010, 2013): cuenta de KLMDM4ExchAdmin***** con la función de grupo Grupo de función KLMDM.
- En Microsoft Exchange Server (2007): cuenta de KLMDM4ExchAdmin*****, un miembro del grupo de seguridad Grupo de seguridad de KLMDM.

El servicio del Servidor de dispositivos móviles de Exchange se ejecuta en esta cuenta.

Si desea cancelar la generación automática de una cuenta, debe crear una personalizada con los derechos siguientes:

- Al usar Microsoft Exchange Server (2010, 2013), se debe asignar una función a la cuenta que tenga permitido ejecutar los cmdlets siguientes:
  - Get-CASMailbox
  - Set-CASMailbox

- Remove-ActiveSyncDevice
- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings
- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy

- Al usar Microsoft Exchange Server (2007), a la cuenta se le deben conceder derechos de acceso a objetos de Active Directory (consulte la tabla a continuación).

Derechos de acceso a objetos de Active Directory

Acceso	Objeto	Cmdlet
Todos	Hilo "CN=Mobile Mailbox Policies,CN=<Nombre de la organización>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nombre del dominio>"	`Add-ADPermission -User <Nombre usuario o grupo> -Identity "CN Mailbox Policies,CN=<Nombre de organización>,CN=Microsoft Exchange,CN=Services,CN=Config <Nombre del dominio>" -Inherit All -AccessRight GenericAll`
Lectura	Hilo "CN=<Nombre de la organización>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nombre del dominio>"	`Add-ADPermission -User <Nombre usuario o grupo> -Identity "CN la organización>,CN=Microsoft Exchange,CN=Services,CN=Config <Nombre del dominio>" -Inherit All -AccessRight GenericRead`
Lectura/escritura	Propiedades msExchMobileMailboxPolicyLink y msExchOmaAdminWirelessEnable para objetos de Active Directory	`Add-ADPermission -User <Nombre usuario o grupo> -Identity "DC del dominio>" -InheritanceType AccessRight ReadProperty,Write Properties msExchMobileMailbox msExchOmaAdminWirelessEnable`
ms-Exch-Store-Active con derecho ampliado	Repositorios de buzones de correo del servidor Exchange, hilo "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Nombre de la organización>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nombre del dominio>"	`Get-MailboxDatabase | Add-ADPe User <Nombre de usuario o grup ExtendedRights ms-Exch-Store-A`

Servidor de MDM para iOS

El Servidor de MDM para iOS le permite administrar dispositivos iOS al instalar perfiles dedicados de MDM para iOS en ellos. Se admiten las siguientes funciones:

- Dispositivo bloqueado.
- Reinicio de contraseñas.
- Datos borrados.
- Instalación o eliminación de aplicaciones.
- Uso de un Perfil de MDM para iOS con configuración avanzada (por ejemplo, configuración de VPN, configuración del correo electrónico, configuración de Wi-Fi, configuración de la cámara, certificados, etc.).

El Servidor de MDM para iOS es un servicio web que recibe conexiones entrantes de dispositivos móviles a través de su puerto TLS (de forma predeterminada, puerto 443), que es administrado por Kaspersky Security Center usando el Agente de red. El Agente de red se instala localmente en un dispositivo con un Servidor de MDM para iOS desplegado.

Al desplegar un Servidor de MDM para iOS, el administrador debe realizar las acciones siguientes:

- Proporcionar al Agente de red acceso al Servidor de administración.
- Proporcionar a los dispositivos móviles acceso al puerto TCP del Servidor de MDM para iOS.

Esta sección aborda dos configuraciones estándares de un Servidor de MDM para iOS.

Configuración estándar: Kaspersky Device Management for iOS en DMZ

Un Servidor de MDM para iOS se ubica en la DMZ de la red local de una organización con acceso a Internet. Una peculiaridad de este enfoque es la ausencia de problemas cuando se accede al servicio web de MDM de iOS desde dispositivos por Internet.

Como la administración de un Servidor de MDM para iOS requiere que el Agente de red esté instalado de manera local, debe garantizar la interacción del Agente de red con el Servidor de administración. Puede garantizar esto usando uno de los siguientes métodos:

- Mueva el Servidor de administración a la DMZ.
- Use una puerta de enlace de conexión:
  a. En el dispositivo con el Servidor de MDM para iOS desplegado, conecte el Agente de red al Servidor de administración a través de una puerta de enlace de conexión.
  b. En el dispositivo con el Servidor de MDM para iOS desplegado, asigne el Agente de red para que actúe como puerta de enlace de conexión.

Configuración estándar: Servidor de MDM para iOS en la red local de una organización

Un Servidor de MDM para iOS está ubicado en la intranet de una organización. El puerto 443 (puerto predeterminado) se debe activar para el acceso externo, por ejemplo, al publicar el servicio web de MDM de iOS en la Microsoft Forefront® Threat Management Gateway (denominado en lo sucesivo TMG).

Cualquier configuración estándar requiere el acceso a servicios web de Apple para el Servidor de MDM para iOS (rango 17.0.0.0/8) a través del puerto TCP 2197. Este puerto se utiliza para notificar a los dispositivos sobre nuevos comandos por medio de un servicio dedicado llamado APNs.

Administración de dispositivos móviles con Kaspersky Endpoint Security for Android

Los dispositivos móviles con Kaspersky Endpoint Security for Android™ instalado (en adelante, denominados dispositivos KES) se administran por medio del Servidor de administración. Kaspersky Security Center 10 Service Pack 1, así como versiones anteriores, admite las siguientes funciones para administrar dispositivos KES:

- Manipulación de dispositivos móviles como dispositivos cliente:
  - Pertenencia a grupos de administración
  - Supervisión, por ejemplo, ver estados, eventos e informes
  - Modificación de la configuración local y asignación de directivas para Kaspersky Endpoint Security for Android
- Envío de comandos en modo centralizado
- Instalación de paquetes de aplicaciones móviles remotamente

El Servidor de administración gestiona los dispositivos KES mediante TLS, puerto TCP 13292.

Información sobre el rendimiento del Servidor de administración

Esta sección presenta los resultados de las pruebas de rendimiento del Servidor de administración para configuraciones del hardware diferentes, así como las limitaciones de la conexión de dispositivos administrados al Servidor de administración.

Limitaciones de conexión con un Servidor de administración

Un Servidor de administración admite la administración de hasta 100.000 dispositivos sin pérdida de rendimiento.

Limitaciones de conexión con un Servidor de administración sin pérdida de rendimiento:

- Un Servidor de administración puede admitir hasta 500 Servidores de administración virtuales.
- El Servidor de administración principal no admite más de 1000 sesiones simultáneamente.
- Los Servidores de administración virtuales no admiten más de 1000 sesiones simultáneamente.

Resultados de las pruebas de rendimiento del Servidor de administración

Los resultados de las pruebas de rendimiento del Servidor de administración nos permitieron definir un número máximo de dispositivos cliente con los cuales se puede sincronizar el Servidor de administración durante períodos de tiempo específicos. Puede utilizar esta información para seleccionar el esquema óptimo para instalar la protección antivirus en redes de dispositivos.

Los dispositivos con las siguientes configuraciones de hardware (consulte las tablas que se incluyen a continuación) se utilizaron para realizar pruebas:

Configuración de hardware del Servidor de administración

Parámetro	Valor
CPU	Intel Xeon CPU E5630, velocidad de reloj de 2,53 GHz, 2 socket, 8 núcleos, 16 procesadores lógicos
RAM	26 GB
Disco duro	Dispositivo de disco para SCSI con IBM ServeRAID M5014, 487 GB
Sistema operativo	Microsoft Windows Server 2019 Standard, versión 10.0.17763, compilación 17763
Red	QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client)

Configuración de hardware del dispositivo de SQL Server

Parámetro	Valor
CPU	Intel Xeon CPU X5570, velocidad de reloj de 2,93 GHz, 2 socket, 8 núcleos, 16 procesadores lógicos
RAM	32 GB
Disco duro	Adaptec Array SCSI Disk Device, 2047 GB
Sistema operativo	Microsoft Windows Server 2019 Standard, versión 10.0.17763, compilación 17763
Red	Intel 82576 Gigabit

El Servidor de administración admitía la creación de 500 Servidores de administración virtuales.

El intervalo de sincronización era de 15 minutos por cada 10 000 dispositivos administrados (consulte la siguiente tabla).

Resultados resumidos de las pruebas de carga del Servidor de administración

Intervalo de sincronización (min)	Número de dispositivos administrados
15	10000
30	20000
45	30000
60	40000
75	50000
90	60000
105	70000
120	80000
135	90000
150	100000

Si conecta el Servidor de administración a un servidor de bases de datos MySQL o SQL Express, recomendamos que no use la aplicación para administrar más de 10 000 dispositivos. Para el sistema de administración de bases de datos MariaDB, el número máximo recomendado de dispositivos administrados es 20 000.

Resultados de pruebas de rendimiento del Servidor proxy de KSN

Si la red de su empresa incluye una gran cantidad de dispositivos cliente y utilizan el Servidor de administración como Servidor proxy de KSN, el hardware del Servidor de administración debe cumplir requisitos específicos para poder procesar las solicitudes de los dispositivos cliente. Puede usar los resultados de las pruebas a continuación para evaluar la carga del Servidor de administración en su red y planificar los recursos de hardware para proporcionar el funcionamiento normal del servicio de proxy de KSN.

Las siguientes tablas muestran la configuración de hardware del Servidor de administración y del SQL Server. Esta configuración se utilizó para las pruebas.

Configuración de hardware del Servidor de administración

Parámetro	Valor
CPU	Intel Xeon CPU E5450, velocidad de reloj de 3,00 GHz, 2 sockets, 8 núcleos, 16 procesadores lógicos
RAM	32 GB
Sistema operativo	Microsoft Windows Server 2016 Standard

Configuración de hardware de SQL Server

Parámetro	Valor
CPU	Intel Xeon CPU E5450, velocidad de reloj de 3,00 GHz, 2 sockets, 8 núcleos, 16 procesadores lógicos
RAM	32 GB
Sistema operativo	Microsoft Windows Server 2019 Standard

La siguiente tabla muestra los resultados de la prueba.

Resultados resumidos de pruebas de rendimiento del Servidor proxy de KSN

Parámetro	Valor
Número máximo de solicitudes procesadas por segundo	4914
Utilización máxima de la CPU	36%

Despliegue del Agente de red y la aplicación de seguridad

Para administrar dispositivos en una organización, debe instalar el Agente de red en cada uno de ellos. El despliegue de Kaspersky Security Center distribuido en dispositivos corporativos normalmente comienza con la instalación del Agente de red en dichos dispositivos.

En Microsoft Windows XP, el Agente de red podría no realizar las siguientes operaciones correctamente: descargar actualizaciones directamente desde los servidores de Kaspersky (como un punto de distribución); funcionando como Proxy KSN (como un punto de distribución); detectar vulnerabilidades de terceros (si se usa la Administración de vulnerabilidades y parches).

Despliegue inicial

Si el Agente de red ya se ha instalado en un dispositivo, la instalación remota de aplicaciones en ese dispositivo se realiza a través de este Agente de red. El paquete de distribución de una aplicación que se instalará se transfiere mediante canales de comunicación entre Agentes de red y el Servidor de administración, junto con la configuración de la instalación definida por el administrador. Para transferir el paquete de distribución, puede usar nodos de distribución de transferencia, es decir puntos de distribución, entrega de la difusión múltiple, etc. Para obtener más información sobre cómo instalar aplicaciones en dispositivos administrados con el Agente de red ya instalado, consulte a continuación de esta sección.

Puede realizar la configuración inicial del Agente de red en dispositivos que ejecutan Windows usando uno de los métodos siguientes:

- Con herramientas de terceros para la instalación remota de aplicaciones.
- Al reproducir una imagen del disco duro del administrador con el sistema operativo y el Agente de red: usando herramientas proporcionadas por Kaspersky Security Center para administrar imágenes del disco o usando herramientas de terceros.
- Con directivas de grupo de Windows: usando herramientas de administración de Windows estándares para directivas de grupo, o en modo automático, a través de la opción correspondiente y dedicada en la tarea de instalación remota de Kaspersky Security Center.
- En modo forzado, usando opciones especiales en la tarea de instalación remota de Kaspersky Security Center.
- Al enviar a usuarios del dispositivo enlaces con paquetes independientes generados por Kaspersky Security Center. Los paquetes independientes son módulos ejecutables que contienen los paquetes de distribución de las aplicaciones seleccionadas con su configuración definida.
- Manualmente, al ejecutar instaladores de la aplicación en dispositivos.

En plataformas además de Microsoft Windows, la configuración inicial del Agente de red en dispositivos administrados se debe realizar a través de herramientas de terceros disponibles. Puede actualizar el Agente de red a una nueva versión o instalar otras aplicaciones de Kaspersky en plataformas que no sean Windows, usando Agentes de red (ya instalados en dispositivos) para realizar tareas de instalación remotas. En este caso, la instalación es idéntica a la de los dispositivos con Microsoft Windows instalado.

Al seleccionar un método y una estrategia para el despliegue de aplicaciones en una red administrada, debe considerar varios factores (lista parcial):

- Configuración de la red de la organización.
- Número total de dispositivos.

- La presencia de dispositivos en la red de la organización, que no son miembros de ningún dominio de Active Directory y la presencia de cuentas uniformes con derechos de administrador en esos dispositivos.
- La capacidad de comunicación entre el Servidor de administración y los dispositivos.
- El tipo de comunicación entre el Servidor de administración y las subredes remotas y la capacidad de los canales de red en esas subredes.
- La configuración de seguridad que se aplicó en dispositivos remotos al inicio del despliegue (por ejemplo, el uso de UAC y el modo de uso compartido simple de archivos).

Configuración de instaladores

Antes de iniciar el despliegue de aplicaciones de Kaspersky en una red, debe especificar la configuración de la instalación, es decir, los parámetros definidos durante la instalación de la aplicación. Al instalar el Agente de red, debe especificar, como mínimo, una dirección para la conexión con el Servidor de administración; también se pueden requerir algunos parámetros avanzados. Según el método de instalación que ha seleccionado, puede definir la configuración de formas diferentes. En el caso más sencillo (instalación interactiva manual en un dispositivo seleccionado), toda la configuración relevante se puede definir a través de la interfaz de usuario del instalador.

Este método de definir la configuración es inadecuado para la instalación ("silenciosa") no interactiva de aplicaciones en grupos de dispositivos. En general, el administrador debe especificar valores para la configuración en el modo centralizado; esos valores se pueden utilizar posteriormente para la instalación no interactiva en dispositivos conectados a una red seleccionados.

Paquetes de instalación

El primer y más importante método para definir la configuración de la instalación de aplicaciones es de uso múltiple y, por lo tanto, es conveniente para todos los métodos de instalación, tanto con herramientas de Kaspersky Security Center como con la mayor parte de las herramientas de terceros. Este método consiste en crear paquetes de instalación de aplicaciones en Kaspersky Security Center.

Los paquetes de instalación se generan usando los métodos siguientes:

- Automáticamente, desde paquetes de distribución especificados, sobre la base de *descriptores* incluidos (archivos con la extensión kud que contienen reglas para instalación y el análisis de resultados y otra información)
- Desde archivos ejecutables de instaladores o desde instaladores con formato Microsoft Windows Installer (MSI) para aplicaciones estándar o admitidas

Los paquetes de instalación generados se organizan jerárquicamente como carpetas con subcarpetas anidadas y archivos. Además del paquete de distribución original, un paquete de instalación contiene configuración editable (incluida la configuración del instalador y reglas para procesar tales casos como la necesidad de reiniciar el sistema operativo a fin de completar la instalación), así como módulos auxiliares menores.

Los valores de la configuración de la instalación que sería específica para una aplicación admitida individual pueden definirse en la interfaz de usuario de la Consola de administración cuando se crea el paquete de instalación. Al realizar la instalación remota de aplicaciones a través de herramientas de Kaspersky Security Center, se entregan paquetes de instalación a dispositivos de modo que la ejecución del instalador de una aplicación ponga toda la configuración definida por los administradores a disposición para esa aplicación. Al usar herramientas de terceros para la instalación de aplicaciones de Kaspersky, solo debe garantizar la disponibilidad del paquete de instalación completo en el dispositivo, es decir, la disponibilidad del paquete de distribución y su configuración. Kaspersky Security Center crea y almacena los paquetes de instalación en una subcarpeta dedicada dentro de la carpeta compartida.

No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación.

Para obtener instrucciones sobre el uso de este método de configuración para las aplicaciones de Kaspersky antes del despliegue a través de herramientas de terceros, consulte la sección "Despliegue con directivas de grupo de Microsoft Windows".

Inmediatamente después de la instalación de Kaspersky Security Center, se generan automáticamente algunos paquetes de instalación; están listos para la instalación e incluyen paquetes del Agente de red y paquetes de la aplicación de seguridad para Microsoft Windows.

Aunque la clave de licencia para una aplicación pueda estar configurada en las propiedades de un paquete de instalación, es aconsejable evitar este método de distribución de la licencia porque, de esta manera, es fácil obtener acceso de lectura a paquetes de instalación. Debe usar claves de licencia distribuidas automáticamente o tareas de instalación para claves de licencia.

Propiedades de MSI y archivos de transformación

Otra forma de configurar la instalación en la plataforma de Windows es definir propiedades MSI y archivos de transformación. Este método se puede aplicar en los casos siguientes:

- Cuando se instala a través de directivas de grupo de Windows usando herramientas regulares de Microsoft u otras herramientas de terceros para administrar directivas de grupo de Windows.
- Cuando se instalan aplicaciones usando herramientas de terceros diseñadas para administrar instaladores con formato de Microsoft Installer.

Despliegue con herramientas de terceros para la instalación remota de aplicaciones

Cuando están disponibles herramientas para la instalación remota de aplicaciones (por ejemplo, Microsoft System Center) en una organización, es cómodo realizar el despliegue inicial usando estas herramientas.

Se deben realizar las acciones siguientes:

- Seleccione el método para configurar la instalación que se adapte mejor a la herramienta de despliegue que se utilizará.
- Defina el mecanismo para la sincronización entre la modificación de la configuración de los paquetes de instalación (a través de la interfaz de la Consola de administración) y el funcionamiento de herramientas de terceros seleccionadas usadas para el despliegue de aplicaciones desde datos del paquete de instalación.

- Al realizar la instalación desde una carpeta compartida, debe asegurarse de que este recurso de archivo tenga capacidad suficiente.

Acerca de las tareas de instalación remota en Kaspersky Security Center

Kaspersky Security Center proporciona varios mecanismos para la instalación remota de aplicaciones, que se implementan como tareas de instalación remota (instalación forzada, instalación al copiar una imagen del disco duro, instalación a través de directivas de grupo de Microsoft Windows). Puede crear una tarea de instalación remota tanto para un grupo de administración específico como para dispositivos específicos o una selección de dispositivos (tales tareas se muestran en la Consola de administración, en la carpeta **Tareas**). Al crear una tarea, puede seleccionar paquetes de instalación (los del Agente de red u otra aplicación) para que se instalen con esta tarea, así como especificar determinada configuración que defina el método de instalación remota. Además, puede usar el Asistente de instalación remota, que se basa en la creación de una tarea de instalación remota y supervisión de resultados.

Las tareas para grupos de administración afectan ambos dispositivos incluidos en un grupo específico y todos los dispositivos en todos los subgrupos dentro de ese grupo de administración. Una tarea abarca dispositivos de Servidores de administración secundarios incluidos en un grupo o cualquiera de sus subgrupos si el parámetro correspondiente está activado en la tarea.

Las tareas para dispositivos específicos actualizan la lista de dispositivos cliente en cada ejecución de acuerdo con el contenido de la selección en el momento en que se inicia la tarea. Si una selección incluye dispositivos que se han conectado a Servidores de administración secundarios, la tarea también se ejecutará en esos dispositivos. Para obtener más información sobre esta configuración y los métodos de instalación, consulte más abajo en esta sección.

Para garantizar un funcionamiento correcto de una tarea de instalación remota en dispositivos conectados a Servidores de administración secundarios, debe usar la tarea de retransmisión para transmitir paquetes de instalación utilizados por su tarea a los Servidores de administración secundarios correspondientes de antemano.

Despliegue capturando y copiando la imagen del disco duro de un dispositivo

Si debe instalar el Agente de red en dispositivos en los cuales también debe instalarse un sistema operativo y otro software (o instalarse nuevamente), puede usar el mecanismo de captura y copia del disco duro de ese dispositivo.

Para realizar el despliegue al capturar y copiar un disco duro, haga lo siguiente:

1. Cree un dispositivo de referencia con un sistema operativo y el software relevante instalados, incluidos el Agente de red y una aplicación de seguridad.

2. Capture la imagen de referencia en el dispositivo y distribuya esa imagen a nuevos dispositivos mediante la tarea dedicada de Kaspersky Security Center.

   Para capturar e instalar imágenes de disco, puede usar herramientas de terceros disponibles en la organización o la función proporcionada (con una licencia de Administración de vulnerabilidades y parches) por Kaspersky Security Center.

Si usa herramientas de terceros para procesar imágenes de disco, debe eliminar la información que Kaspersky Security Center utiliza para identificar el dispositivo administrado al realizar el despliegue en un dispositivo desde una imagen de referencia. De lo contrario, el Servidor de administración no podrá distinguir correctamente los dispositivos que se hayan creado al copiar la misma imagen.

Al capturar una imagen de disco con herramientas de Kaspersky Security Center, este problema se soluciona automáticamente.

Copia de una imagen de disco con herramientas de terceros

Al aplicar herramientas de terceros para capturar la imagen de un dispositivo con el Agente de red instalado, use uno de los métodos siguientes:

- Método recomendado. Al instalar el Agente de red en un dispositivo de referencia, capture la imagen del dispositivo antes de la primera ejecución del servicio del Agente de red (porque los datos exclusivos que identifican el dispositivo se crean en la primera conexión del Agente de red con el Servidor de administración). Después de esto, se recomienda que evite ejecutar el servicio del Agente de red hasta la finalización de la operación de captura de la imagen.

- En el dispositivo de referencia, detenga el servicio del Agente de red y ejecute la utilidad klmover con la clave -dupfix. La utilidad klmover se incluye en el paquete de instalación del Agente de red. Evite cualquier ejecución subsiguiente del servicio del Agente de red hasta que la operación de captura de la imagen se complete.

- Asegúrese que klmover se ejecute con la clave -dupfix antes (requisito obligatorio) de la primera ejecución del servicio del Agente de red en dispositivos de destino, en el primer lanzamiento del sistema operativo después del despliegue de la imagen. La utilidad klmover se incluye en el paquete de instalación del Agente de red.

Si la imagen del disco duro se ha copiado incorrectamente, puede resolver este problema.

Puede aplicar una situación alternativa para el despliegue del Agente de red en nuevos dispositivos a través de imágenes del sistema operativo:

- La imagen capturada no contiene ningún Agente de red instalado.

- Un paquete de instalación independiente del Agente de red localizado en la carpeta compartida de Kaspersky Security Center se ha añadido a la lista de archivos ejecutables que se ejecutan después de la finalización del despliegue de la imagen en dispositivos de destino.

Esta situación de despliegue añade flexibilidad: puede usar una única imagen del sistema operativo junto con varias opciones de instalación para el Agente de red y la aplicación de seguridad, incluidas las reglas de movimiento de dispositivos relacionadas con el paquete independiente. Esto complica ligeramente el proceso de despliegue: tiene que proporcionar el acceso a la carpeta de red con paquetes de instalación independientes desde un dispositivo.

Despliegue con directivas de grupo de Microsoft Windows

Se recomienda que realice el despliegue inicial de Agentes de red a través de directivas de grupo de Microsoft Windows si se cumplen las condiciones siguientes:

- Este dispositivo pertenece al dominio de Active Directory.

- El esquema de despliegue le permite esperar el siguiente reinicio rutinario de los dispositivos de destino antes del despliegue inicial de los Agentes de red en ellos (o puede forzar que se aplique una directiva de grupo de Windows en esos dispositivos).

Este esquema de despliegue consiste en lo siguiente:

- El paquete de distribución de aplicación con formato de Microsoft Installer (paquete MSI) se ubica en una carpeta compartida (una carpeta donde las cuentas de LocalSystem de dispositivos de destino tienen permisos de lectura).

- En la directiva de grupo de Active Directory, se crea un objeto de instalación para el paquete de distribución.

- La cobertura de instalación se configura al especificar la unidad organizativa (OU) o el grupo de seguridad, que incluye los dispositivos de destino.

- La próxima vez un dispositivo de destino inicia sesión en el dominio (antes de que los usuarios del dispositivo inicien sesión en el sistema), todas las aplicaciones instaladas se examinan para comprobar la presencia de la aplicación requerida. Si la aplicación no se encuentra, el paquete de distribución se descarga desde el recurso especificado en la directiva y, luego, se instala.

Una ventaja de este esquema de despliegue consiste en que las aplicaciones asignadas se instalan en dispositivos de destino mientras el sistema operativo se está cargando, es decir, incluso antes de que el usuario inicie sesión en el sistema. Aun si un usuario con derechos suficientes elimina la aplicación, esta se instalará de nuevo en el siguiente lanzamiento del sistema operativo. El defecto de este esquema de despliegue es que los cambios hechos por el administrador a la directiva de grupo no entrarán en vigor hasta que los dispositivos se reinicien (si no se involucra ninguna herramienta avanzada).

Puede usar directivas de grupo para instalar tanto el Agente de red como otras aplicaciones si sus respectivos instaladores tienen el formato de Windows Installer.

Cuando se selecciona este esquema de despliegue, también debe evaluar la carga en el recurso de archivo del cual se copiarán los archivos a los dispositivos después de aplicar la directiva de grupo de Windows.

Administración de directivas de Microsoft Windows mediante la tarea de instalación remota de Kaspersky Security Center

La forma más sencilla de instalar aplicaciones a través de directivas de grupo de Microsoft Windows es seleccionar la opción **Asignar instalación del paquete en las directivas de grupo de Active Directory** en las propiedades de la tarea de instalación remota de Kaspersky Security Center. En este caso, el Servidor de administración automáticamente realiza las acciones siguientes cuando ejecuta la tarea:

- Crea objetos requeridos en la directiva de grupo de Microsoft Windows.

- Crea grupos de seguridad dedicados, incluye los dispositivos de destino en esos grupos y asigna la instalación de aplicaciones seleccionadas para ellos. El conjunto de grupos de seguridad se actualizará en cada ejecución de tarea, de acuerdo con el grupo de dispositivos en el momento de la ejecución.

Para que esta función sea operable, en las propiedades de la tarea, especifique una cuenta que tenga permisos de escritura en directivas de grupo de Active Directory.

Si tiene la intención de instalar tanto el Agente de red como otra aplicación a través de la misma tarea, seleccionar la opción **Asignar instalación del paquete en las directivas de grupo de Active Directory** hace que la aplicación cree un objeto de instalación en la directiva de Active Directory solo para el Agente de red. La segunda aplicación seleccionada en la tarea se instalará a través de las herramientas del Agente de red tan pronto como este se instale en el dispositivo. Si desea instalar una aplicación además del Agente de red a través de directivas de grupo de Windows, debe crear una tarea de instalación solo para ese paquete de instalación (sin el paquete del Agente de red). No todas las aplicaciones se pueden instalar utilizando las directivas de grupo de Microsoft Windows. Para conocer esta función, puede consultar información sobre los métodos posibles para instalar la aplicación.

Si los objetos requeridos se crean en la directiva de grupo usando herramientas de Kaspersky Security Center, la carpeta compartida de Kaspersky Security Center se utilizará como el origen del paquete de instalación. Al planear el despliegue, debe correlacionar la velocidad de lectura de esta carpeta con el número de dispositivos y el tamaño del paquete de distribución que se instalará. Puede ser útil localizar la carpeta compartida de Kaspersky Security Center en un repositorio de archivo dedicado de alto rendimiento.

Además de su facilidad de uso, la creación automática de directivas de grupo de Windows a través de Kaspersky Security Center tiene esta ventaja: al planear la instalación del Agente de red, puede especificar fácilmente el grupo de administración de Kaspersky Security Center al cual se moverán automáticamente los dispositivos después de que la instalación se complete. Puede especificar este grupo en el Asistente para añadir tareas o en la ventana de configuración de la tarea de instalación remota.

> Al administrar directivas de grupo de Windows a través de Kaspersky Security Center, puede especificar dispositivos para el objeto de una directiva de grupo al crear un grupo de seguridad. Kaspersky Security Center sincroniza el contenido del grupo de seguridad con el conjunto actual de dispositivos en la tarea. Al usar otras herramientas para administrar directivas de grupo, puede asociar objetos de directivas de grupo con OU seleccionadas de Active Directory directamente.

Instalación no asistida de aplicaciones mediante directivas de Microsoft Windows

El administrador puede crear objetos requeridos para la instalación en una directiva de grupo de Windows en su propio nombre. En este caso, puede proporcionar enlaces a paquetes almacenados en la carpeta compartida de Kaspersky Security Center o cargar estos paquetes a un servidor de archivos dedicado y luego proporcionar enlaces a este.

Pueden producirse las siguientes situaciones de instalación:

- El administrador crea un paquete de instalación y configura sus propiedades en la Consola de administración. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en la carpeta compartida de Kaspersky Security Center.

- El administrador crea un paquete de instalación y configura sus propiedades en la Consola de administración. A continuación, el administrador copia la subcarpeta EXEC completa de este paquete desde la carpeta compartida de Kaspersky Security Center a una carpeta en un recurso de archivo dedicado de la organización. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en una subcarpeta en el recurso de archivo dedicado de la organización.

- El administrador descarga el paquete de distribución de aplicaciones (incluido el del Agente de red) de Internet y lo carga al recurso de archivo dedicado de la organización. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en una subcarpeta en el recurso de archivo dedicado de la organización. La configuración de la instalación se define al configurar las propiedades MSI o al configurar archivos de transformación MST.

Despliegue forzado mediante la tarea de instalación remota de Kaspersky Security Center

Si debe empezar a desplegar Agentes de red u otras aplicaciones inmediatamente, sin esperar la próxima vez que los dispositivos de destino inicien sesión en el dominio, o si están disponibles dispositivos de destino que no sean miembros del dominio de Active Directory, puede forzar la instalación de paquetes de instalación seleccionados a través de la tarea de instalación remota de Kaspersky Security Center.

En este caso, puede especificar dispositivos de destino ya sea explícitamente (con una lista) o al seleccionar el grupo de administración de Kaspersky Security Center al cual pertenecen, o al crear una selección de dispositivos basada en un criterio específico. El tiempo del inicio de la instalación es definido por la programación de la tarea. Si el parámetro **Ejecutar tareas no realizadas** está activado en las propiedades de la tarea, la tarea se puede ejecutar inmediatamente después de que se enciendan los dispositivos de destino o cuando se muevan al grupo de administración de destino.

Este tipo de instalación consiste en la copia de archivos al recurso administrativo (admin$) en cada dispositivo y la realización del registro remoto de los servicios compatibles en ellos. Las siguientes condiciones deben cumplirse en este caso:

- Los dispositivos deben estar disponibles para la conexión ya sea desde el lado del Servidor de administración o desde el lado del punto de distribución.
- La resolución del nombre para los dispositivos de destino debe funcionar correctamente en la red.
- Los usos compartidos administrativos (admin$) deben permanecer activados en los dispositivos de destino.
- El servicio del sistema del Servidor debe ejecutarse en los dispositivos de destino (de forma predeterminada, se está ejecutando).
- Los siguientes puertos deben estar abiertos en los dispositivos de destino para permitir el acceso remoto a través de las herramientas de Windows: TCP 139, TCP 445, UDP 137 y UDP 138.
- El modo de uso compartido simple de archivos debe estar desactivado en los dispositivos de destino.
- En los dispositivos de destino, el modelo de acceso compartido y seguridad debe configurarse como *Clásico: los usuarios locales se autentican como ellos mismos*, no puede ser de ninguna manera *Solo invitados: los usuarios locales se autentican como invitados*.
- Los dispositivos de destino deben ser miembros del dominio, o deben crearse cuentas uniformes con derechos de administrador en los dispositivos de destino de antemano.

Los dispositivos en los grupos de trabajo pueden ajustarse de acuerdo con los requisitos indicados anteriormente usando la utilidad riprep.exe, que se describe en el sitio web del Servicio de soporte técnico de Kaspersky.

Durante la instalación en nuevos dispositivos que todavía no se han asignado a ninguno de los grupos de administración de Kaspersky Security Center, puede abrir las propiedades de la tarea de instalación remota y especificar el grupo de administración al cual se moverán los dispositivos después de la instalación del Agente de red.

Al crear una tarea de grupo, tenga en cuenta que cada tarea de grupo afecta todos los dispositivos en todos los grupos anidados dentro de un grupo seleccionado. Por lo tanto, debe evitar duplicar las tareas de instalación en los subgrupos.

La instalación automática es una forma simplificada de crear tareas para la instalación forzada de aplicaciones. Para hacer esto, abra las propiedades del grupo de administración, abra la lista de paquetes de instalación y seleccione los que deben instalarse en los dispositivos en este grupo. Como resultado, los paquetes de instalación seleccionados se instalarán automáticamente en todos los dispositivos en este grupo y todos sus subgrupos. El intervalo de tiempo durante el cual los paquetes se instalarán depende del rendimiento de la red y del número total de dispositivos en red.

La instalación forzada también se puede aplicar si el Servidor de administración no puede acceder a los dispositivos directamente: por ejemplo, los dispositivos están en redes aisladas, o están en una red local mientras que el elemento del Servidor de administración está en la DMZ. Para que la instalación forzada sea posible, debe proporcionar puntos de distribución a cada una de las redes aisladas.

Usar puntos de distribución como centros de instalación locales también puede ser útil al realizar la instalación en dispositivos en subredes comunicados con el Servidor de administración mediante un canal de capacidad reducida mientras está disponible un canal más amplio entre dispositivos en la misma subred. Sin embargo, tenga en cuenta que este método de instalación coloca una carga significativa en los dispositivos que actúan como puntos de distribución. Por lo tanto, se recomienda que seleccione dispositivos eficaces con unidades de almacenamiento de alto rendimiento como puntos de distribución. Además, el espacio disponible en disco en la partición con la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit debe superar, por muchas veces, el tamaño total de los paquetes de distribución de las aplicaciones instaladas.

La ejecución de paquetes independientes creada por Kaspersky Security Center

Los métodos descritos anteriormente de despliegue inicial del Agente de red y otras aplicaciones no siempre pueden implementarse porque no es posible cumplir todas las condiciones aplicables. En tales casos, puede crear un archivo ejecutable común llamado un *paquete de instalación independiente* a través de Kaspersky Security Center, usando paquetes de instalación con la configuración de la instalación relevante que hayan sido preparados por el administrador. El paquete de instalación independiente se almacena en la carpeta compartida de Kaspersky Security Center.

Puede usar Kaspersky Security Center para enviar a usuarios seleccionados un mensaje de correo electrónico que contenga un enlace a este archivo en la carpeta compartida, solicitándoles ejecutar el archivo (ya sea en modo interactivo o con la clave "-s" para la instalación silenciosa). Puede adjuntar el paquete de instalación independiente a un mensaje de correo electrónico y luego enviarlo a los usuarios de dispositivos que no tengan acceso a la carpeta compartida de Kaspersky Security Center. El administrador también puede copiar el paquete independiente a una unidad extraíble, distribuirlo al dispositivo correspondiente y ejecutarlo más adelante.

Puede crear un paquete independiente a partir de un paquete del Agente de red, un paquete de otra aplicación (por ejemplo, la aplicación de seguridad), o ambos. Si el paquete independiente se ha creado a partir de un Agente de red y otra aplicación, la instalación comienza con el Agente de red.

Al crear un paquete independiente con el Agente de red, puede especificar el grupo de administración al cual se moverán automáticamente los nuevos dispositivos (los que no hayan sido asignados a ninguno de los grupos de administración) cuando la instalación del Agente de red se complete en ellos.

Los paquetes independientes pueden ejecutarse en modo interactivo (de forma predeterminada), mostrando el resultado para la instalación de las aplicaciones que contienen, o pueden ejecutarse en modo silencioso (cuando se ejecutan con la clave "-s"). El modo silencioso puede utilizarse para la instalación a partir de scripts, por ejemplo, de scripts configurados para ejecutarse después de que se despliega una imagen del sistema operativo. El resultado de la instalación en modo silencioso está determinado por el código de devolución del proceso.

Opciones para la instalación manual de aplicaciones

Los administradores o los usuarios experimentados pueden instalar aplicaciones manualmente en modo interactivo. Pueden usar paquetes de distribución originales o paquetes de instalación generados a partir de ellos y almacenados en la carpeta compartida de Kaspersky Security Center. De forma predeterminada, los instaladores se ejecutan en modo interactivo y solicitan a los usuarios todos los valores requeridos. Sin embargo, al ejecutar el proceso setup.exe desde la raíz de un paquete de instalación con la clave "-s", el instalador se ejecutará en modo silencioso y con la configuración que se haya definido al configurar el paquete de instalación.

Al ejecutar setup.exe desde la raíz de un paquete de instalación almacenado en la carpeta compartida de Kaspersky Security Center, el paquete se copiará primero a una carpeta local temporal y, luego, el instalador de la aplicación se ejecutará desde la carpeta local.

Instalación remota de aplicaciones en dispositivos con el Agente de red instalado

Si el Agente de red operable conectado al Servidor de administración principal (o a alguno de sus Servidores secundarios) está instalado en un dispositivo, puede actualizar el Agente de red en este dispositivo, así como instalar, actualizar o eliminar cualquier aplicación admitida a través del Agente de red.

Puede activar la opción **Usando el Agente de red** en las propiedades de la tarea de instalación remota.

Si se selecciona esta opción, los paquetes de instalación con la configuración de la instalación definida por el administrador se transferirán a los dispositivos de destino mediante canales de comunicación entre el Agente de red y el Servidor de administración.

Para optimizar la carga en el Servidor de administración y minimizar el tráfico entre el Servidor de administración y los dispositivos, es útil asignar puntos de distribución en cada red remota o en cada dominio de difusión (consulte las secciones Acerca de los puntos de distribución y Creación de una estructura de grupos de administración y asignación de puntos de distribución). En este caso, los paquetes de instalación y la configuración del instalador se distribuyen desde el Servidor de administración a los dispositivos de destino a través de puntos de distribución.

Asimismo, puede usar puntos de distribución para la entrega por difusión (multidifusión) de paquetes de instalación, que permite reducir el tráfico de red considerablemente al desplegar aplicaciones.

Al transferir paquetes de instalación a dispositivos de destino sobre canales de comunicación entre Agentes de red y el Servidor de administración, todos los paquetes de instalación que se han preparado para la transferencia también se ocultarán en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Al usar varios paquetes de instalación grandes de diversos tipos e implicar un gran número de puntos de distribución, el tamaño de esta carpeta puede aumentar drásticamente.

Los archivos no pueden eliminarse de la carpeta FTServer manualmente. Cuando los paquetes de instalación originales se eliminen, los datos correspondientes se eliminarán automáticamente de la carpeta FTServer.

Los datos recibidos por los puntos de distribución se guardan en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Los archivos no pueden eliminarse de la carpeta $FTCITmp manualmente. A medida que las tareas que usan datos de esta carpeta se completan, el contenido de esta carpeta se elimina automáticamente.

Como los paquetes de instalación se distribuyen por canales de comunicación entre el Servidor de administración y los Agentes de red desde un repositorio intermedio en un formato optimizado para las transferencias de red, no se permiten cambios en los paquetes de instalación almacenados en la carpeta original de cada paquete de instalación. Esos cambios no serán registrados automáticamente por el Servidor de administración. Si debe modificar los archivos de los paquetes de instalación manualmente (aunque se recomienda evitar esta situación), debe modificar la configuración de un paquete de instalación en la Consola de administración. La modificación de la configuración de un paquete de instalación en la Consola de administración hace que el Servidor de administración actualice la imagen del paquete en el caché que se ha preparado para la transferencia a los dispositivos de destino.

Administración de reinicios de dispositivos en la tarea de instalación remota

Los dispositivos a menudo deben reiniciarse para completar la instalación remota de aplicaciones (en particular, en Windows).

Si usa la tarea de instalación remota de Kaspersky Security Center, en el Asistente para añadir tareas o en la ventana de propiedades de la tarea que se ha creado (sección **Reinicio del sistema operativo**), puede seleccionar la acción para realizar cuando se requiera un reinicio:

- **No reiniciar el dispositivo**. En este caso, no se realizará ningún reinicio automático. Para completar la instalación, debe reiniciar el dispositivo (por ejemplo, manualmente o a través de la tarea de administración del dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas de instalación en servidores y otros dispositivos donde la operación continua es crítica.

- **Reiniciar el dispositivo**. En este caso, el dispositivo siempre se reinicia automáticamente si se requiere un reinicio para la finalización de la instalación. Esta opción es útil para las tareas de instalación en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**. En este caso, en la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). La opción **Solicitar al usuario una acción** es la más conveniente para las estaciones de trabajo donde los usuarios necesitan la posibilidad de seleccionar la hora más cómoda para un reinicio.

Conveniencia de la actualización de bases de datos en un paquete de instalación de una aplicación de seguridad

Antes de iniciar el despliegue de la protección, debe tener en cuenta la posibilidad de actualizar las bases de datos antivirus (incluidos los módulos de los parches automáticos) que se envían junto con el paquete de distribución de la aplicación de seguridad. Es útil actualizar las bases de datos en el paquete de instalación de la aplicación antes de iniciar el despliegue (por ejemplo, usando el comando correspondiente en el menú contextual de un paquete de instalación seleccionado). Esto reducirá el número de reinicios requeridos para la finalización del despliegue de la protección en los dispositivos de destino.

Utilización de herramientas para la instalación remota de aplicaciones en Kaspersky Security Center para ejecutar archivos ejecutables relevantes en dispositivos administrados

Con el Asistente de nuevo paquete, puede seleccionar cualquier archivo ejecutable y definir la configuración de la línea de comandos para este. Para hacerlo, puede añadir al paquete de instalación el propio archivo seleccionado o la carpeta completa en la cual se almacena este archivo. Luego, debe crear la tarea de instalación remota y seleccionar el paquete de instalación que se ha creado.

Mientras la tarea se está ejecutando, el archivo ejecutable especificado con la configuración definida de la solicitud de comando se ejecutará en los dispositivos de destino.

Si usa instaladores con formato Microsoft Windows Installer (MSI), Kaspersky Security Center analiza los resultados de instalación por medio de herramientas estándar.

Si está disponible una licencia de Administración de vulnerabilidades y parches, Kaspersky Security Center (al crear un paquete de instalación para cualquier aplicación admitida en el entorno corporativo) también usa reglas para la instalación y el análisis de los resultados de la instalación que están en su base de datos que se actualiza.

De otro modo, la tarea predeterminada para los archivos ejecutables espera la finalización del proceso en ejecución y de todos sus procesos secundarios. Después de la finalización de todos los procesos en ejecución, la tarea se completará correctamente independientemente del código de devolución del proceso inicial. Para cambiar tal comportamiento de esta tarea, antes de crear la tarea, debe modificar manualmente los archivos .kpd generados por Kaspersky Security Center en la carpeta del paquete de instalación recientemente creada.

Para que la tarea no espere la finalización del proceso en ejecución, configure el valor del parámetro Wait en 0 en la sección [SetupProcessResult]:

Ejemplo:
[SetupProcessResult]
Wait=0

Para que la tarea solo espere la finalización del proceso en ejecución en Windows, no la finalización de todos los procesos secundarios, configure el valor del parámetro WaitJob en 0 en la sección [SetupProcessResult], por ejemplo:

Ejemplo:
[SetupProcessResult]
WaitJob=0

Para que la tarea se complete correctamente o devuelva un error según el código de devolución del proceso en ejecución, enumere los códigos de devolución correctos en [SetupProcessResult_SuccessCodes], sección, por ejemplo:

Ejemplo:
[SetupProcessResult_SuccessCodes]
0=
3010=

En este caso, cualquier código además de los enumerados causará la devolución de un error.

Para que se muestre una cadena con un comentario sobre la finalización correcta de la tarea o un error en los resultados de la tarea, introduzca breves descripciones de los errores que correspondan a códigos de devolución del proceso en las secciones [SetupProcessResult_SuccessCodes] y [SetupProcessResult_ErrorCodes], por ejemplo:

Ejemplo:

[SetupProcessResult_SuccessCodes]

0=La instalación ha finalizado correctamente

3010=Se requiere un reinicio para completar la instalación

```
[SetupProcessResult_ErrorCodes]
1602=La instalación fue cancelada por el usuario
1603=Error grave durante la instalación.
```

Para usar herramientas de Kaspersky Security Center para administrar el reinicio del dispositivo (si se requiere un reinicio para completar una operación), enumere los códigos de devolución del proceso que indican que se debe realizar un reinicio, en la sección [SetupProcessResult_NeedReboot]:

```
Ejemplo:
[SetupProcessResult_NeedReboot]
3010=
```

Supervisión del despliegue

Para supervisar el despliegue de Kaspersky Security Center y asegurarse de que una aplicación de seguridad y el Agente de red estén instalados en los dispositivos administrados, debe comprobar el semáforo en la sección **Despliegue**. Este semáforo se localiza en el espacio de trabajo del nodo del Servidor de administración en la ventana principal de Consola de administración. El semáforo refleja el estado de despliegue actual. El número de dispositivos con el Agente de red y la aplicación de seguridad instalados se muestra al lado del semáforo. Cuando se está ejecutando una tarea de instalación, puede supervisar su progreso aquí. Si ocurre algún error de instalación, el número de errores se muestra aquí. Puede ver los detalles de cualquier error haciendo clic en el enlace.

También puede usar el gráfico de despliegue en el espacio de trabajo de la carpeta **Dispositivos administrados** en la ficha **Grupos**. El gráfico refleja el proceso de despliegue y muestra el número de dispositivos sin el Agente de red, con el Agente de red o con el Agente de red y una aplicación de seguridad.

Para obtener más información sobre el progreso del despliegue (o el funcionamiento de una tarea de instalación específica), abra la ventana de resultados de la tarea de instalación remota relevante: haga clic con el botón secundario del ratón en la tarea y seleccione **Resultados** el menú contextual. La ventana muestra dos listas: la superior contiene los estados de la tarea en los dispositivos, mientras que la inferior contiene los eventos de la tarea en el dispositivo que está seleccionado actualmente en la lista superior.

Se añade información sobre los errores de despliegue en el Registro de eventos de Kaspersky en el Servidor de administración. También encontrará información sobre errores mediante la selección de eventos correspondiente en el nodo del Servidor de administración en la ficha **Eventos**.

Configuración de instaladores

Esta sección proporciona información sobre los archivos de los instaladores de Kaspersky Security Center y la configuración de la instalación, así como recomendaciones sobre cómo instalar el Servidor de administración y el Agente de red en modo silencioso.

Información general

Los instaladores de los componentes de Kaspersky Security Center 14 (Servidor de administración, Agente de red y Consola de administración) utilizan la tecnología de Windows Installer. Un paquete MSI es el núcleo de un instalador. Este formato de paquete permite usar todas las ventajas proporcionadas por Windows Installer: la escalabilidad, la disponibilidad de un sistema de parches, el sistema de transformación, la instalación centralizada a través de soluciones de terceros y el registro transparente con el sistema operativo.

Instalación en modo silencioso (con un archivo de respuesta)

Los instaladores del Servidor de administración y el Agente de red tienen la función de trabajar con el archivo de respuesta (ss_install.xml), donde está integrada la parámetros para la instalación en modo silencioso sin la participación del usuario. El archivo ss_install.xml se ubica en la misma carpeta que el paquete MSI; se utiliza automáticamente durante la instalación en modo silencioso. Puede habilitar el modo de instalación silenciosa con la clave de línea de comando "/s".

A continuación, se proporciona una descripción general de una ejecución de ejemplo:

```
setup.exe /s
```

El archivo ss_install.xml es una instancia del formato interno de la parámetros del instalador de Kaspersky Security Center. Los paquetes de distribución contienen el archivo ss_install.xml con la parámetros predeterminada.

No modifique ss_install.xml manualmente. Este archivo puede modificarse mediante las herramientas de Kaspersky Security Center al modificar la parámetros de los paquetes de instalación en la Consola de administración.

Instalación del Agente de red en modo silencioso (sin un archivo de respuesta)

Puede instalar el Agente de red con un único paquete msi, especificando los valores de las propiedades MSI de la forma estándar. Esta situación permite que el Agente de red se instale usando directivas de grupo. Para evitar conflictos entre los parámetros definida mediante las propiedades MSI y los parámetros definida en el archivo de respuesta, puede desactivar el archivo de respuesta al configurar la propiedad `DONT_USE_ANSWER_FILE=1`. A continuación, se especifica un ejemplo de una ejecución del instalador del Agente de red con un paquete msi.

La instalación del Agente de red en modo no interactivo requiere la aceptación de las condiciones del Contrato de licencia de usuario final. Utilice el parámetro `EULA=1` solo si ha leído, y entiende y acepta todas las condiciones del Contrato de licencia de usuario final.

Ejemplo:

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

También puede definir los parámetros de la instalación para un paquete msi al preparar el archivo de respuesta de antemano (uno con la extensión mst). Este comando aparece de la forma siguiente:

Ejemplo:

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

Puede especificar varios archivos de respuesta en un solo comando.

Configuración de la instalación parcial a través de setup.exe

Al ejecutar la instalación de aplicaciones mediante setup.exe, puede añadir los valores de cualquiera de las propiedades de MSI al paquete MSI.

Este comando aparece de la forma siguiente:

Ejemplo:
`/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"`

Parámetros de la instalación del Servidor de administración

La siguiente tabla describe las propiedades MSI que puede configurar al instalar el Servidor de administración. Toda los parámetros es opcional, excepto EULA y PRIVACYPOLICY.

Parámetros de la instalación del Servidor de administración en modo no interactivo

Propiedad de MSI	Descripción	Valores disponibles
EULA	Aceptación de las condiciones de las licencias (requerida)	• 1: He leído, y entiendo y acepto todas las condiciones del Contrato de licencia de usuario final. • Otro valor o sin valor: no acepto las condiciones del Contrato de licencia (no se realiza la instalación).
PRIVACYPOLICY	Aceptación de las condiciones de la Política de privacidad (requerido)	• 1: Entiendo y acepto que todos mis datos serán manejados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad. Confirmo que he leído y entendido completamente la Política de privacidad. • Otro valor o sin valor: No acepto las condiciones de la Política de privacidad (no se realiza la instalación).
INSTALLATIONMODETYPE	Tipo de instalación del Servidor de administración	• Estándar. • Personalizada.
INSTALLDIR	Carpeta de instalación de la aplicación	Valor de cadena.
ADDLOCAL	Lista de componentes para instalar (separados por comas)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Lista mínima de componentes suficientes para la instalación apropiada del Servidor de administración: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Tamaño de la red	• NRT_1_100: de 1 a 100 dispositivos.

		• NRT_100_1000: De 101 a 1000 dispositivos. • NRT_GREATER_1000: más de 1000 dispositivos.
SRV_ACCOUNT_TYPE	Forma de especificar el usuario para el funcionamiento del servicio del Servidor de administración	• SrvAccountDefault: La cuenta de usuario se creará automáticamente. • SrvAccountUser: La cuenta de usuario se define manualmente.
SERVERACCOUNTNAME	Nombre de usuario para el servicio	Valor de cadena.
SERVERACCOUNTPWD	Contraseña de usuario para el servicio	Valor de cadena.
DBTYPE	Tipo de la base de datos	• MySQL: se utilizará un servidor de bases de datos MySQL o MariaDB. • MSSQL: se utilizará un servidor de bases de datos Microsoft SQL Server (SQL Server Express).
MYSQLSERVERNAME	Nombre completo del servidor de bases de datos MySQL o MariaDB	Valor de cadena.
MYSQLSERVERPORT	Número de puerto para la conexión al servidor de bases de datos MySQL o MariaDB	Valor numérico.
MYSQLDBNAME	Nombre del servidor de bases de datos MySQL o MariaDB	Valor de cadena.
MYSQLACCOUNTNAME	Nombre de usuario para la conexión con el servidor de bases de datos MySQL o MariaDB	Valor de cadena.
MYSQLACCOUNTPWD	Contraseña de usuario para la conexión con el servidor de bases de datos MySQL o MariaDB	Valor de cadena.
MSSQLCONNECTIONTYPE	Tipo de uso de la base de datos de MSSQL	• InstallMSSEE: Instalar desde un paquete. • ChooseExisting: Usar el servidor instalado.
MSSQLSERVERNAME	Nombre completo de la instancia de SQL Server	Valor de cadena.
MSSQLDBNAME	Nombre de la base de datos de SQL Server	Valor de cadena.
MSSQLAUTHTYPE	Método de autenticación	• Windows.

	para la conexión con SQL Server	• SQLServer.
MSSQLACCOUNTNAME	Nombre de usuario para la conexión con SQL Server en modo SQLServer	Valor de cadena.
MSSQLACCOUNTPWD	Contraseña de usuario para la conexión con SQL Server en modo SQLServer	Valor de cadena.

CREATE_SHARE_TYPE	Método de especificación de la carpeta compartida	• Crear: cree una nueva carpeta compartida; en este caso, se deben definir las siguientes propiedades:
		  • SHARELOCALPATH: Ruta a una carpeta local.
		  • SHAREFOLDERNAME: Nombre de red de una carpeta.
		• Null: La propiedad de EXISTSHAREFOLDERNAME se debe especificar.

EXISTSHAREFOLDERNAME	Ruta completa a una carpeta compartida existente	Valor de cadena.
SERVERPORT	Número de puerto para conectar con el Servidor de administración	Valor numérico.
SERVERSSLPORT	Número de puerto para establecer la conexión SSL al Servidor de administración	Valor numérico.
SERVERADDRESS	Dirección de Servidor de administración	Valor de cadena.
SERVERCERT2048BITS	Tamaño de la clave del certificado del Servidor de administración (bits)	• 1: El tamaño de la clave del certificado del Servidor de administración es de 2.048 bits. • 0: El tamaño de la clave del certificado del Servidor de administración es de 1.024 bits. • Si no se especifica ningún valor, el tamaño de la clave del certificado del Servidor de administración es de 1.024 bits.
MOBILESERVERADDRESS	Dirección del Servidor de administración para la conexión de dispositivos móviles; se ignora si no se ha seleccionado el componente MobileSupport	Valor de cadena.

Parámetros de la instalación del Agente de red

La siguiente tabla describe las propiedades MSI que puede configurar al instalar el Agente de red. Toda los parámetros es opcional, excepto EULA y SERVERADDRESS.

Parámetros de la instalación del Agente de red en modo no interactivo

Propiedad de MSI	Descripción	Valores disponibles
EULA	Aceptación de las condiciones del Contrato de licencia	• 1: He leído, y entiendo y acepto todas las condiciones del Contrato de licencia de usuario final. • 0—I: No acepto los términos del Contrato de licencia (no se realiza la instalación). • Sin valor: No acepto las condiciones del Contrato de licencia (no se realiza la instalación).
DONT_USE_ANSWER_FILE	Leer la configuración de la instalación del archivo de respuesta	• 1—No utilizar. • Otro valor o ningún valor—Leer.
INSTALLDIR	Ruta a la carpeta de instalación del Agente de red	Valor de cadena.
SERVERADDRESS	Dirección del Servidor de administración (requerida)	Valor de cadena.
SERVERPORT	Número de un puerto para la conexión al Servidor de administración	Valor numérico.
SERVERSSLPORT	Número del puerto para conexión cifrada al Servidor de administración usando el protocolo SSL	Valor numérico.
USESSL	Si se debe utilizar una conexión SSL	• 1: Utilizar. • Otro valor o ningún valor: No utilizar.
OPENUDPPORT	Si se debe abrir un puerto UDP	• 1: Abrir. • Otro valor o ningún valor: No abrir.
UDPPORT	Número de puerto UDP	Valor numérico.
USEPROXY	Si se debe utilizar un servidor proxy	

		• 1: Utilizar. • Otro valor o ningún valor: No utilizar.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Dirección del proxy y número de puerto para la conexión con el servidor proxy	Valor de cadena.
PROXYLOGIN	Contraseña para la conexión a un servidor proxy	Valor de cadena.
PROXYPASSWORD	Contraseña de la cuenta para la conexión a un servidor proxy (no especifique ningún detalle de las cuentas privilegiadas en los parámetros de los paquetes de instalación).	Valor de cadena.
GATEWAYMODE	Modo de uso de la puerta de enlace de conexión	• 0: No usar puerta de enlace de conexión. • 1: Usar este Agente de red como puerta de enlace de conexión. • 2: Conectar con el Servidor de administración usando la puerta de enlace de conexión.
GATEWAYADDRESS	Dirección de la puerta de enlace de conexión	Valor de cadena.
CERTSELECTION	Método de recepción de un certificado	• GetOnFirstConnection: Recibir un certificado del Servidor de administración. • GetExistent: seleccione un certificado existente. Si esta opción está seleccionada, debe especificarse la propiedad CERTFILE.
CERTFILE	Ruta al archivo de certificado	Valor de cadena.
VMVDI	Activar el modo dinámico de Infraestructura de Escritorio Virtual (VDI)	• 1: Activar. • 0: No activar. • Sin valor: no activar.
LAUNCHPROGRAM	Si se debe ejecutar el servicio del Agente de red tras la instalación	• 1: Iniciar.

		• Otro valor o ningún valor: No iniciar.
NAGENTTAGS	Etiqueta para el Agente de red (tiene prioridad sobre la etiqueta dada en el archivo de respuestas)	Valor de cadena.

Infraestructura virtual

Kaspersky Security Center admite el uso de máquinas virtuales. Puede instalar el Agente de red y la aplicación de seguridad en cada máquina virtual, y puede proteger las máquinas virtuales a nivel del hipervisor. En el primer caso, puede usar una aplicación de seguridad estándar o Kaspersky Security for Virtualization o Light Agent para proteger sus máquinas virtuales. En el segundo caso, puede utilizar Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center admite la reversión de máquinas virtuales a su estado anterior.

Sugerencias para reducir la carga en máquinas virtuales

Al instalar el Agente de red en una máquina virtual, se le aconseja considerar desactivar algunas funciones de Kaspersky Security Center que parecen ser de poco uso para las máquinas virtuales.

Al instalar el Agente de red en una máquina virtual o en una plantilla diseñada para la generación de máquinas virtuales, recomendamos realizar las acciones siguientes:

- Si está ejecutando una instalación remota, en la ventana de propiedades del paquete de instalación del Agente de red (en la sección **Avanzado**), seleccione la opción **Optimizar la configuración para VDI**.
- Si está ejecutando una instalación interactiva a través de un Asistente, en la ventana del Asistente, seleccione la opción **Optimizar la configuración del Agente de red para la infraestructura virtual**.

Seleccionar esas opciones altera la configuración del Agente de red de modo que las funciones siguientes permanecen desactivadas de forma predeterminada (antes de aplicar una directiva):

- Recuperación de información sobre el software instalado.
- Recuperación de información sobre el hardware.
- Recuperación de información sobre las vulnerabilidades detectadas.
- Recuperación de información sobre las actualizaciones requeridas.

Por lo general, estas funciones no son necesarias en máquinas virtuales porque usan software uniforme y hardware virtual.

La desactivación de las funciones es irreversible. Si se requiere alguna de las funciones desactivadas, puede activarla a través de la directiva del Agente de red, o a través de la configuración local del Agente de red. La configuración local del Agente de red está disponible a través del menú contextual del dispositivo relevante en la Consola de administración.

Compatibilidad para máquinas virtuales dinámicas

Kaspersky Security Center admite máquinas virtuales dinámicas (solo Windows). Si se ha desplegado una infraestructura virtual en la red de la organización, en ciertos casos pueden usarse máquinas virtuales (temporales) dinámicas. Las máquinas virtuales dinámicas se crean bajo nombres únicos según una plantilla preparada por el administrador. El usuario trabaja en la máquina virtual un tiempo, luego, después de apagarse, esta máquina virtual se eliminará de la infraestructura virtual. Si Kaspersky Security Center se ha desplegado en la red de la organización, se añadirá una máquina virtual con el Agente de red instalado a la base de datos del Servidor de administración. Después de que se apague una máquina virtual, la entrada correspondiente también se debe eliminar de la base de datos del Servidor de administración.

Para hacer funcional la función de la eliminación automática de entradas en máquinas virtuales, al instalar el Agente de red en una plantilla para máquinas virtuales dinámicas, seleccione la opción **Activar modo dinámico para VDI**:

- Para la instalación remota: en la ventana de propiedades del paquete de instalación del Agente de red (sección **Avanzado**)
- Para la instalación interactiva: en el Asistente de instalación del Agente de red

En ningún caso seleccione la opción **Activar modo dinámico para VDI** al instalar el Agente de red en dispositivos físicos.

Si desea que los eventos de las máquinas virtuales dinámicas se almacenen en el Servidor de administración durante un tiempo después de eliminar esas máquinas virtuales, en la ventana de propiedades del Servidor de administración, en la sección **Repositorio de eventos**, seleccione la opción **Almacenar eventos tras la eliminación de los dispositivos** y especifique el plazo de almacenamiento máximo para los eventos (en días).

Compatibilidad para la copia de máquinas virtuales

La copia de una máquina virtual con el Agente de red instalado o la creación un desde una plantilla con el Agente de red instalado son idénticas al despliegue de Agentes de red mediante la captura y la copia de una imagen del disco duro. De este modo, en el caso general, al copiar máquinas virtuales, tiene que realizar las mismas acciones que al desplegar el Agente de red al copiar una imagen de disco.

Sin embargo, los dos casos descritos a continuación muestran el Agente de red, que detecta la copia automáticamente. Debido a los motivos indicados anteriormente, no debe realizar las operaciones sofisticadas descritas en "Despliegue al capturar y copiar el disco duro de un dispositivo":

- La opción **Activar modo dinámico para VDI** estaba seleccionada cuando el Agente de red se instaló: después de cada reinicio del sistema operativo, esta máquina virtual se reconocerá como un nuevo dispositivo, sin tener en cuenta si se lo ha copiado o no.
- Uno de los siguientes hipervisores está en uso: VMware™, HyperV® o Xen®: el Agente de red detecta la copia de la máquina virtual por los ID cambiados del hardware virtual.

El análisis de los cambios en el hardware virtual no es absolutamente confiable. Antes de aplicar este método de forma generalizada, debe probarlo en un pequeño grupo de máquinas virtuales para comprobar la versión del hipervisor que se usa actualmente en su organización.

Compatibilidad de la reversión del sistema de archivos para dispositivos con el Agente de red

Kaspersky Security Center es una aplicación distribuida. La reversión del sistema de archivos a un estado anterior en un dispositivo con el Agente de red instalado llevará a la cancelación de la sincronización de los datos y el funcionamiento incorrecto de Kaspersky Security Center.

El sistema de archivos (o parte de este) puede revertirse en los siguientes casos:

- Al copiar una imagen del disco duro.
- Al restaurar un estado de la máquina virtual por medio de la infraestructura virtual.
- Al restaurar datos desde una copia de seguridad o un punto de recuperación.

Las situaciones en las cuales el software de terceros en dispositivos con el Agente de red instalado afecta la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ son situaciones solo críticas para Kaspersky Security Center. Por lo tanto, siempre debe excluir esta carpeta del procedimiento de recuperación, de ser posible.

Dado que las reglas del lugar de trabajo de algunas organizaciones ofrecen la reversión del sistema de archivos en los dispositivos, se ha habilitado la reversión del sistema de archivos en los dispositivos con el Agente de red instalado en Kaspersky Security Center a partir de la versión 10 Maintenance Release 1 (el Servidor de administración y los Agentes de red deben ser de la versión 10 Maintenance Release 1 o posteriores). Cuando se detectan, esos dispositivos se vuelven a conectar automáticamente al Servidor de administración con el borrado de todos datos y la sincronización completa.

De forma predeterminada, la compatibilidad con la detección de la reversión del sistema de archivos está activada en Kaspersky Security Center 14.

Siempre que sea posible, evite revertir la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ en los dispositivos con el Agente de red instalado, porque la resincronización completa de datos requiere una gran cantidad de recursos.

La reversión del estado del sistema está totalmente prohibida en un dispositivo con el Servidor de administración instalado. Tampoco se permite la reversión de la base de datos usada por el Servidor de administración.

Puede restaurar un estado del Servidor de administración desde una copia de seguridad solo con la utilidad klbackup estándar.

Instalación local de aplicaciones

Esta sección proporciona un procedimiento de instalación para las aplicaciones que pueden instalarse únicamente en dispositivos locales.

Para realizar la instalación local de aplicaciones en un dispositivo cliente específico, debe tener derechos de administrador para ese dispositivo.

Para instalar aplicaciones localmente en un dispositivo cliente específico:

1. Instale el Agente de red en el dispositivo cliente y configure la conexión entre el dispositivo cliente y el Servidor de administración.

2. Instale las aplicaciones requeridas en el dispositivo como se describe en las guías de estas aplicaciones.

3. Instale un complemento de administración para cada una de las aplicaciones instaladas en la estación de trabajo del administrador.

Kaspersky Security Center también la opción de instalación local de aplicaciones con un paquete de instalación independiente. Kaspersky Security Center no admite la instalación de todas las aplicaciones de Kaspersky.

Instalación local del Agente de red

Para instalar el Agente de red en un dispositivo localmente:

1. En el dispositivo, ejecute el archivo setup.exe desde el paquete de distribución descargado de Internet.

   Se abre una ventana que le solicita que seleccione las aplicaciones Kaspersky que desea instalar.

2. En la ventana de selección de aplicación, haga clic en el enlace **Instalar solo el Agente de red de Kaspersky Security Center 14** para iniciar el Asistente de instalación del Agente de red. Siga las instrucciones del Asistente.

   Mientras se ejecuta el Asistente de instalación, puede especificar la configuración avanzada del Agente de red (consulte a continuación).

3. Si quiere utilizar el dispositivo como la puerta de enlace de conexión de un grupo de administración específico, en la ventana **Puerta de enlace de conexión** del Asistente de instalación, seleccione **Usar el Agente de red como puerta de enlace de conexión en DMZ**.

4. Para configurar el Agente de red durante la instalación en una máquina virtual:

   a. Si planea crear máquinas virtuales dinámicas desde la imagen de la máquina virtual, active el modo dinámico del Agente de red para la infraestructura de escritorio virtual (VDI). Para ello, en la ventana **Configuración avanzada** del Asistente de instalación, seleccione la opción **Activar modo dinámico para VDI**.

      Omita este paso si no va a crear máquinas virtuales dinámicas a partir de la imagen de la máquina virtual.

      El uso del modo dinámico para VDI está disponible solo para dispositivos que ejecutan Windows.

   b. Optimice la operación del Agente de red para VDI. Para ello, en la ventana **Configuración avanzada** del Asistente de instalación, seleccione la opción **Optimizar la configuración de Agente de red de Kaspersky Security Center para la infraestructura de virtual**.

      Se desactivará el análisis de los archivos ejecutables para buscar vulnerabilidades al iniciarse el dispositivo. Además, esto deshabilita el envío de información sobre los objetos siguientes al Servidor de administración:

      - Registro de hardware
      - Aplicaciones instaladas en el dispositivo
      - Actualizaciones de Microsoft Windows que se deben instalar en el dispositivo cliente local
      - Vulnerabilidades de software detectadas en el dispositivo cliente local

      Además, podrá habilitar el envío de esta información en las propiedades del Agente de red o en la configuración de la directiva del Agente de red.

Cuando el Asistente de instalación se completa, el Agente de red se instala en el dispositivo.

Puede ver las propiedades del servicio del Agente de red de Kaspersky Security Center; también puede iniciar, detener y supervisar la actividad del Agente de red mediante las herramientas estándar de Microsoft Windows: Administración de equipos \ Servicios.

Instalación del Agente de red en modo no interactivo (silencioso)

El Agente de red se puede instalar en modo silencioso; es decir, sin la introducción interactiva de los parámetros de instalación. La instalación no interactiva usa un paquete de Windows Installer (MSI) para el Agente de red. El archivo MSI se encuentra en el paquete de distribución de Kaspersky Security Center, en la carpeta Packages\NetAgent\exec.

Para instalar el Agente de red en un dispositivo local en modo no interactivo:

1. Lea el Contrato de licencia de usuario final. Utilice el siguiente comando solo si comprende y acepta las condiciones del Contrato de licencia de usuario final.

2. Ejecute el comando
   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```
   donde `setup_parameters` es una lista de parámetros de configuración y sus respectivos valores separados por espacios (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   En la lista de parámetros, debe incluir `EULA=1`. De lo contrario, el Agente de red no se instalará.

Si está utilizando la configuración de conexión estándar para Kaspersky Security Center 11 y versiones posteriores, y el Agente de red en dispositivos remotos, ejecute el comando:

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

`/l*vx` es la clave para escribir registros. El registro se crea durante la instalación del Agente de red y se guarda en C:\windows\temp\nag_inst.log.

Además de nag_inst.log, la aplicación crea el archivo $klssinstlib.log, que contiene el registro de instalación. Este archivo se almacena en la carpeta %windir%\temp or %temp% folder. Para solucionar problemas, es posible que usted o un especialista del Servicio de soporte técnico de Kaspersky necesiten los dos archivos de registro: nag_inst.log y $klssinstlib.log.

Si necesita especificar adicionalmente el puerto para la conexión al Servidor de administración, ejecute el comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

El parámetro `SERVERPORT` corresponde al número de puertos para la conexión al Servidor de administración.

Los nombres y los valores posibles para los parámetros que se pueden usar al instalar el Agente de red en modo no interactivo se enumeran en la sección de parámetros de instalación del Agente de red.

Instalación de Agente de red para Linux en modo silencioso (con un archivo de respuestas)

Puede instalar Agente de red en dispositivos Linux utilizando un archivo de respuestas, que es un archivo de texto que contiene un conjunto personalizado de parámetros de instalación: variables y sus respectivos valores. El uso de este archivo de respuestas le permite ejecutar una instalación en modo silencioso (no interactivo), es decir, sin la participación del usuario.

Para instalar Agente de red para Linux en modo silencioso:

1. Prepare el dispositivo Linux correspondiente para la instalación remota. Descargue y cree el paquete de instalación remota, utilizando un paquete .deb o .rpm de Agente de red, mediante un sistema de administración de paquetes apropiado.

2. Si desea instalar Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, instale el paquete insserv-compat primero para configurar el Agente de red.

3. Lea el Contrato de licencia de usuario final. Siga los siguientes pasos solo si comprende y acepta las condiciones del Contrato de licencia de usuario final.

4. Establezca el valor de la variable de entorno KLAUTOANSWERS ingresando el nombre completo del archivo de respuestas (incluida la ruta), por ejemplo, de la siguiente manera:

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

5. Cree el archivo de respuestas (en formato TXT) en el directorio que ha especificado en la variable de entorno. Añada al archivo de respuestas una lista de variables en formato VARIABLE_NAME=variable_value, cada una en una línea separada.

   Para el uso correcto del archivo de respuestas, debe incluir en él un conjunto mínimo de las tres variables requeridas:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   También puede añadir cualquier variable opcional para usar parámetros más específicos de su instalación remota. La siguiente tabla enumera todas las variables que se pueden incluir en el archivo de respuesta:

   Variables del archivo de respuestas utilizadas como parámetros de instalación de Agente de red para Linux en modo silencioso

Variables del archivo de respuestas utilizadas como parámetros de instalación de Agente de red para Linux en modo silencioso

Nombre de la variable	Necesario	Descripción	Valores posibles
KLNAGENT_SERVER	Sí	Contiene el nombre del Servidor de administración presentado como nombre de dominio completo (FQDN) o dirección IP.	Nombre de DNS o dirección IP
KLNAGENT_AUTOINSTALL	Sí	Define si el modo de instalación silenciosa (no interactiva) está habilitado.	1: el modo silencioso está habilitado; no se le solicita al usuario ninguna acción durante la instalación. Otro: el modo silencioso está desactivado; se le pueden solicitar al usuario acciones durante la instalación.
EULA_ACCEPTED	Sí	Define si el usuario acepta el Contrato de licencia de usuario final (EULA) del Agente de red; si no está presente, puede interpretarse como la no aceptación del EULA.	1: Confirmo que he leído, y entiendo y acepto los términos y condiciones de este Contrato de licencia de usuario final. Otro o no especificado: No acepto los términos del Contrato de licencia (no se realiza la instalación).
KLNAGENT_PROXY_USE	No	Define si la conexión con el Servidor de administración utilizará la configuración del proxy. El valor predeterminado es 0.	1: se utiliza la configuración del proxy. Otro: no se utiliza la configuración del proxy.
KLNAGENT_PROXY_ADDR	No	Define la dirección del servidor proxy utilizado para la conexión con el Servidor de administración.	Nombre de DNS o dirección IP
KLNAGENT_PROXY_LOGIN	No	Define el nombre de usuario utilizado para iniciar sesión en el servidor proxy.	Cualquier nombre de usuario existente.
KLNAGENT_PROXY_PASSWORD	No	Define la contraseña del usuario utilizado para iniciar sesión en el servidor proxy.	Cualquier conjunto de caracteres alfanuméricos permitidos por el

			formato de contraseña en el sistema operativo.
KLNAGENT_VM_VDI	No	Define si el Agente de red está instalado en una imagen para la creación de máquinas virtuales dinámicas.	1: el Agente de red se instala en una imagen, que posteriormente se utiliza para la creación de máquinas virtuales dinámicas. Otro: no se utiliza ninguna imagen durante la instalación.
KLNAGENT_VM_OPTIMIZE	No	Define si la configuración del Agente de red es óptima para el hipervisor.	1: la configuración local predeterminada del Agente de red se modifica para permitir el uso optimizado en el hipervisor.
KLNAGENT_TAGS	No	Enumera las etiquetas asignadas a la instancia del Agente de red.	Uno o varios nombres de etiqueta separados por punto y coma.
KLNAGENT_UDP_PORT	No	Define el puerto UDP utilizado por el Agente de red. El valor predeterminado es 15000.	Cualquier número de puerto existente.
KLNAGENT_PORT	No	Define el puerto no TLS utilizado por el Agente de red. El valor predeterminado es 14000.	Cualquier número de puerto existente.
KLNAGENT_SSLPORT	No	Define el puerto TLS utilizado por el Agente de red. El valor predeterminado es 13000.	Cualquier número de puerto existente.
KLNAGENT_USESSL	No	Define si la Seguridad de la capa de transporte (TLS, Transport Layer Security) se usa para la conexión.	1 (predeterminado): se utiliza TLS. Otro: no se utiliza TLS.
KLNAGENT_GW_MODE	No	Define si se usa la puerta de enlace de conexión.	1 (predeterminado): la configuración actual no se modifica (en la primera llamada, no se especifica una puerta de enlace de conexión).

			2: no se utiliza la puerta de enlace de conexión. 3: se utiliza la puerta de enlace de conexión. 4: la instancia del Agente de red se utiliza como puerta de enlace de conexión en la zona desmilitarizada (DMZ).
KLNAGENT_GW_ADDRESS	No	Define la dirección de la puerta de enlace de conexión. El valor solo es aplicable si KLNAGENT_GW_MODE = 3.	Nombre de DNS o dirección IP

6. Ejecute el script postinstall.pl ejecutando el siguiente comando:

   - Para un sistema operativo de 32 bits: `$ sudo /opt/kaspersky/klnagent/lib/bin/setup/postinstall.pl`
   - Para un sistema operativo de 64 bits: `$ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`

La instalación de Agente de red para Linux comienza en modo silencioso; No se le solicita al usuario ninguna acción durante el proceso.

Instalación local del complemento de administración de aplicaciones

Para instalar el complemento de administración de aplicaciones, siga estos pasos:

En un dispositivo con la Consola de administración instalada, ejecute el archivo klcfginst.exe, que se incluye en el paquete de distribución de aplicaciones.

El archivo klcfginst.exe se incluye en todas las aplicaciones que se pueden administrar mediante Kaspersky Security Center. La instalación se facilita con el Asistente y no requiere la configuración manual de los parámetros.

Instalación de aplicaciones en modo silencioso

Para instalar una aplicación en modo silencioso:

1. Abra la ventana principal de la aplicación de Kaspersky Security Center.
2. En la carpeta **Instalación remota** del árbol de consola, abra la subcarpeta **Paquetes de instalación** y seleccione el paquete de instalación de la aplicación pertinente o cree un paquete de instalación nuevo para esta aplicación.

El paquete de instalación se almacenará en el Servidor de administración en la carpeta de servicio Paquetes dentro de la carpeta compartida. Una subcarpeta por separado corresponde a cada paquete de instalación.

3. Abra la carpeta del paquete de instalación requerido de una de las siguientes formas:

   - Copie la carpeta correspondiente al paquete de instalación relevante desde el Servidor de administración al dispositivo cliente. A continuación abra la carpeta copiada en el dispositivo cliente.
   - Abra desde el dispositivo cliente la carpeta compartida correspondiente al paquete de instalación requerido en el Servidor de administración.

Si la carpeta compartida está ubicada en un dispositivo que ejecuta Microsoft Windows Vista, seleccione el valor **Desactivado** para el parámetro **Control de cuentas de usuario: ejecutar todos los administradores en Modo de aprobación de administrador** (**Inicio** → **Panel de control** → **Administración** → **Directiva de seguridad local** → **Configuración de seguridad**).

4. Según la aplicación seleccionada, realice las siguientes acciones:

   - En el caso de Kaspersky Anti-Virus for Windows Workstation, Kaspersky Anti-Virus for Windows Servers y Kaspersky Security Center, abra la subcarpeta exec e inicie el archivo ejecutable (un archivo con la extensión .exe) con la clave /s.
   - En el caso de otras aplicaciones Kaspersky, inicie el archivo ejecutable (un archivo con la extensión .exe) con la clave /s en la carpeta abierta.

La ejecución del archivo con las claves `EULA=1` y `PRIVACYPOLICY=1` significa que ha leído, entendido y acepta las condiciones del Contrato de licencia de usuario final y la Política de privacidad respectivamente. También entiende que sus datos serán manejados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad. El texto del Contrato de licencia y la Política de privacidad se incluye en el kit de distribución de Kaspersky Security Center. Se requiere la aceptación de las condiciones del Contrato de licencia y de la Política de privacidad para instalar o actualizar una versión anterior de la aplicación.

Instalación de software con paquetes independientes

Kaspersky Security Center permite crear paquetes de instalación independientes para las aplicaciones. Un paquete de instalación independiente es un archivo ejecutable que se encuentra en un servidor web, se envía por correo electrónico o se transfiere al dispositivo cliente de otra manera. Este archivo recibido se puede ejecutar de manera local en el dispositivo cliente para instalar una aplicación sin implicar a Kaspersky Security Center.

Para instalar una aplicación con el paquete de instalación independiente:

1. Conéctese al Servidor de administración necesario.
2. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
3. En el espacio de trabajo, seleccione el paquete de instalación de la aplicación requerida.
4. Inicie el proceso de creación de un paquete de instalación independiente mediante una de las siguientes formas:

- Seleccionando **Crear un paquete de instalación independiente** en el menú contextual del paquete de instalación.
- Haga clic en el enlace **Crear un paquete de instalación independiente** en el espacio de trabajo del paquete de instalación.

Se inicia el Asistente para crear paquete de instalación independiente. Siga las instrucciones del Asistente.

En el paso final del Asistente, seleccione un método para transmitir el paquete de instalación independiente a un dispositivo cliente.

5. Transmita el paquete de instalación independiente al dispositivo cliente.
6. Ejecute el paquete de instalación independiente en el dispositivo cliente.

Como resultado, la aplicación se instala ahora en el dispositivo cliente con la configuración especificada en el paquete independiente.

Al crear un paquete de instalación independiente, se publica automáticamente en el Servidor Web. El enlace para descargar el paquete independiente se muestra en la lista de paquetes de instalación independiente creados. Si es necesario, puede cancelar la publicación del paquete independiente y volver a publicarlo en el Servidor web. De forma predeterminada, se utiliza el puerto 8060 para descargar paquetes de instalación independientes.

Configuración del paquete de instalación del Agente de red

Para configurar un paquete de instalación del Agente de red, haga lo siguiente:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.

   La carpeta **Instalación remota** es una subcarpeta de la carpeta predeterminada **Avanzado**.
2. En el menú contextual del paquete de instalación del Agente de red, seleccione **Propiedades**.

Se abre la ventana de propiedades del paquete de instalación del Agente de red.

General

La sección **General** muestra información general sobre el paquete de instalación:

- Nombre del paquete de instalación
- Nombre y versión de la aplicación para la que se ha creado el paquete de instalación
- Tamaño del paquete de instalación
- Fecha de creación del paquete de instalación
- Ruta a la carpeta del paquete de instalación

Configuración

Esta sección muestra los parámetros requeridos para asegurar el correcto funcionamiento del Agente de red inmediatamente después de su instalación. La configuración en esta sección está disponible solo en dispositivos que ejecutan Windows.

En el grupo de configuración de la **Carpeta de destino**, puede seleccionar la carpeta del dispositivo cliente en la cual se instalará el Agente de red.

- **Instalar en la carpeta predeterminada**

  Si se selecciona esta opción, el Agente de red se instalará en la carpeta <Unidad de disco>:\Archivos de programa\Kaspersky Lab\NetworkAgent. Si esta carpeta no existe, el programa la creará automáticamente.

  Esta opción está seleccionada de forma predeterminada.

- **Instalar en la carpeta especificada**

  Si se selecciona esta opción, el Agente de red se instalará en la carpeta especificada en el campo de entrada.

En el siguiente grupo de configuración, puede especificar una contraseña para una tarea de desinstalación remota del Agente de red:

- **Utilizar contraseña de desinstalación**

  Si se selecciona esta opción, al hacer clic en el botón **Modificar** puede introducir la contraseña de desinstalación (solo disponible para el Agente de red en dispositivos con sistemas operativos Windows).

  Esta opción está desactivada de forma predeterminada.

- **Estado**

  Estado de la contraseña: **Contraseña establecida** o **Contraseña no establecida**.

  De forma predeterminada, la contraseña no está instalada.

- **Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración**

  Una vez que el Agente de red se instala en un dispositivo administrado, el componente no se puede eliminar ni reconfigurar sin los privilegios necesarios. El servicio del Agente de red no se puede detener.

  Esta opción está desactivada de forma predeterminada.

- **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir**

  Si esta opción está seleccionada, todas las actualizaciones y los parches descargados para el Servidor de administración, el Agente de red, la Consola de administración, el Servidor de dispositivos móviles de Exchange y el Servidor de MDM para iOS se instalarán automáticamente (la actualización automática y los parches solo están disponibles a partir de la versión Kaspersky Security Center 10 Service Pack 2).

  Si esta opción está desactivada, todas las actualizaciones y los parches descargados se instalarán únicamente después de que cambie su estado a *Aprobado*. Las actualizaciones y los parches con el estado *Sin definir* no se instalarán.

  Esta opción está activada de forma predeterminada.

Conexión

En esta sección, puede configurar la conexión del Agente de red al Servidor de administración:

En esta sección, puede configurar la conexión del Agente de red al Servidor de administración. Para establecer una conexión, puede utilizar el protocolo SSL o UDP. Para configurar la conexión, especifique los siguientes parámetros:

- **Servidor de administración**

  Dirección del nodo con el Servidor de administración instalado.

- **Puerto**

  Número de puerto que se utiliza en la conexión.

- **Puerto SSL**

  Número de puerto que se utiliza para la conectar con el protocolo SSL.

- **Utilizar certificado de servidor**

  Si esta opción está activada, la autenticación del acceso del Agente de red al Servidor de administración usará el archivo del certificado que puede especificar haciendo clic en el botón **Examinar**.

  Si esta opción está desactivada, el archivo del certificado se recibirá del Servidor de administración en la primera conexión del Agente de red a la dirección especificada en el campo **Dirección del servidor**.

  No recomendamos desactivar esta opción, porque la recepción automática de un certificado de Servidor de administración por parte del Agente de red al conectarse al Servidor de administración no se considera segura.

  De forma predeterminada, esta casilla está seleccionada.

- **Utilizar SSL**

  Si esta opción está activada, la conexión al Servidor de administración se establece a través de un puerto seguro a través de SSL.

  Esta opción está desactivada de forma predeterminada. Le recomendamos que no desactive esta opción para que su conexión siga siendo segura.

- **Usar puerto UDP**

  Si esta opción está activada, el Agente de red se conecta al Servidor de administración a través de un puerto UDP. Esto permite administrar los dispositivos cliente y recibir información sobre ellos.

  El puerto UDP debe estar abierto en los dispositivos administrados donde está instalado el Agente de red. Por lo tanto, le recomendamos que no desactive esta opción.

  Esta opción está activada de forma predeterminada.

- **Número de puerto UDP**

En este campo, puede especificar el puerto para conectar el Agente de red al Servidor de administración a través del protocolo UDP.

El puerto UDP predeterminado es el 15000.

- **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**

  Si se selecciona esta opción, después de instalar el Agente de red en el dispositivo cliente, se agregará un puerto UDP a la lista de exclusiones de firewall de Microsoft Windows. El puerto UDP es necesario para que el Agente de red se ejecute correctamente.

  Esta opción está activada de forma predeterminada.

Avanzado

En la sección **Opciones avanzadas**, puede configurar cómo usar la puerta de enlace de conexión. Para ello, puede hacer lo siguiente:

- Utilice el Agente de red como puerta de enlace de conexión en la zona desmilitarizada (DMZ) para conectarse al Servidor de administración, comunicarse con él y mantener seguros los datos en el Agente de red durante la transmisión de datos.
- Conéctese al Servidor de administración mediante una puerta de enlace de conexión para reducir la cantidad de conexiones al Servidor de administración. En este caso, introduzca la dirección del dispositivo que actuará como puerta de enlace de conexión en el campo **Dirección de la puerta de enlace de conexión**.
- Configure la conexión para la infraestructura de escritorio virtual (VDI) si su red incluye máquinas virtuales. Para ello, haga lo siguiente:
  - **Activar modo dinámico para VDI**

    Si se selecciona esta opción, el modo dinámico para la infraestructura de escritorio virtual (VDI) se activará para el Agente de red instalado en la máquina virtual.

    Esta opción está desactivada de forma predeterminada.

  - **Optimizar la configuración para VDI**

    Si se selecciona esta opción, se desactiva las siguientes funciones en la configuración del Agente de red:

    - Recuperación de información sobre el software instalado.
    - Recuperación de información sobre el hardware.
    - Recuperación de información sobre las vulnerabilidades detectadas.
    - Recuperación de información sobre las actualizaciones requeridas.

      Esta opción está desactivada de forma predeterminada.

Componentes adicionales

En esta sección, puede seleccionar componentes adicionales para la instalación simultánea con el Agente de red.

Etiquetas

La sección **Etiquetas** muestra una lista de palabras claves (etiquetas) que se pueden agregar a los dispositivos cliente una vez instalado el Agente de red. Puede agregar etiquetas a la lista y quitarlas, así como cambiarles el nombre.

Si se selecciona la casilla al lado de una etiqueta, esta etiqueta automáticamente se añade a los dispositivos administrados durante la instalación del Agente de red.

Si la casilla se desactiva al lado de una etiqueta, la etiqueta no se agregará automáticamente a los dispositivos administrados durante la instalación del Agente de red. Puede agregar manualmente esta etiqueta a dispositivos.

Al eliminar una etiqueta de la lista, esta se elimina automáticamente de todos los dispositivos a los cuales se haya añadido.

Historial de revisión

En esta sección puede ver el historial de revisiones del paquete de instalación. Puede comparar revisiones, ver revisiones, guardar revisiones de un archivo y agregar y modificar descripciones de la revisión.

La configuración del paquete de instalación del Agente de red disponible para un sistema operativo específico se encuentra en la tabla a continuación.

Configuración del paquete de instalación del Agente de red

Sección Propiedad	Windows	Mac	Linux
General	✓	✓	✓
Configuración	✓	–	–
Conexión	✓	✓ (excepto para las opciones **Abrir puertos del Agente de red en el Firewall de Microsoft Windows** y **Utilizar solo detección automática de servidor proxy**)	✓ (excepto para las opciones **Abrir puertos del Agente de red en el Firewall de Microsoft Windows** y **Utilizar solo detección automática de servidor proxy**)
Avanzado	✓	✓	✓
Componentes adicionales	✓	✓	✓
Etiquetas	✓	✓ (excepto las reglas de etiquetado automático)	✓ (excepto las reglas de etiquetado automático)
Historial de revisiones	✓	✓	✓

Consulta de la Política de privacidad

La Política de privacidad está disponible en línea en https://www.kaspersky.com/products-and-services-privacy-policy, y también está disponible sin conexión. Tiene la posibilidad de leer la Política de privacidad, por ejemplo, antes de instalar Agente de red.

Para leer la Política de privacidad, si no tiene conexión a Internet:

1. Inicie la instalación de Kaspersky Security Center.
2. En la ventana del instalador, vaya al enlace **Extraer paquetes de instalación**.
3. En la lista que se abre, seleccione Agente de red de Kaspersky Security Center 14 y luego haga clic en **Siguiente**.

El archivo privacy_policy.txt aparece en su dispositivo, en la carpeta que especificó, en la subcarpeta NetAgent_<versión actual>.

Despliegue de sistemas de administración de dispositivos móviles

Esta sección describe el despliegue de sistemas de administración de dispositivos móviles mediante Exchange ActiveSync, MDM de iOS y los protocolos de Kaspersky Endpoint Security.

Despliegue de un sistema para administrarlo mediante el protocolo Exchange ActiveSync

Kaspersky Security Center le permite administrar dispositivos móviles que están conectados al Servidor de administración mediante el protocolo Exchange ActiveSync. Los dispositivos móviles de Exchange ActiveSync (EAS) son aquellos que se conectan a un servidor de dispositivos móviles de Exchange y se administran mediante un Servidor de administración.

Los sistemas operativos siguientes admiten el protocolo de Exchange ActiveSync:

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

El conjunto de parámetros de administración para un dispositivo Exchange ActiveSync depende del sistema operativo bajo el que se ejecuta el dispositivo móvil. Para obtener detalles sobre las características de compatibilidad del protocolo Exchange ActiveSync para un sistema operativo específico, consulte la documentación incluida con el sistema operativo.

El despliegue de un sistema de administración de dispositivos móviles con el protocolo Exchange ActiveSync consta de los siguientes pasos:

1. El administrador instala el servidor de dispositivos móviles de Exchange en el dispositivo cliente seleccionado.
2. El administrador crea perfiles de administración en la Consola de administración para administrar dispositivos EAS y agrega los perfiles a los buzones de correo de los usuarios de Exchange ActiveSync.

El *Perfil de administración de dispositivos móviles de Exchange ActiveSync* es una directiva de ActiveSync que se usa en un servidor Microsoft Exchange Server para administrar dispositivos móviles de Exchange ActiveSync. Solo se puede asignar un perfil de administración de dispositivos EAS a un buzón de correo de Microsoft Exchange.

Los usuarios de dispositivos móviles EAS se conectan a sus buzones de correo de Exchange. Cualquier perfil de la administración impone algunas restricciones a los dispositivos móviles.

Instalación de un servidor de dispositivos móviles para Exchange ActiveSync

Un Servidor de dispositivos móviles Exchange se instala en un dispositivo cliente con un servidor Microsoft Exchange instalado. Se recomienda instalar el Servidor de dispositivos móviles Exchange en un servidor Microsoft Exchange con la función Client Access asignada. Si hay varios servidores de Microsoft Exchange con la función Acceso de cliente en el mismo dominio combinados en la matriz de acceso de cliente, se recomienda instalar el Servidor de dispositivos móviles Exchange en cada servidor Microsoft Exchange de dicha matriz en modo de clúster.

Para instalar un Servidor de dispositivos móviles Exchange en un dispositivo local, siga estos pasos:

1. Ejecute el archivo ejecutable setup.exe.

   Se abre una ventana que le solicita que seleccione las aplicaciones Kaspersky que desea instalar.

2. En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar servidor de dispositivos móviles de Exchange** para ejecutar el Asistente de instalación del Servidor de dispositivos móviles Exchange.

3. En la ventana **Configuración de la instalación**, seleccione el tipo de instalación del servidor de dispositivos móviles de Exchange:

   - Para instalar el Servidor de dispositivos móviles Exchange con la configuración predeterminada, seleccione **Instalación estándar** y haga clic en el botón **Siguiente**.

   - Para configurar manualmente el Servidor de dispositivos móviles Exchange, seleccione **Instalación personalizada** y haga clic en el botón **Siguiente**. A continuación, realice lo siguiente:

     a. Seleccione la carpeta de destino en la ventana **Carpeta de destino**. La carpeta predeterminada es <Unidad de disco>:\Archivos de programa\Kaspersky Lab\Administración de dispositivos móviles para Exchange. Si la carpeta no existe, se crea automáticamente durante la instalación. Puede cambiar la carpeta de destino con el botón **Examinar**.

     b. Elija el modo de instalación (normal o clúster) del Servidor de dispositivos móviles de Exchange en la ventana **Modo de instalación**.

     c. En la ventana **Seleccionar cuenta**, seleccione una cuenta que se utilizará para administrar los dispositivos móviles:

        - **Crear cuenta y grupo de roles automáticamente**. La cuenta se creará automáticamente.

        - **Especificar una cuenta**. La cuenta se debe seleccionar manualmente. Haga clic en el botón **Examinar** para seleccionar la cuenta de usuario y especificar la contraseña. El usuario seleccionado debe pertenecer a un grupo con derechos para administrar dispositivos móviles usando ActiveSync.

     d. En la ventana **Configuración de IIS**, permita o prohíba la configuración automática de las propiedades del servidor web de Internet Information Services (IIS).

Si ha prohibido la configuración automática de las propiedades de Internet Information Services (IIS), active el mecanismo de autenticación de Windows manualmente en la configuración de IIS para el directorio virtual de Microsoft PowerShell. Si se desactiva el mecanismo de autenticación de Windows, el Servidor de dispositivos móviles Exchange no funcionará correctamente. Consulte la documentación de IIS para obtener más información sobre cómo configurar IIS.

e. Haga clic en **Siguiente**.

4. En la ventana que se abre, verifique las propiedades de instalación del Servidor de dispositivos móviles Exchange y haga clic en **Instalar**.

Cuando el Asistente finalice, el Servidor de dispositivos móviles Exchange habrá quedado instalado en el dispositivo local. El Servidor de dispositivos móviles de Exchange se mostrará en la carpeta **Administración de dispositivos móviles** del árbol de consola.

Conexión de dispositivos móviles a un Servidor de dispositivos móviles Exchange

Antes de conectar cualquier dispositivo móvil, debe configurar Microsoft Exchange Server para permitir que los dispositivos se conecten mediante el protocolo ActiveSync.

Para conectar un dispositivo móvil a un Servidor de dispositivos móviles Exchange, el usuario se conecta a su buzón de correo de Microsoft Exchange desde el dispositivo móvil mediante ActiveSync. Cuando se conecte, el usuario debe configurar la conexión en el cliente de ActiveSync e indicar datos tales como la dirección y la contraseña de la cuenta de correo electrónico.

El dispositivo móvil del usuario conectado al servidor Microsoft Exchange se muestra en la subcarpeta **Dispositivos móviles** que se encuentra en la carpeta **Administración de dispositivos móviles** del árbol de consola.

Después de conectar el dispositivo móvil de Exchange ActiveSync con el Servidor de dispositivos móviles Microsoft Exchange, el administrador puede administrar el dispositivo móvil Exchange ActiveSync conectado.

Configuración del servidor web de Internet Information Services

Al usar Microsoft Exchange Server (versiones 2010 y 2013), debe activar el mecanismo de autenticación de Windows para un directorio virtual de Windows PowerShell™ en la configuración del servidor web de Internet Information Services (IIS). Este mecanismo de autenticación se activa automáticamente si la opción **Configurar Microsoft Internet Information Services (IIS) automáticamente** está seleccionada en el Asistente de instalación del Servidor de dispositivos móviles de Exchange (opción predeterminada).

De lo contrario, deberá activar el mecanismo de autenticación por su cuenta.

Para activar el mecanismo de autenticación de Windows para un directorio virtual de PowerShell manualmente:

1. En la consola de Administrador de Internet Information Services (IIS), abra las propiedades del directorio virtual de PowerShell.

2. Vaya a la sección **Autenticación**.

3. Seleccione **Autenticación de Windows** y luego haga clic en el botón **Activar**.

4. Abra **Configuración avanzada**.

5. Seleccione la opción **Activar la autenticación en modo Kernel**.

6. En la lista desplegable **Ampliar la protección**, seleccione **Requerido**.

Cuando se utiliza Microsoft Exchange Server 2007, el servidor web de IIS no requiere ninguna configuración.

Instalación local de un Servidor de dispositivos móviles de Exchange

Para una instalación local de un Servidor de dispositivos móviles de Exchange, el administrador debe realizar las operaciones siguientes:

1. Copie el contenido de la carpeta \Server\Packages\MDM4Exchange\ del paquete de distribución de Kaspersky Security Center a un dispositivo cliente.

2. Ejecute el archivo ejecutable setup.exe.

La instalación local incluye dos tipos de instalación:

- La instalación estándar es una instalación simplificada que no requiere que el administrador defina ninguna configuración; se recomienda en la mayoría de los casos.

- La instalación extendida es una instalación que requiere que el administrador defina la configuración siguiente:

  - La ruta para la instalación del Servidor de dispositivos móviles de Exchange.

  - El modo de operación del Servidor de dispositivos móviles de Exchange: modo estándar o modo del clúster.

  - La posibilidad de especificar la cuenta en la cual se ejecutará el servicio del Servidor de dispositivos móviles de Exchange.

  - La activación/desactivación de la configuración automática del servidor web de IIS.

El Asistente de instalación del Servidor de Dispositivos móviles de Exchange se debe ejecutar bajo una cuenta que tiene todos los derechos requeridos.

Instalación remota de un Servidor de dispositivos móviles de Exchange

Para configurar la instalación remota de un Servidor de dispositivos móviles de Exchange, el administrador debe realizar las siguientes acciones:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Instalación remota**, a continuación, la subcarpeta **Paquetes de instalación**.

2. En la subcarpeta **Paquetes de instalación**, abra las propiedades del paquete del **Servidor de dispositivos móviles de Exchange**.

3. Vaya a la sección **Configuración**.

   Esta sección contiene la misma configuración que la utilizada para la instalación local de la aplicación.

Después de que se configura la instalación remota, puede empezar a instalar el Servidor de dispositivos móviles de Exchange.

Para instalar un Servidor de dispositivos móviles de Exchange:

1. En el árbol de la Consola de administración de Kaspersky Security Center, seleccione la carpeta **Instalación remota**, a continuación, la subcarpeta **Paquetes de instalación**.

2. En la subcarpeta **Paquetes de instalación**, seleccione el paquete del **Servidor de dispositivos móviles de Exchange**.

3. Abra el menú contextual del paquete y seleccione **Instalar aplicación**.

4. En el Asistente de instalación remota que se abre, seleccione un dispositivo (o varios dispositivos para la instalación en el modo de clúster).

5. En el campo **Ejecutar el Asistente de instalación de la aplicación con la cuenta especificada**, especifique la cuenta en la cual se ejecutará el proceso de instalación en el dispositivo remoto.

   La cuenta debe tener los derechos requeridos.

Despliegue de un sistema para administración mediante el protocolo MDM de iOS

Kaspersky Security Center permite administrar los dispositivos móviles en los que se ejecuta iOS. Los dispositivos MDM con iOS son dispositivos móviles iOS conectados a un Servidor de MDM para iOS y administrados mediante el Servidor de administración.

La conexión de dispositivos móviles a un Servidor de MDM para iOS se realiza en el siguiente orden:

1. El administrador instala el servidor de MDM para iOS en el dispositivo cliente seleccionado. La instalación del Servidor de MDM para iOS se realiza con las herramientas estándar del sistema operativo.

2. El administrador recibe un certificado de servicio de Apple Push Notification (APNs).

   El certificado de APNs permite al Servidor de administración conectarse al servidor APN para enviar notificaciones de inserción a dispositivos móviles MDM con iOS.

3. El administrador instala el certificado de APNs en el Servidor de MDM para iOS.

4. El administrador crea un perfil de MDM para iOS para el usuario del dispositivo móvil iOS.

   El perfil de MDM para iOS contiene una colección de parámetros para la conexión de dispositivos móviles iOS al Servidor de administración.

5. El administrador emite un certificado compartido para el usuario.

   Se precisa el certificado compartido para confirmar que el dispositivo móvil es propiedad del usuario.

6. El usuario hace clic en el enlace que ha enviado el administrador y descarga un paquete de instalación en el dispositivo móvil.

   El paquete de instalación contiene un certificado y un perfil de MDM para iOS.

   Cuando el perfil de MDM para iOS se haya descargado y el dispositivo con MDM de iOS se haya sincronizado con el Servidor de administración, el dispositivo se mostrará en **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de consola.

7. El administrador agrega un perfil de configuración al Servidor de MDM para iOS y lo instala en el dispositivo móvil después de que éste se conecta.

   El perfil de configuración contiene una colección de parámetros y restricciones para el dispositivo con MDM de iOS; por ejemplo, los parámetros de la instalación de aplicaciones, la configuración para el uso de las distintas funciones del dispositivo y la configuración correo electrónico y programación. Un perfil de configuración permite configurar los dispositivos móviles MDM con iOS de acuerdo con las directivas de seguridad de la organización.

8. Si es necesario, el administrador agrega perfiles de aprovisionamiento al Servidor de MDM para iOS y después instala dichos perfiles en los dispositivos móviles.

   El *Perfil de aprovisionamiento* es un perfil que se usa para administrar las aplicaciones distribuidas de distintas maneras, salvo a través de la App Store®. Un perfil de aprovisionamiento contiene información sobre la licencia y está vinculado a una aplicación específica.

Instalar el servidor de MDM para iOS

Para instalar el Servidor de MDM para iOS en un dispositivo local, siga estos pasos:

1. Ejecute el archivo ejecutable setup.exe.

   Se abre una ventana que le solicita que seleccione las aplicaciones Kaspersky que desea instalar.

   En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar el servidor de MDM para iOS** para iniciar el Asistente de instalación del Servidor de MDM para iOS.

2. Seleccionar la carpeta de destino.

   La carpeta de destino predeterminada es <Unidad de disco>:\Archivos de programa\Kaspersky Lab\Administración de dispositivos móviles para iOS. Si la carpeta no existe, se crea automáticamente durante la instalación. Puede cambiar la carpeta de destino con el botón **Examinar**.

3. En la ventana **Especifique los ajustes de conexión con el servidor de MDM para iOS** del Asistente, en el campo **Puerto externo para conectar con el servicio MDM de iOS**, especifique un puerto externo para la conexión de dispositivos móviles al servicio de MDM de iOS.

   El puerto externo 5223 se utiliza para que los dispositivos móviles se comuniquen con el servidor de APNs. Asegúrese de que el puerto 5223 está abierto en el firewall para que se conecte con el intervalo de direcciones 17.0.0.0/8.

   El Puerto 443 se utiliza para la conexión con el Servidor de MDM para iOS de forma predeterminada. Si otro servicio u otra aplicación están utilizando ya el puerto 443, puede sustituirlo por el puerto 9443, por ejemplo.

   El Servidor de MDM para iOS utiliza el puerto externo 2197 para enviar notificaciones al servidor de APNs.

   Los servidores APNs se ejecutan en modo de equilibrio de carga. Los dispositivos móviles no siempre se conectan a las mismas direcciones IP para recibir notificaciones. El intervalo de direcciones 17.0.0.0/8 está reservado para Apple, por lo que se recomienda especificar todo el intervalo como permitido en la configuración de Firewall.

4. Si desea configurar los puertos de interacción de los componentes de la aplicación manualmente, seleccione la opción **Definir puertos locales manualmente** y especifique los valores de los siguientes parámetros:

   - **Puerto para conectar con el Agente de red**. En este campo, especifique un puerto para la conexión del servicio de MDM de iOS con el Agente de red. El número de puerto predeterminado es el 9799.

   - **Puerto local para conectar con el servicio MDM de iOS**. En este campo, especifique un puerto local para la conexión del Agente de red con el servicio de MDM de iOS. El número de puerto predeterminado es el 9899.

   Se recomienda usar los valores predeterminados.

5. En la ventana **Dirección externa del Servidor de dispositivos móviles** del Asistente, en el campo **Dirección web para conexión remota con el Servidor de dispositivos móviles**, especifique la dirección del dispositivo cliente en el que se instalará el Servidor de MDM para iOS.

   Esta dirección se usa para la conexión de los dispositivos móviles administrados al servicio de MDM de iOS. Este dispositivo cliente debe estar disponible para la conexión de los dispositivos MDM con iOS.

Puede especificar la dirección de un dispositivo cliente en cualquiera de los formatos siguientes:

- FQDN del dispositivo (por ejemplo, mdm.example.com)
- Nombre NetBIOS del dispositivo
- Dirección IP del dispositivo

Evite agregar el esquema de URL y el número de puerto a la cadena de dirección: estos valores se agregarán automáticamente.

Cuando el Asistente finaliza la operación, el Servidor de MDM para iOS se instala en el dispositivo local. El Servidor de MDM para iOS se muestra en la carpeta **Administración de dispositivos móviles** del árbol de consola.

Instalación del Servidor de MDM para iOS en modo silencioso

Kaspersky Security Center le permite instalar el Servidor de MDM para iOS en un dispositivo local en modo no interactivo, es decir, sin ingresar de forma interactiva los ajustes de instalación.

Para instalar el Servidor de MDM para iOS en un dispositivo local en modo no interactivo:

1. Lea el Contrato de licencia de usuario final. Utilice el siguiente comando solo si comprende y acepta las condiciones del Contrato de licencia de usuario final.

2. Ejecute el siguiente comando:

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

   Donde `setup_parameters` es una lista de parámetros de configuración y sus respectivos valores separados por espacios (`PRO1=PROP1VAL PROP2=PROP2VAL`). El archivo setup.exe se ubica en la carpeta Servidor, que es parte del kit de distribución de Kaspersky Security Center.

Los nombres y valores posibles para los parámetros que se pueden utilizar al instalar el Servidor de MDM para iOS en modo silencioso se enumeran en la tabla a continuación. Los parámetros se puede especificar en cualquier orden conveniente.

Los parámetros de instalación del Servidor de MDM para iOS en modo no interactivo

Nombre del parámetro	Descripción del parámetro	Valores disponibles
EULA	Aceptación de las condiciones del Contrato de licencia de usuario final. Este parámetro es obligatorio.	• 1: He leído, y entiendo y acepto todas las condiciones del Contrato de licencia de usuario final. • Otro valor o sin valor: no acepto las condiciones del Contrato de licencia (no se realiza la instalación).
DONT_USE_ANSWER_FILE	Si usar o no un archivo XML con la configuración de instalación del Servidor de MDM para iOS.	• 1: No utilizar el archivo XML con los parámetros.

	El archivo de XML se incluye en el paquete de instalación o se almacena en el Servidor de administración. No tiene que especificar una ruta adicional para el archivo. Este parámetro es obligatorio.	• Otro valor o sin valor: utilizar el archivo de XML con los parámetros.
INSTALLDIR	Carpeta de instalación del Servidor de MDM para iOS. Este parámetro es opcional.	Valor de cadena, por ejemplo, `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	Puerto local para la conexión del servicio de MDM de iOS con el Agente de red. El número de puerto predeterminado es el 9799. Este parámetro es opcional.	Valor numérico.
LOCALSERVERPORT	Puerto local para la conexión del Agente de red con el servicio de MDM de iOS. El número de puerto predeterminado es el 9899. Este parámetro es opcional.	Valor numérico.
EXTERNALSERVERPORT	Puerto para conectar un dispositivo al Servidor de MDM para iOS. El número de puerto predeterminado es el 443. Este parámetro es opcional.	Valor numérico.
EXTERNAL_SERVER_URL	La dirección externa del dispositivo cliente en el cual el Servidor de MDM para iOS se debe instalar. Esta dirección se usa para la conexión de los dispositivos móviles administrados al servicio de MDM de iOS. El dispositivo cliente debe estar disponible para la conexión a través de MDM de iOS. La dirección no debe incluir el esquema de la URL y el número del puerto, ya que estos valores se agregarán automáticamente. Este parámetro es opcional.	• FQDN del dispositivo (por ejemplo, mdm.example.com) • Nombre NetBIOS del dispositivo • Dirección IP del dispositivo
WORKFOLDER	Carpeta de trabajo del Servidor de MDM para iOS. Si no se especifica ninguna carpeta de trabajo, los datos se escribirán en la carpeta predeterminada. Este parámetro es opcional.	Valor de cadena, por ejemplo, `WORKFOLDER=\"C:\work\"`
MTNCY	Uso del Servidor de MDM para iOS por varios Servidores virtuales. Este parámetro es opcional.	• 1: el Servidor de MDM para iOS será utilizado por varios Servidores de administración virtuales. • Otro valor o ningún valor: el Servidor de MDM para iOS

		no será utilizado por varios Servidores de administración virtuales.

Ejemplo:

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

Los parámetros de instalación del Servidor de MDM para iOS se detallan en la sección "Instalación del Servidor de MDM para iOS".

Escenarios de despliegue del Servidor de MDM para iOS

El número de copias del Servidor de MDM para iOS que se instalará puede seleccionarse según el hardware disponible o según el número total de dispositivos móviles abarcados.

Tenga en cuenta que el número máximo recomendado de dispositivos móviles para una sola instalación de Kaspersky Device Management for iOS es 50 000. A fin de reducir la carga, el conjunto completo de dispositivos puede distribuirse entre varios servidores que tengan instalado el Servidor de MDM para iOS.

La autenticación de los dispositivos iOS con MDM se realiza a través de certificados de usuario (cualquier perfil instalado en un dispositivo contiene el certificado del propietario del dispositivo). Por lo tanto, son posibles dos esquemas de despliegue para un Servidor de MDM para iOS:

- Esquema simplificado.
- Esquema de despliegue con la delegación limitada de Kerberos (KCD).

Esquema de despliegue simplificado

Al desplegar un Servidor de MDM para iOS según el esquema simplificado, los dispositivos móviles se conectan directamente al servicio web de MDM de iOS. En este caso, los certificados de usuario emitidos por el Servidor de administración solo se pueden aplicar a la autenticación de dispositivos. La integración con la infraestructura de clave pública (PKI) es imposible para los certificados de usuario.

Esquema de despliegue con la delegación limitada de Kerberos (KCD).

El esquema de despliegue con la delegación limitada de Kerberos (KCD) requiere que el Servidor de administración y el Servidor de MDM para iOS estén localizados en la intranet de la organización.

Este esquema de despliegue asegura lo siguiente:

- Integración con Microsoft Forefront TMG.
- Uso de KCD para la autenticación de dispositivos móviles.
- Integración con la PKI para aplicar certificados de usuario.

Al usar este esquema de despliegue, debe hacer lo siguiente:

- En la Consola de administración, en la configuración del servicio web de MDM de iOS, seleccione la casilla **Garantizar la compatibilidad con la delegación limitada de Kerberos**.
- Como con el certificado para el servicio web de MDM de iOS, especifique el certificado personalizado que se definió cuando se publicó el servicio web de MDM de iOS en TMG.
- Los certificados de usuario para los dispositivos iOS deben ser emitidos por la entidad de certificación (CA) del dominio. Si el dominio contiene varios CA raíz, los certificados de usuario deben ser emitidos por la CA que se especificó cuando se publicó el servicio web de MDM de iOS en TMG.

  Puede asegurarse de que el certificado de usuario cumpla con este requisito de la emisión de la CA con uno de los siguientes métodos:

  - Especifique el certificado de usuario en el Asistente para nuevo perfil de MDM para iOS y en el Asistente de instalación de certificados.
  - Integre el Servidor de administración con la PKI del dominio y defina la configuración correspondiente en las reglas para la emisión de certificados:

    1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
    2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el enlace **Configurar reglas de emisión de certificados** para abrir la ventana **Reglas de emisión de certificados**.
    3. En la sección **Integración con la PKI**, configure la integración con la infraestructura de clave pública.
    4. En la sección **Emisión de certificados móviles**, especifique el origen de los certificados.

A continuación, se especifica un ejemplo de la configuración de la delegación limitada de Kerberos (KCD) con las siguientes suposiciones:

- El servicio web de MDM de iOS se está ejecutando en el puerto 443.
- El nombre del dispositivo con TMG es tmg.mydom.local.
- El nombre del dispositivo con el servicio web de MDM de iOS es iosmdm.mydom.local.
- El nombre de la publicación externa del servicio web de MDM de iOS es iosmdm.mydom.global.

Nombre principal del servicio para http/iosmdm.mydom.local

En el dominio, debe registrar el nombre principal del servicio (SPN) para el dispositivo con el servicio web de MDM de iOS (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Configuración de las propiedades de dominio del dispositivo con TMG (tmg.mydom.local)

Para delegar el tráfico, confíe al dispositivo con TMG (tmg.mydom.local) el servicio definido por el SPN (http/iosmdm.mydom.local).

Para confiar al dispositivo con TMG el servicio definido por el SPN (http/iosmdm.mydom.local), el administrador debe realizar las siguientes acciones:

1. En el complemento de MMC denominado "Equipos y usuarios de Active Directory", seleccione el dispositivo con TMG instalado (tmg.mydom.local).

2. En las propiedades del dispositivo, en la ficha **Delegación**, configure la opción de **Confiar en este equipo para la delegación al servicio especificado únicamente** en **Usar cualquier protocolo de autenticación**.

3. Añada el SPN (http/iosmdm.mydom.local) a la lista **Servicios a los que esta cuenta puede presentar credenciales delegadas**.

Certificado especial (personalizado) para el servicio web publicado (iosmdm.mydom.global)

Debe emitir un certificado especial (personalizado) para el servicio web de MDM de iOS en FQDN iosmdm.mydom.global y especificar que reemplaza el certificado predeterminado en la configuración del servicio web de MDM de iOS en la Consola de administración.

Tenga en cuenta que el contenedor del certificado (el archivo con la extensión p12 o pfx) también debe contener una cadena de certificados raíz (claves públicas).

Publicación del servicio web de MDM de iOS en TMG

En TMG, para el tráfico que va de un dispositivo móvil al puerto 443 de iosmdm.mydom.global, debe configurar KCD en el SPN (http/iosmdm.mydom.local) usando el certificado emitido para FQDN (iosmdm.mydom.global). Tenga en cuenta que el servicio web publicado y de publicación deben compartir el mismo certificado del servidor.

Uso del Servidor de MDM para iOS por varios Servidores virtuales

Para habilitar el uso del Servidor de MDM para iOS por varios Servidores de administración virtuales, siga estos pasos:

1. Abra el registro del dispositivo cliente que tenga instalado el Servidor de MDM para iOS (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).

2. Vaya al siguiente subárbol:

   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDI

3. Para la clave ConnectorFlags (DWORD), establezca el valor 02102482.

4. Vaya al siguiente subárbol:

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

5. Para la clave ConnInstalled (DWORD), establezca el valor 00000001.

6. Reinicie el servicio del Servidor de MDM para iOS.

Los valores de clave se deben introducir en la secuencia especificada.

Recepción de un certificado de APNs

Si ya tiene un certificado de APNs, .considere renovarlo en lugar de crear uno nuevo. Cuando reemplaza el certificado de APNs existente por uno recién creado, el Servidor de administración pierde la capacidad de administrar los dispositivos móviles iOS conectados actualmente.

Cuando se crea la solicitud de firma de certificado (CSR) en el primer paso del Asistente de instalación de certificado de APNs, su clave privada se almacena en la memoria RAM del dispositivo. Por lo tanto, todos los pasos del Asistente se deben completar en una sola sesión de la aplicación.

Para recibir un certificado de APNs:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.
3. En el menú contextual del servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de MDM para iOS.
4. En la ventana de propiedades del servidor de MDM para iOS, seleccione la sección **Certificados**.
5. En la sección **Certificados**, en el grupo de configuraciones **Certificado de Apple Push Notification**, haga clic en el botón **Solicitar nuevo**.

   Se inicia el Asistente Recibir certificados de APNs y se abre la ventana **Solicitar nuevo**.
6. Cree una solicitud de firma de certificado (en adelante, conocida como CSR). Para ello, realice las siguientes acciones:

   a. Haga clic en el botón **Crear CSR**.

   b. En la ventana **Crear CSR** que se abre, especifique un nombre para la solicitud, los nombres de la empresa y el departamento, la ciudad, la región y el país.

   c. Haga clic en el botón **Guardar** y especifique un nombre para el archivo en el que se guardará CSR.

   La clave privada del certificado se guardará en la memoria del dispositivo.
7. Envíe mediante CompanyAccount el archivo con CSR que ha creado a Kaspersky para que la apruebe.

   La firma de CSR solo estará disponible después de que cargue en el portal CompanyAccount una clave que permita usar Administración de dispositivos móviles.

   Una vez que se haya procesado la solicitud en línea, recibirá un archivo CSR firmada por Kaspersky.
8. Envíe el archivo CSR firmado al sitio web de Apple Inc. con un ID de Apple aleatorio.

   Se recomienda que evite usar un ID personal de Apple. Cree un ID de Apple específico para utilizarlo como ID corporativo. Cuando haya creado un ID de Apple, vincúlelo con el buzón de correo de la organización, no con el de un empleado.

   Cuando CSR se haya procesado en Apple Inc., recibirá la clave pública del certificado de APNs. Guarde el archivo en un disco.

9. Exporte el certificado de APNs junto con la clave privada que se crea al generar CSR, en formato pfx. Para hacer esto:

    a. En la ventana **Solicitar certificado de APNs nuevo**, haga clic en el botón **Finalizar CSR**.

    b. En la ventana **Abrir**, elija un archivo con la clave pública del certificado, procedente de Apple Inc. como resultado del procesamiento de CSR, y haga clic en el botón **Abrir**.

    Se iniciará el proceso de exportación del certificado.

    c. En la ventana siguiente, introduzca la contraseña de la clave privada y haga clic en **Aceptar**.

    Esta contraseña se utilizará para la instalación del certificado de APNs en el Servidor de MDM para iOS.

    d. En la ventana **Guardar certificado de APNs**, especifique el nombre de archivo del certificado de APNs, elija una carpeta y haga clic en **Guardar**.

Se combinan las claves privadas y públicas del certificado y el certificado de APNs y se guarda en formato PFX. Después de eso, puede instalar el certificado de APNs en el Servidor de MDM para iOS.

Renovación de certificados de APNs

Para renovar un certificado de APNs:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.

2. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.

3. En el menú contextual del servidor de MDM para iOS, seleccione **Propiedades**.

    Se abre la ventana de propiedades del Servidor de MDM para iOS.

4. En la ventana de propiedades del servidor de MDM para iOS, seleccione la sección **Certificados**.

5. En la sección **Certificados**, en el grupo de configuraciones **Certificado de Apple Push Notification**, haga clic en el botón **Renovar**.

    Se inicia el Asistente de renovación de certificados de APNs y se abre la ventana **Renovar certificado de APNs**.

6. Cree una solicitud de firma de certificado (en adelante, conocida como CSR). Para ello, realice las siguientes acciones:

    a. Haga clic en el botón **Crear CSR**.

    b. En la ventana **Crear CSR** que se abre, especifique un nombre para la solicitud, los nombres de la empresa y el departamento, la ciudad, la región y el país.

    c. Haga clic en el botón **Guardar** y especifique un nombre para el archivo en el que se guardará CSR.

    La clave privada del certificado se guardará en la memoria del dispositivo.

7. Envíe mediante CompanyAccount el archivo con CSR que ha creado a Kaspersky para que la apruebe.

La firma de CSR solo estará disponible después de que cargue en el portal CompanyAccount una clave que permita usar Administración de dispositivos móviles.

Una vez que se haya procesado la solicitud en línea, recibirá un archivo CSR firmada por Kaspersky.

8. Envíe el archivo CSR firmado al sitio web de Apple Inc. con un ID de Apple aleatorio.

   Se recomienda que evite usar un ID personal de Apple. Cree un ID de Apple específico para utilizarlo como ID corporativo. Cuando haya creado un ID de Apple, vincúlelo con el buzón de correo de la organización, no con el de un empleado.

   Cuando CSR se haya procesado en Apple Inc., recibirá la clave pública del certificado de APNs. Guarde el archivo en un disco.

9. Solicite la clave pública del certificado. Para ello, realice las siguientes acciones:

   a. Vaya al portal de certificados de Apple Push. Para iniciar sesión en el portal, use el ID de Apple que recibió en la solicitud inicial del certificado.

   b. En la lista de certificados, seleccione el certificado cuyo nombre APSP (en formato "APSP: <número>") coincida con el nombre APSP del certificado utilizado por el servidor de MDM para iOS y haga clic en el botón **Renovar**.

      El certificado de APNs se renueva.

   c. Guarde el certificado creado en el portal.

10. Exporte el certificado de APNs junto con la clave privada que se crea al generar CSR, en formato pfx. Para ello, realice las siguientes acciones:

    a. En la ventana **Renovar certificado de APNs**, haga clic en el botón **Finalizar CSR**.

    b. En la ventana **Abrir**, seleccione un archivo con la clave pública del certificado, procedente de Apple Inc. como resultado del procesamiento de CSR, y pulse el botón **Abrir**.

       Se iniciará el proceso de exportación del certificado.

    c. En la ventana siguiente, introduzca la contraseña de la clave privada y haga clic en **Aceptar**.

       Esta contraseña se utilizará para la instalación del certificado de APNs en el Servidor de MDM para iOS.

    d. En la ventana **Renovar certificado de APNs** que se abre, especifique el nombre de archivo del certificado de APNs, elija una carpeta y haga clic en **Guardar**.

Se combinan las claves privadas y públicas del certificado y el certificado de APNs y se guarda en formato PFX.

Configurar un certificado de servidor de MDM para iOS de reserva

La funcionalidad del servidor de MDM para iOS le permite emitir un certificado de reserva. Este certificado está diseñado para usarse en los perfiles de configuración de MDM de iOS, para garantizar un cambio sin problemas de los dispositivos iOS administrados después de que expire el certificado del servidor de MDM para iOS.

Si su servidor de MDM para iOS utiliza un certificado predeterminado emitido por Kaspersky, puede emitir un certificado de reserva (o especificar su propio certificado personalizado como reserva) antes de que caduque el certificado del servidor de MDM para iOS. De forma predeterminada, el certificado de reserva se emite automáticamente 60 días antes de la expiración del certificado del servidor de MDM para iOS. El certificado de reserva de servidor de MDM para iOS se convierte en el certificado principal inmediatamente después de la expiración del certificado de servidor de MDM para iOS. La clave pública se distribuye a todos los dispositivos administrados a través de los perfiles de configuración, por lo que no es necesario transmitirla manualmente.

Para emitir un certificado de servidor de MDM para iOS de reserva o especificar un certificado de reserva personalizado:

1. En el árbol de consola, en la carpeta **Administración de dispositivos móviles**, seleccione la subcarpeta **Servidores de dispositivos móviles**.

2. En la lista de servidores de dispositivos móviles, seleccione el servidor de MDM para iOS correspondiente y, en el panel derecho, haga clic en el botón **Configurar servidor de MDM para iOS**.

3. En la ventana de configuración del servidor de MDM para iOS que se abre, seleccione la sección **Certificados**.

4. En el bloque de configuración **Certificado de reserva**, haga uno de los siguientes:

   - Si piensa seguir utilizando un certificado autofirmado (es decir, el emitido por Kaspersky):

     a. Haga clic en el botón **Problema**.

     b. En la ventana que se abre **Fecha de activación**, seleccione una de las dos opciones para la fecha en que se debe aplicar el certificado de reserva:

        - Si desea aplicar el certificado de reserva en el momento de la expiración del certificado actual, seleccione la opción **Cuando expire el certificado actual**.

        - Si desea aplicar el certificado de reserva antes de que expire el certificado actual, seleccione la opción **Después del periodo especificado (días)**. En el campo de entrada junto a esta opción, especifique la duración del periodo tras el cual el certificado de reserva debe sustituir al certificado actual.

        El periodo de validez del certificado de reserva que especifique no puede superar el plazo de validez del certificado actual del servidor de MDM para iOS.

     c. Haga clic en el botón **Aceptar**.

     Se emite el certificado de servidor de MDM para iOS de reserva.

   - Si tiene previsto utilizar un certificado personalizado emitido por su autoridad de certificación:

     a. Haga clic en el botón **Agregar**.

     b. En la ventana del Explorador de archivos que se abre, especifique un archivo de certificado en formato PEM, PFX o P12, que esté almacenado en su dispositivo, y luego pulse el botón **Abrir**.

     Su certificado personalizado se especifica como el certificado de servidor de MDM para iOS de reserva.

Tiene un certificado de servidor de MDM para iOS de reserva. Los detalles del certificado de reserva se muestran en el bloque de configuración **Certificado de reserva** (nombre del certificado, nombre del emisor, fecha de vencimiento y la fecha en que se debe aplicar el certificado de reserva, si corresponde).

Instalación de un certificado de APNs en un servidor de MDM para iOS

Después de recibir el certificado de APNs, debe instalarlo en el servidor de MDM para iOS.

Para instalar el certificado de APNs en el Servidor de MDM para iOS, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.
3. En el menú contextual del servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de MDM para iOS.
4. En la ventana de propiedades del servidor de MDM para iOS, seleccione la sección **Certificados**.

En la sección **Certificados**, en el bloque de configuración **Certificado de Apple Push Notification**, haga clic en el botón **Instalar**.

1. Seleccione el archivo PFX que contiene el certificado de APNs.
2. Introduzca la contraseña de la clave privada que se especificó al exportar el certificado de APNs.

El certificado de APNs se instalará en el Servidor de MDM para iOS. Los detalles del certificado aparecerán en la ventana de propiedades del Servidor de MDM para iOS, en la sección **Certificados**.

Configuración del acceso al servicio de Apple Push Notification

Para garantizar el correcto funcionamiento del servicio web de MDM de iOS y las respuestas oportunas de los dispositivos móviles a los comandos del administrador, debe especificar un Certificado de notificación de inserción de Apple (en adelante, denominado certificado de APNs) en la configuración del Servidor de MDM para iOS.

El servicio web de MDM para iOS, que interactúa con la Notificación de inserción de Apple (en adelante, denominada APNs), se conecta a la dirección externa api.push.apple.com a través del puerto 2197 (saliente). Por lo tanto, el servicio web de MDM de iOS requiere acceso al puerto TCP 2197 para el rango de direcciones 17.0.0.0/8. Desde el lado del dispositivo iOS se accede al puerto TCP 5223 para el rango de direcciones 17.0.0.0/8.

Si tiene la intención de acceder a APNs desde el lado del servicio web de MDM de iOS a través de un servidor proxy, debe realizar las siguientes acciones en el dispositivo con el servicio web de MDM de iOS instalado:

1. Agregue las siguientes cadenas al registro:

   - Para un sistema operativo de 32 bits:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
"ApnProxyHost"="<Nombre del Host del Proxy>"
"ApnProxyPort"="<Puerto del Proxy>"
"ApnProxyLogin"="<Inicio de sesión del Proxy>"
"ApnProxyPwd"="<Contraseña de Proxy>"
```

- Para un sistema operativo de 64 bits:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSM
"ApnProxyHost"="<Nombre del Host del Proxy>"
"ApnProxyPort"="<Puerto del Proxy>"
"ApnProxyLogin"="<Inicio de sesión del Proxy>"
"ApnProxyPwd"="<Contraseña de Proxy>"
```

2. Reinicie el servicio web de MDM de iOS.

Emisión e instalación de un certificado general en un dispositivo móvil

Para emitir un certificado compartido a un usuario, siga estos pasos:

1. En el árbol de consola, seleccione una cuenta de usuario en la carpeta **Cuentas de usuario**.
2. En el menú contextual de la cuenta de usuario, seleccione **Instalar certificado**.

Se inicia el Asistente de instalación de certificados. Siga las instrucciones del Asistente.

Cuando finalice el Asistente, se creará y se agregará un certificado a la lista de certificados del usuario.

El usuario descargará el certificado asignado junto con el paquete de instalación que contiene el perfil de MDM para iOS.

Cuando el dispositivo móvil se conecta al Servidor de MDM para iOS, la configuración del perfil de MDM para iOS se aplica al dispositivo del usuario. El administrador podrá gestionar el dispositivo tras la conexión.

El dispositivo móvil del usuario conectado al Servidor de MDM para iOS se muestra en la subcarpeta **Dispositivos móviles** que se encuentra en la carpeta **Administración de dispositivos móviles** del árbol de consola.

Agregar un dispositivo KES de la lista de dispositivos administrados

Para agregar el dispositivo KES a la lista de dispositivos administrados utilizando un enlace a Google Play™:

1. En el árbol de consola, seleccione la carpeta **Cuentas de usuario**.

   De forma predeterminada, la carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado**.

2. Seleccione la cuenta de usuario cuyo dispositivo móvil desea agregar a la lista de dispositivos administrados.
3. En el menú contextual de la cuenta de usuario, seleccione **Agregar dispositivo móvil**.

   El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse. En la ventana **Origen del certificado** del Asistente, debe especificar el método de creación del certificado compartido que utilizará el Servidor de administración para identificar el dispositivo móvil. Puede especificar un certificado compartido usando uno de los siguientes métodos:

   - Creando un certificado compartido automáticamente, mediante las herramientas del Servidor de administración, y luego entregando el certificado al dispositivo.

- Especificando un archivo de certificado compartido.

4. En la ventana **Tipo de dispositivos** del Asistente, seleccione **Enlace a Google Play**.

5. En la ventana **Método de notificación del usuario** del Asistente, defina la configuración para la notificación al usuario del dispositivo móvil de la creación del certificado (con un mensaje de texto, por correo electrónico o mostrando la información cuando se complete el Asistente).

6. En la ventana Información del certificado del Asistente, haga clic en el botón **Finalizar** para cerrar el Asistente de instalación de certificados.

Cuando el Asistente finalice sus actividades, se enviarán un enlace y un código QR al dispositivo móvil del usuario, que le permitirán descargar Kaspersky Endpoint Security desde Google Play. El usuario va a Google Play usando el enlace o escaneando el código de QR. A continuación, el sistema operativo del dispositivo solicita al usuario que acepte la instalación de Kaspersky Endpoint Security for Android. Una vez descargado e instalado Kaspersky Endpoint Security for Android, el dispositivo móvil se conecta al Servidor de administración y descarga un certificado compartido. Una vez instalado el certificado en el dispositivo móvil, el dispositivo se muestra en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de consola.

Si Kaspersky Endpoint Security for Android ya se ha instalado en el dispositivo, el usuario tiene que recibir la configuración de conexión del Servidor de administración desde el administrador, y después introducirlas por sí mismo. Después haber definido la configuración de conexión, el dispositivo móvil se conecta al Servidor de administración. El administrador emite un certificado compartido para el dispositivo y envía al usuario un mensaje de correo electrónico o un mensaje de texto con un inicio de sesión y una contraseña para la descarga del certificado. El usuario descarga e instala el certificado compartido. Una vez instalado el certificado en el dispositivo móvil, el dispositivo se muestra en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de consola. En este caso, Kaspersky Endpoint Security for Android no se descargará ni se instalará de nuevo.

Conexión de dispositivos KES al Servidor de administración

Según el método usado para la conexión de dispositivos al Servidor de administración, son posibles dos esquemas de despliegue para Kaspersky Device Management for iOS para los dispositivos KES:

- Esquema de despliegue con conexión directa de dispositivos al Servidor de administración
- Esquema de despliegue que involucra a Forefront® Threat Management Gateway (TMG)

Conexión directa de dispositivos al Servidor de administración

Los dispositivos KES pueden conectarse directamente al puerto 13292 del Servidor de administración.

Según el método usado para la autenticación, son posibles dos opciones para la conexión de dispositivos KES al Servidor de administración:

- Conexión de dispositivos con un certificado de usuario
- Conexión de dispositivos sin un certificado de usuario

Conexión de un dispositivo con un certificado de usuario

Al conectar un dispositivo con un certificado de usuario, ese dispositivo está asociado con la cuenta de usuario a la cual se ha asignado el certificado correspondiente a través de las herramientas del Servidor de administración.

En este caso, se utilizará la autenticación SSL bidireccional (autenticación mutua). Tanto el Servidor de administración como el dispositivo serán autenticados con certificados.

Conexión de un dispositivo sin un certificado de usuario

Al conectar un dispositivo sin un certificado de usuario, ese dispositivo no está asociado con ninguna de las cuentas de usuario en el Servidor de administración. Sin embargo, cuando el dispositivo reciba cualquier certificado, el dispositivo se asociará con el usuario al cual se haya asignado el certificado correspondiente a través de las herramientas del Servidor de administración.

Al conectar ese dispositivo al Servidor de administración, se aplicará la autenticación SSL unidireccional, lo que significa que solo el Servidor de administración se autentica con el certificado. Después de que el dispositivo recupere el certificado de usuario, el tipo de autenticación cambiará a la autenticación SSL bidireccional (autenticación SSL bidireccional, autenticación mutua).

Esquema para conectar dispositivos KES al servidor con la delegación limitada de Kerberos (KCD)

El esquema para conectar dispositivos KES al Servidor de administración que involucra la delegación limitada de Kerberos (KCD) brinda lo siguiente:

- Integración con Microsoft Forefront TMG.
- Uso de la delegación limitada de Kerberos (en adelante, denominada KCD) para la autenticación de dispositivos móviles.
- Integración con la infraestructura de clave pública (en adelante, denominada PKI) para aplicar certificados de usuario.

Al usar este esquema de conexión, tenga en cuenta lo siguiente:

- El tipo de conexión de dispositivos KES a TMG debe ser la "Autenticación SSL bidireccional", es decir, un dispositivo debe conectarse a TMG a través de su certificado de usuario patentado. Para esto, debe integrar el certificado de usuario en el paquete de instalación de Kaspersky Endpoint Security for Android, que se ha instalado en el dispositivo. Este paquete KES debe ser creado por el Servidor de administración específicamente para este dispositivo (usuario).
- Debe especificar el certificado especial (personalizado) en vez del certificado del servidor predeterminado para el protocolo móvil:

  1. En la ventana de propiedades del Servidor de administración, en la sección **Configuración**, seleccione la casilla **Abrir puerto para dispositivos móviles** y, luego, seleccione **Agregar certificado** en la lista desplegable.
  2. En la ventana que se abre, especifique el mismo certificado que se configuró en TMG cuando se publicó el punto de acceso al protocolo móvil en el Servidor de administración.

- Los certificados de usuario para los dispositivos KES deben ser emitidos por la entidad de certificación (CA) del dominio. Tenga en cuenta que si el dominio incluye varios CA raíz, los certificados de usuario deben ser

emitidos por la CA que se haya configurado en la publicación de TMG.

Puede asegurarse de que el certificado de usuario cumpla con los requisitos especificados anteriormente con uno de los siguientes métodos:

- Especifique el certificado de usuario especial en el Asistente para nuevo paquete de Instalación y en el Asistente de instalación de certificados.
- Integre el Servidor de administración con la PKI del dominio y defina la configuración correspondiente en las reglas para la emisión de certificados:

  1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
  2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el botón **Configurar reglas de emisión de certificados** para abrir la ventana **Reglas de emisión de certificados**.
  3. En la sección **Integración con la PKI**, configure la integración con la infraestructura de clave pública.
  4. En la sección **Emisión de certificados móviles**, especifique el origen de los certificados.

A continuación, se especifica un ejemplo de la configuración de la delegación limitada de Kerberos (KCD) con las siguientes suposiciones:

- El punto del acceso al protocolo móvil en el lado del Servidor de administración está configurado en el puerto 13292.
- El nombre del dispositivo con TMG es tmg.mydom.local.
- El nombre del dispositivo con el Servidor de administración es ksc.mydom.local.
- El nombre de la publicación externa del punto de acceso al protocolo móvil es kes4mob.mydom.global.

Cuenta de dominio para el Servidor de administración

Debe crear una cuenta de dominio (por ejemplo, KSCMobileSrvcUsr) en la que se ejecutará el servicio del Servidor de administración. Puede especificar una cuenta para el servicio del Servidor de administración al instalar el Servidor de administración o a través de la utilidad klsrvswch. La utilidad klsrvswch se ubica en la carpeta de instalación del Servidor de administración.

Debe especificarse una cuenta de dominio por las siguientes razones:

- La función para la administración de dispositivos KES es una parte integral del Servidor de administración.
- Para asegurar el correcto funcionamiento de la delegación limitada de Kerberos (KCD), el lado de recepción (es decir, el Servidor de administración) se debe ejecutar bajo una cuenta de dominio.

Nombre principal del servicio para http/kes4mob.mydom.local

En el dominio, en la cuenta de KSCMobileSrvcUsr, añada un SPN para publicar el servicio del protocolo móvil en el puerto 13292 del dispositivo con el Servidor de administración. Para el dispositivo kes4mob.mydom.local con el Servidor de administración, esto aparecerá de la siguiente forma:

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

Configuración de las propiedades de dominio del dispositivo con TMG (tmg.mydom.local)

Para delegar el tráfico, confíe al dispositivo con TMG (tmg.mydom.local) el servicio definido por el SPN (http/kes4mob.mydom.local:13292).

Para confiar al dispositivo con TMG el servicio definido por el SPN (http/kes4mob.mydom.local:13292), el administrador debe realizar las siguientes acciones:

1. En el complemento de MMC denominado "Equipos y usuarios de Active Directory", seleccione el dispositivo con TMG instalado (tmg.mydom.local).

2. En las propiedades del dispositivo, en la ficha **Delegación**, configure la opción de **Confiar en este equipo para la delegación al servicio especificado únicamente** en **Usar cualquier protocolo de autenticación**.

3. En la lista **Servicios a los que esta cuenta puede presentar credenciales delegadas**, añada el SPN http/kes4mob.mydom.local:13292.

Certificado especial (personalizado) para la publicación (kes4mob.mydom.global)

Para publicar el protocolo móvil del Servidor de administración, debe emitir un certificado especial (personalizado) para FQDN kes4mob.mydom.global y especificarlo en vez del certificado del servidor predeterminado en la configuración del protocolo móvil del Servidor de administración en la Consola de administración. Para hacerlo, en la ventana de propiedades del Servidor de administración, en la sección **Configuración**, seleccione la casilla **Abrir puerto para dispositivos móviles** y, luego, seleccione **Agregar certificado** en la lista desplegable.

Tenga en cuenta que el contenedor del certificado del servidor (el archivo con la extensión p12 o pfx) también debe contener una cadena de certificados raíz (claves públicas).

Configuración de la publicación en TMG

En TMG, para el tráfico que va desde el lado del dispositivo móvil al puerto 13292 de kes4mob.mydom.global, debe configurar KCD en el SPN (http/kes4mob.mydom.local:13292) usando el certificado del servidor emitido para FQND kes4mob.mydom.global. Tenga en cuenta que el punto del acceso de publicación y publicado (puerto 13292 del Servidor de administración) deben compartir el mismo certificado del servidor.

Uso de Google Cloud Firebase Messaging

Para garantizar las respuestas oportunas de los dispositivos KES en Android a los comandos del administrador, debe activar el uso de Google™ Firebase Cloud Messaging (en adelante, denominado FCM) en las propiedades del Servidor de administración.

Para activar el uso de FCM:

1. En la Consola de administración, seleccione el nodo **Administración de dispositivos móviles** y la carpeta **Dispositivos móviles**.

2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.

3. En las propiedades de la carpeta, seleccione la sección **Configuración de Google Firebase Cloud Messaging**.

4. En los campos **ID de remitente** y **Clave de servidor**, especifique la configuración de FCM: SENDER_ID y de la Clave de API.

El servicio de FCM se ejecuta en los siguientes rangos de direcciones:

- Desde el lado del dispositivo KES, se requiere acceso a los puertos 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) y 5230 (HTTPS) de las siguientes direcciones:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Todas las direcciones IP enumeradas en ASN de Google de 15169
- Desde el lado del Servidor de administración, se requiere acceso al puerto 443 (HTTPS) de las siguientes direcciones:
  - fcm.googleapis.com
  - Todas las direcciones IP enumeradas en ASN de Google de 15169

Si la configuración del servidor proxy (**Avanzado**/**Configuración del acceso a Internet**) se ha definido en las propiedades del Servidor de administración en la Consola de administración, se utilizarán para la interacción con FCM.

Configuración de FCM: recuperación de SENDER_ID y la clave de API

Para configurar FCM, el administrador debe realizar las siguientes acciones:

1. Regístrese en el portal de Google.
2. Vaya al portal para programadores.
3. Cree un nuevo proyecto haciendo clic en el botón **Crear proyecto** y especifique el nombre del proyecto y el ID.
4. Espere que el proyecto se cree.

   En la primera página del proyecto, en la parte superior de la página, el campo **Número de proyecto** muestra el SENDER_ID relevante.
5. Vaya a la sección **API y autenticación/APIs** y active **Google Firebase Cloud Messaging para Android**.
6. Vaya a la sección **API y autenticación/Credenciales** y haga clic en **Crear nueva clave**.
7. Haga clic en el botón **Clave de servidor**.
8. Imponga restricciones (si corresponde) y haga clic en el botón **Crear**.
9. Recupere la clave de API desde las propiedades de la clave recién creada (campo **Clave de servidor**).

Integración con la infraestructura de clave pública

La integración con la infraestructura de clave pública (en adelante, denominada PKI) está diseñada principalmente para simplificar la emisión de certificados de usuario de dominio por parte del Servidor de administración.

El administrador puede asignar un certificado de dominio para un usuario en la Consola de administración. Esto puede realizarse usando uno de los métodos siguientes:

- Asigne al usuario un certificado especial (personalizado) de un archivo en el Asistente de Conexión de nuevo dispositivo o en el Asistente de instalación de certificados.
- Realice la integración con la PKI y asigne la PKI para que funcione como el origen de certificados para un tipo específico de certificados o para todos los tipos de certificados.

La configuración de integración con PKI está disponible en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados** haciendo clic en el enlace **Integrar con la infraestructura de clave pública**.

Principio general de integración con la PKI para la emisión de certificados de usuario de dominio

En la Consola de administración, haga clic en el enlace **Integrar con la infraestructura de clave pública** en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados** para especificar una cuenta de dominio que utilizará el Servidor de administración para emitir certificados de usuario de dominio a través de la CA del dominio (en adelante, se hace referencia como la cuenta bajo la cual se realiza la integración con la PKI).

Tenga en cuenta lo siguiente:

- La configuración de la integración con la PKI le proporciona la posibilidad de especificar la plantilla predeterminada para todos los tipos de certificados. Tenga en cuenta que las reglas para la emisión de certificados (disponibles en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados** haciendo clic en **Configurar reglas de emisión de certificados**) le permiten especificar una plantilla individual para cada tipo de certificado.
- Un certificado especial de Agente de inscripción (EA) debe instalarse en el dispositivo con el Servidor de administración, en el repositorio de certificados de la cuenta bajo la cual se realiza la integración con la PKI. El certificado del Agente de inscripción (EA) es emitido por el administrador de la CA (entidad de certificación) del dominio.

La cuenta bajo la cual se realiza la integración con la PKI debe cumplir los siguientes criterios:

- Ser un usuario de dominio.
- Ser un administrador local del dispositivo con el Servidor de administración desde el cual se inicia la integración con la PKI.
- Tener el permiso para *Iniciar sesión como servicio*.
- El dispositivo con el Servidor de administración instalado debe ejecutarse al menos una vez con esta cuenta para crear un perfil de usuario permanente.

Servidor web de Kaspersky Security Center

El Servidor web de Kaspersky Security Center (en adelante, denominado Servidor web) es un componente de Kaspersky Security Center. El Servidor web está diseñado para publicar paquetes de instalación independientes, paquetes de instalación independientes para dispositivos móviles, perfiles de MDM para iOS y archivos de una carpeta compartida.

Los perfiles de MDM para iOS y los paquetes de instalación que se han creado se publican en el Servidor web automáticamente y, luego, se eliminan después de la primera descarga. El administrador puede enviar el nuevo enlace al usuario de cualquier forma que convenga; por ejemplo, por correo electrónico.

Al hacer clic en el enlace, el usuario puede descargar la información necesaria en un dispositivo móvil.

Configuración del servidor web

Si se requiere la configuración avanzada del Servidor web, las propiedades del Servidor web de la Consola de administración proporcionan la posibilidad de cambiar puertos por HTTP (8060) y HTTPS (8061). Además del cambio de puertos, puede reemplazar el certificado del servidor para HTTPS y cambiar FQDN del Servidor web por HTTP.

La Instalación de Kaspersky Security Center

Esta sección describe la instalación de los componentes de Kaspersky Security Center. Si desea instalar la aplicación de manera local en un solo dispositivo, hay dos opciones de instalación disponibles:

- **Estándar**. Esta opción se recomienda si desea probar Kaspersky Security Center, por ejemplo, comprobando su funcionamiento en un área pequeña dentro su red. Durante la instalación estándar, solo configura la base de datos. También puede instalar solo el conjunto predeterminado de complementos de administración para las aplicaciones de Kaspersky. También puede utilizar la instalación estándar si ya tiene experiencia de trabajo con Kaspersky Security Center y sabe cómo especificar todas las configuraciones relevantes después de la instalación estándar.

- **Personalizada**. Esta opción se recomienda si planea modificar la configuración de Kaspersky Security Center, como la ruta a la carpeta compartida, las cuentas y los puertos para la conexión con el Servidor de administración y la configuración de la base de datos. La instalación personalizada le permite especificar qué complementos de administración de Kaspersky instalar. Si es necesario, puede iniciar la instalación personalizada en el modo no interactivo.

Si al menos un Servidor de administración se instala en la red, los Servidores se pueden instalar en otros dispositivos remotamente a través de la tarea de instalación remota usando la instalación forzada. Al crear la tarea de instalación remota, debe usar el paquete de instalación del Servidor de administración: ksc_<número_versión>.<número de compilación>_full_<idioma de localización>.exe.

Use este paquete si desea instalar todos los componentes requeridos para la funcionalidad completa de Kaspersky Security Center o actualizar las versiones actuales de estos componentes.

Si desea desplegar el clúster de conmutación por error de Kaspersky, debe instalar Kaspersky Security Center en todos los nodos del clúster.

Preparación para la instalación

Antes de iniciar la instalación, asegúrese de que el hardware y el software del dispositivo cumplen los requisitos del Servidor de administración y la Consola de administración.

Se recomienda instalar el Servidor de administración en un servidor dedicado, y no en un controlador de dominio.

Kaspersky Security Center almacena su información en una base de datos SQL Server. Para hacerlo, debe instalar la base de datos de SQL Server por su cuenta (obtenga más información sobre cómo seleccionar un DBMS). Se pueden utilizar otros servidores SQL para almacenar datos. Se deben instalar en la red antes de Kaspersky Security Center. La instalación de Kaspersky Security Center requiere privilegios de administrador en el dispositivo en el que se va a realizar la instalación.

Instale el Servidor de administración, el Agente de red y la Consola de administración en carpetas que tengan desactivada la distinción entre mayúsculas y minúsculas. Además, la distinción entre mayúsculas y minúsculas debe estar desactivada para la carpeta compartida del Servidor de administración y la carpeta oculta de Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

La versión de servidor del Agente de red se instala en el dispositivo junto con el Servidor de administración. El Servidor de administración no puede instalarse junto con la versión normal del Agente de red. Si la versión de servidor del Agente de red ya está instalada en el dispositivo, elimínela y vuelva a iniciar la instalación del Servidor de administración.

A partir de la versión 10 del Service Pack 3, Kaspersky Security Center es compatible con cuentas de servicio administradas y cuentas de servicio administradas de grupo. Si en su dominio se usan estos tipos de cuentas y desea especificar una de ellas como la cuenta para el servicio del Servidor de administración, primero instale la cuenta en el mismo dispositivo en el que desea instalar el Servidor de administración. Para obtener detalles sobre la instalación de cuentas de servicio administradas en un dispositivo local, consulte la documentación oficial de Microsoft.

Cuentas para trabajar con el DBMS

La siguiente tabla proporciona información sobre cómo la selección de un sistema de administración de bases de datos (DBMS) afecta a las propiedades de las cuentas elegidas para trabajar con el DBMS.

El *DBMS local* es un DBMS instalado en el mismo dispositivo que el Servidor de administración. El *DBMS remoto* es un DBMS instalado en un dispositivo diferente.

Conceda todos los derechos necesarios para la cuenta del Servidor de administración antes de iniciar el servicio del Servidor de administración.

SQL Server con autenticación de Windows y con autenticación de SQL Server

DBMS: SQL Server (incluido Express Edition) con autenticación de Windows

Ubicación del DBMS	Local	Local	Remoto	Remoto
Quién crea la base de datos KAV	El instalador (automáticamente)	Administrador (manualmente)	El instalador (automáticamente)	Administrador (manualmente)
Cuenta en la que se está ejecutando el programa de instalación	Local o dominio	Local o dominio	Dominio	Dominio
Derechos de la cuenta en la que se está	• Sistema: derechos de	• Sistema: derechos de administrador local	• Sistema: derechos de	• Sistema: derechos de

ejecutando el programa de instalación	administrador local • SQL Server: función de administrador del sistema	• SQL Server: Funciones a nivel del servidor: “public” y “dbcreator” Permiso `VIEW ANY DEFINITION` Permiso `VIEW SERVER STATE` (si la función Always On está activada) Para bases de datos principales y “tempdb”: función “public” y esquema “dbo” Para la base de datos KAV (solo si se utiliza una base de datos KAV existente): función “db_owner” y esquema “dbo”	administrador local • SQL Server: función sysadmin	administrador local. • SQL Server: Funciones a nivel del servidor: “public” y “dbcreator” Permiso `VIEW ANY DEFINITION` Permiso `VIEW SERVER STATE` (si la función Always On está activada) Para bases de datos principales y “tempdb”: función “public” y esquema “dbo” Para la base de datos KAV (solo si se utiliza una base de datos KAV existente): función “db_owner” y esquema “dbo”
Cuenta del Servidor de administración	• Creada automáticamente en formato KL-AK-* • Cuenta local seleccionada por el administrador • Cuenta de dominio seleccionada por el administrador	• Creada automáticamente en formato KL-AK-* • Cuenta local seleccionada por el administrador • Cuenta de dominio seleccionada por el administrador	Dominio.	Dominio.
Derechos de la cuenta del servicio del Servidor de administración	• Sistema: derechos necesarios asignados por el programa de instalación. • SQL Server: derechos	• Sistema: derechos necesarios asignados por el programa de instalación. • SQL Server: Función a nivel del servidor: “public”	• Sistema: derechos necesarios asignados por el programa de instalación. • SQL Server: derechos	• Sistema: derechos necesarios asignados por el programa de instalación. • SQL Server:

	necesarios asignados por el programa de instalación.	Permiso `VIEW ANY DEFINITION` Permiso `VIEW SERVER STATE` (si la función Always On está activada) Para bases de datos principales y "tempdb": función "public" y esquema "dbo" Para la base de datos KAV: función "db_owner" y esquema "dbo"	necesarios asignados por el programa de instalación.	Función a nivel del servidor: "public" Permiso `VIEW ANY DEFINITION` Permiso `VIEW SERVER STATE` (si la función Always On está activada) Para bases de datos principales y "tempdb": función "public" y esquema "dbo" Para la base de datos KAV: función "db_owner" y esquema "dbo"

DBMS: SQL Server (incluido Express Edition) con autenticación de SQL Server

Ubicación del DBMS	Local.	Remoto.
Quién crea la base de datos KAV	Administrador (manualmente) o el instalador (automáticamente).	Administrador (manualmente) o el instalador (automáticamente).
Cuenta en la que se está ejecutando el programa de instalación	Local.	Dominio.
Derechos de la cuenta en la que se está ejecutando el programa de instalación	• Sistema: derechos de administrador local. • SQL Server: la cuenta del programa de instalación no requiere acceso a SQL Server.	• Sistema: derechos de administrador local. • SQL Server: la cuenta del programa de instalación no requiere acceso a SQL Server.
Cuenta de servicio del Servidor de administración	Local o dominio.	Dominio.
Derechos de la cuenta del servicio del Servidor de administración	• Sistema: derechos necesarios asignados por el programa de instalación. • SQL Server: la cuenta del servicio del Servidor de administración no requiere acceso a SQL Server.	• Sistema: derechos necesarios asignados por el programa de instalación. • SQL Server: la cuenta del servicio del Servidor de administración no requiere acceso a SQL Server.
Información adicional	En el programa de instalación, el administrador especifica explícitamente	En el programa de instalación, el administrador especifica explícitamente

	una cuenta interna de SQL Server que requiere la función sysadmin.	una cuenta interna de SQL Server que requiere la función sysadmin.

MySQL

DBMS: MySQL

Ubicación del DBMS	Local o remoto.	Local o remoto.
Quién crea la base de datos KAV	El instalador (automáticamente).	Administrador (manualmente).
Cuenta en la que se está ejecutando el programa de instalación	Local o dominio.	Local o dominio.
Derechos de la cuenta en la que se está ejecutando el programa de instalación	• Sistema: derechos de administrador local. • MySQL Server: la cuenta del programa de instalación no requiere acceso a MySQL.	• Sistema: derechos de administrador local. • MySQL Server: la cuenta del programa de instalación no requiere acceso a MySQL.
Cuenta de servicio del Servidor de administración	Local o dominio.	Local o dominio.
Derechos de la cuenta del servicio del Servidor de administración	• Sistema: derechos necesarios asignados por el programa de instalación. • MySQL Server: la cuenta del servicio del Servidor de administración no requiere acceso a MySQL.	• Sistema: derechos necesarios asignados por el programa de instalación. • MySQL Server: la cuenta del servicio del Servidor de administración no requiere acceso a MySQL.
Información adicional	En el programa de instalación, el administrador especifica explícitamente una cuenta interna de SQL que requiere acceso a raíz	El administrador especifica explícitamente en el Instalador una cuenta interna de MySQL que requiere GRANT ALL para la base de datos KAV y SELECT, SHOW VIEW, PROCESS para las tablas del sistema. Los permisos requeridos para MySQL Server son: • `SELECT` • `INSERT` • `UPDATE` • `DELETE`

		• CREATE • DROP • PROCESS • REFERENCES • INDEX • ALTER • SHOW DATABASES • CREATE TEMPORARY TABLES • LOCK TABLES • EXECUTE • CREATE VIEW • SHOW VIEW • CREATE ROUTINE • ALTER ROUTINE • EVENT • TRIGGER • SUPER El permiso SUPER solo se requiere para restaurar desde una copia de seguridad.

MariaDB

DBMS: MariaDB

Ubicación del DBMS	Local o remoto.	Local o remoto.
Quién crea la base de datos KAV	El instalador (automáticamente).	Administrador (manualmente).
Cuenta en la que se está ejecutando el programa de instalación	Local o dominio.	Local o dominio.
Derechos de la cuenta en la que	• Sistema: derechos de administrador local.	• Sistema: derechos de administrador local.

se está ejecutando el programa de instalación	• Servidor MariaDB: la cuenta del programa de instalación no requiere acceso a MariaDB.	• Servidor MariaDB: la cuenta del programa de instalación no requiere acceso a MariaDB.
Cuenta de servicio del Servidor de administración	Local o dominio.	Local o dominio.
Derechos de la cuenta del servicio del Servidor de administración	• Sistema: derechos necesarios asignados por el programa de instalación. • Servidor MariaDB: la cuenta de servicio del Servidor de administración no requiere acceso a MariaDB.	• Sistema: derechos necesarios asignados por el programa de instalación. • Servidor MariaDB: la cuenta de servicio del Servidor de administración no requiere acceso a MariaDB.
Información adicional	En el programa de instalación, el administrador especifica explícitamente una cuenta interna de SQL que requiere acceso a raíz	El administrador especifica explícitamente en el instalador una cuenta interna de MariaDB que requiere los permisos `GRANT ALL` para la base de datos KAV y `SELECT`, `SHOW VIEW` y `PROCESS` para las tablas del sistema.

Escenario: Autenticación de Microsoft SQL Server

La información de esta sección solo es aplicable a las configuraciones en las que Kaspersky Security Center utiliza Microsoft SQL Server como sistema de administración de bases de datos.

Para proteger frente al acceso no autorizado los datos de Kaspersky Security Center transferidos hacia o desde la base de datos y los datos almacenados en la base de datos contra el acceso, debe asegurar la comunicación entre Kaspersky Security Center y SQL Server. La forma más confiable de proporcionar una comunicación segura es instalar Kaspersky Security Center y SQL Server en el mismo dispositivo y usar el mecanismo de memoria compartida para ambas aplicaciones. En todos los demás casos, le recomendamos que use un certificado SSL o TLS para autenticar la instancia de SQL Server. Puede usar un certificado de una autoridad de certificación (CA) confiable o un certificado autofirmado. Le recomendamos que utilice un certificado de una CA de confianza porque un certificado autofirmado solo proporciona protección limitada.

La autenticación de SQL Server se lleva a cabo en etapas:

1. **Generar un certificado SSL o TLS autofirmado para SQL Server de acuerdo con los requisitos del certificado**

   Si ya tiene un certificado para SQL Server, omita este paso.

   Un certificado SSL solo es aplicable a las versiones de SQL Server anteriores a 2016 (13.x). En SQL Server 2016 (13.x) y versiones posteriores, use un certificado TLS.

   Por ejemplo, para generar un certificado TLS, ejecute el siguiente comando en PowerShell:

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

En el comando, en vez de SQL_HOST_NAME, debe escribir el nombre de host de SQL Server si el host está incluido en el dominio o escribir el *nombre de dominio completo* (FQDN) del host si el host no está incluido en el dominio. El mismo nombre (nombre de host o FQDN) debe especificarse como nombre de instancia de SQL Server en el Asistente de instalación del Servidor de administración.

2. **Añadir el certificado en la instancia de SQL Server**

   Las instrucciones para esta etapa dependen de la plataforma en la que se ejecuta SQL Server. Consulte la documentación oficial para más detalles.

   - Windows
   - Linux
   - Amazon Relational Database Service
   - Windows Azure

   Para usar el certificado en un clúster con tolerancia a fallos (failover cluster), debe instalar el certificado en cada nodo del clúster con tolerancia a fallos. Para más detalles, consulte la documentación de Microsoft.

3. **Asignación de permisos de la cuenta de servicio**

   Asegúrese de que la cuenta de servicio bajo la cual se ejecuta el servicio SQL Server tenga el permiso de Control total para acceder a las claves privadas. Para más detalles, consulte la documentación de Microsoft.

4. **Añadir el certificado a la lista de certificados de confianza para Kaspersky Security Center**

   En el dispositivo del Servidor de administración, añada el certificado a la lista de certificados confiables. Para más detalles, consulte la documentación de Microsoft.

5. **Activar conexiones cifradas entre la instancia de SQL Server y Kaspersky Security Center**

   En el dispositivo del Servidor de administración, establezca el valor `1` en la variable de entorno `KLDBADO_UseEncryption`. Por ejemplo, en Windows Server 2012 R2, puede cambiar las variables de entorno al hacer clic en **Variables de entorno** en la pestaña **Avanzado** de la ventana **Propiedades del sistema**. Agregue una nueva variable, asígnele el nombre `KLDBADO_UseEncryption` y luego establezca el valor `1`.

6. **Configuración adicional para usar el protocolo TLS 1.2**

   Si usa el protocolo TLS 1.2, haga también lo siguiente:

   - Asegúrese de que la versión instalada de SQL Server sea una aplicación de 64 bits.
   - Instale el controlador Microsoft OLE DB en el dispositivo del Servidor de administración. Para más detalles, consulte la documentación de Microsoft.
   - En el dispositivo del Servidor de administración, asigne el valor `1` a la variable de entorno `KLDBADO_UseMSOLEDBSQL`. Por ejemplo, en Windows Server 2012 R2, puede cambiar las variables de entorno al hacer clic en **Variables de entorno** en la pestaña **Avanzado** de la ventana **Propiedades del sistema**. Agregue una nueva variable, asígnele el nombre `KLDBADO_UseMSOLEDBSQL` y luego establezca el valor `1`.

7. **Activación del uso del protocolo TCP/IP en una instancia SQL Server con nombre**

   Si usa una instancia SQL Server con nombre, también habilite el uso del protocolo TCP/IP y asigne un número de puerto TCP/IP a SQL Server Database Engine. Cuando configure la conexión de SQL Server en el Asistente de instalación del Servidor de administración, especifique el nombre de host de SQL Server y el número de puerto en el campo **Nombre de instancia de SQL Server**.

Recomendaciones para la instalación del Servidor de administración

Esta sección contiene recomendaciones sobre cómo instalar el Servidor de administración. Esta sección también proporciona situaciones para usar una carpeta compartida en el dispositivo del Servidor de administración a fin de desplegar el Agente de red en dispositivos cliente.

Creación de cuentas para los servicios del Servidor de administración en un clúster de conmutación por error

De forma predeterminada, el instalador crea automáticamente cuentas sin privilegios para los servicios del Servidor de administración. Este comportamiento es el más cómodo para la instalación del Servidor de administración en un dispositivo ordinario.

Sin embargo, la instalación del Servidor de administración en un clúster de conmutación por error requiere una situación diferente:

1. Cree cuentas de dominio sin privilegios para servicios del Servidor de administración y hágalas miembros de un grupo de seguridad de dominio global denominado KLAdmins.

2. En el programa de instalación del Servidor de administración, especifique las cuentas de dominio que se han creado para los servicios.

Definición de una carpeta compartida

Al instalar el Servidor de administración, puede especificar la ubicación de la carpeta compartida. También puede especificar la ubicación de la carpeta compartida después de la instalación, en las propiedades del Servidor de administración. De forma predeterminada, la carpeta compartida se creará en el dispositivo con el Servidor de administración (con derechos de lectura para el subgrupo **Todos**). Sin embargo, en algunos casos (como cuando hay carga alta o se debe acceder desde una red aislada, etc.), es útil localizar la carpeta compartida en un recurso de archivo dedicado.

La carpeta compartida se utiliza de vez en cuando en el despliegue del Agente de red.

Se debe desactivar la distinción entre mayúsculas y minúsculas para la carpeta compartida.

Instalación remota con herramientas del Servidor de administración mediante directivas de grupo de Active Directory

Si los dispositivos de destino se encuentran dentro de un dominio de Windows (no grupos de trabajo), el despliegue inicial (la instalación del Agente de red y la aplicación de seguridad en dispositivos que aún no están administrados) debe realizarse mediante directivas de grupo de Active Directory. El despliegue se realiza usando la tarea estándar para la instalación remota de Kaspersky Security Center. Si la red es a gran escala, es útil localizar la carpeta compartida en un recurso de archivo dedicado para reducir la carga en el subsistema del disco del dispositivo del Servidor de administración.

Instalación remota mediante la entrega de la ruta UNC a un paquete independiente

Si los usuarios de dispositivos conectados a una red en la organización tienen derechos de administrador local, otro método del despliegue inicial es crear un paquete de Agente de red independiente (o, incluso, un paquete de Agente de red "conectado" junto con la aplicación de seguridad). Después de crear un paquete independiente, envíe a usuarios un enlace a ese paquete, que se almacena en la carpeta compartida. La instalación comienza cuando los usuarios hacen clic en el enlace.

Actualización desde la carpeta compartida del Servidor de administración

En la tarea de actualización del antivirus, puede configurar la actualización desde la carpeta compartida del Servidor de administración. Si la tarea se ha asignado a un gran número de dispositivos, es útil localizar la carpeta compartida en un recurso de archivo dedicado.

Instalación de imágenes de sistemas operativos

Las imágenes del sistema operativo siempre se instalan a través de la carpeta compartida: los dispositivos leen imágenes del sistema operativo desde la carpeta compartida. Si tiene la intención de desplegar imágenes en un gran número de dispositivos corporativos, es recomendable localizar la carpeta compartida en un recurso de archivo específico.

Especificación de la dirección del Servidor de administración

Al instalar el Servidor de administración, puede especificar la dirección del host Servidor de administración. Esta dirección se utilizará como la dirección predeterminada al crear paquetes de instalación del Agente de red.

Como dirección del Servidor de administración, puede especificar lo siguiente:

- Nombre NetBIOS del Servidor de administración, que se especifica de forma predeterminada
- Nombre de dominio completo (FQDN) del Servidor de administración si el Sistema de nombres de dominio (DNS) de la red de la organización se ha configurado y funciona correctamente
- Dirección externa si el Servidor de administración está instalado en la zona desmilitarizada (DMZ)

Después de esto, podrá cambiar la dirección del Servidor de administración usando herramientas de la Consola de administración; la dirección no cambiará automáticamente en los paquetes de instalación del Agente de red que ya hayan sido creados.

Instalación estándar

La instalación estándar es una instalación del Servidor de administración que usa las rutas predeterminadas para los archivos de aplicación, instala el conjunto predeterminado de complementos y no habilita la Administración de dispositivos móviles.

Para instalar el Servidor de administración de Kaspersky Security Center en un dispositivo local, siga estos pasos:

Ejecute el archivo ejecutable ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe.

Se abre una ventana que le solicita que seleccione las aplicaciones Kaspersky que desea instalar. En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar el Servidor de administración de Kaspersky Security Center 14** para iniciar el Asistente de instalación del Servidor de administración. Siga las instrucciones del Asistente.

Paso 1. Revisión del Contrato de licencia y la Política de privacidad

En este paso del Asistente de instalación, debe leer el Contrato de licencia, que se formaliza entre Kaspersky y usted, así como la Política de privacidad.

También es posible que se le solicite que consulte los Contratos de licencia y las Políticas de privacidad para los complementos de administración de aplicaciones disponibles en el kit de distribución de Kaspersky Security Center.

Lea detenidamente el siguiente Contrato de licencia y la Política de privacidad. Si acepta todas las condiciones del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido por completo, y que acepto lo siguiente**:

- **Los términos y condiciones de este EULA**
- **La Política de privacidad que describe la gestión de los datos**

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación de la aplicación haciendo clic en el botón **Cancelar**.

Paso 2. Selección de un método de instalación

En la ventana de selección del tipo de instalación, seleccione **Estándar**.

Se recomienda la instalación estándar si desea probar Kaspersky Security Center, por ejemplo, al probar su funcionamiento en un área pequeña dentro su red empresarial. Durante la instalación estándar, solo configura la base de datos. No especifica ninguna configuración del Servidor de administración: en cambio, se utilizan sus respectivos valores predeterminados. La instalación estándar no permite seleccionar complementos de administración para instalar; solo se instala el conjunto predeterminado de complementos. Durante la instalación estándar, no se crea ningún paquete de instalación para dispositivos móviles. Sin embargo, los puede crear más adelante en la Consola de administración.

Paso 3. Instalar Kaspersky Security Center 14 Web Console

Este paso se muestra solo si está utilizando un sistema operativo de 64 bits. De lo contrario, este paso no se muestra, porque Kaspersky Security Center 14 Web Console no funciona con sistemas operativos de 32 bits.

De forma predeterminada, se instalarán tanto Kaspersky Security Center 14 Web Console como la consola de administración basada en MMC.

Si solo desea instalar Kaspersky Security Center 14 Web Console:

1. Seleccione **Instalar solo este**.
2. Elija la **consola basada en Web** en la lista desplegable.

La instalación de Kaspersky Security Center 14 Web Console se inicia automáticamente después de completar la instalación del Servidor de Administración.

Si quiere instalar solo la consola basada en MMC:

1. Seleccione **Instalar solo este**.
2. Elija la **consola basada en MMC** en la lista desplegable.

Paso 4. Selección del tamaño de la red

Especifique el tamaño de la red en la que se está instalando Kaspersky Security Center. Según el número de dispositivos en la red, el Asistente configura la instalación y el aspecto de la interfaz de la aplicación para que coincidan.

En la siguiente tabla se muestran los parámetros de instalación de la aplicación y los parámetros del aspecto de la interfaz que se ajustan según los distintos tamaños de red.

Dependencia de la configuración de instalación en la escala de red seleccionada

Configuración	1 a 100 dispositivos	101 a 1000 dispositivos	1001 a 5000 dispositivos	Más de 5000 dispositivos
Visualizar en el árbol de la consola el nodo de Servidores de administración esclavos y virtuales y todas las configuraciones relacionadas con los Servidores esclavos y virtuales	No disponible	No disponible	Disponible	Disponible
Visualizar las secciones **Seguridad** en las ventanas de propiedades del Servidor de administración y los grupos de administración	No disponible	No disponible	Disponible	Disponible
Distribución aleatoria del tiempo de inicio de la tarea de actualización en los dispositivos cliente	No disponible	Sobre un intervalo de 5 minutos	Sobre un intervalo de 10 minutos	Sobre un intervalo de 10 minutos

Si conecta el Servidor de administración a un servidor de bases de datos MySQL 5.7 o SQL Express, recomendamos que no use la aplicación para administrar más de 10 000 dispositivos. Para el sistema de administración de bases de datos MariaDB, el número máximo recomendado de dispositivos administrados es 20 000.

Paso 5. Selección de una base de datos

En este paso del Asistente, debe seleccionar el mecanismo [Microsoft SQL Server (SQL Express) o MySQL] que se utilizarán para almacenar la base de datos del Servidor de administración. La opción MySQL es relevante tanto para MySQL como para MariaDB.

Se recomienda instalar el Servidor de administración en un servidor dedicado, y no en un controlador de dominio. Sin embargo, si instala Kaspersky Security Center en un servidor que actúe como controlador de dominio de solo lectura (RODC), Microsoft SQL Server (SQL Express) no se debe instalar de manera local (en el mismo dispositivo). En este caso, le recomendamos que instale Microsoft SQL Server (SQL Express) de forma remota (en un dispositivo diferente), o que use MySQL o MariaDB si necesita instalar el DBMS de manera local.

La estructura de la base de datos del Servidor de administración se proporciona en el archivo klakdb.chm, que se encuentra en la carpeta de instalación de Kaspersky Security Center (este archivo también está disponible en el portal de Kaspersky: klakdb.zip).

Paso 6. Configuración de SQL Server

En este paso del Asistente se configura el SQL Server.

Según la base de datos que haya seleccionado, especifique los siguientes ajustes:

- Si ha seleccionado **Microsoft SQL Server (SQL Server Express)** en el paso anterior:
  - En el campo **Nombre de la instancia de SQL Server**, especifique el nombre del equipo de SQL Server en la red. Para ver una lista de todos los SQL Server instalados en la red, haga clic en el botón **Examinar**. Este campo está en blanco de forma predeterminada.

    Si se conecta a SQL Server a través de un puerto personalizado, junto con el nombre de host de SQL Server especifique el número de puerto separado con una coma, por ejemplo:

    ```
    SQL_Server_host_name,1433
    ```

    Si protege la comunicación entre el Servidor de administración y SQL Server por medio de un certificado, especifique en el campo **Nombre de instancia de SQL Server** el mismo nombre de host que se utilizó al generar del certificado. Si utiliza una instancia de SQL Server con nombre, junto con el nombre de host de SQL Server especifique el número de puerto separado con una coma, por ejemplo:

    ```
    SQL_Server_name,1433
    ```

    Si usa varias instancias de SQL Server en el mismo host, especifique también el nombre de la instancia separado con una barra diagonal inversa, por ejemplo:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

Si un SQL Server de la red empresarial tiene activada la función Always On, especifique el nombre del agente de escucha del grupo de disponibilidad en el campo **Nombre de la instancia de SQL Server**. Tenga en cuenta que el Servidor de administración solo admite el modo de disponibilidad de confirmación síncrona cuando la función Always On está activada.

- En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

- Si ha seleccionado **MySQL** en el paso anterior:

  - En el campo **Nombre de la instancia de SQL Server**, especifique el nombre de la instancia de SQL Server. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.

  - En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con la base de datos de SQL Server. El número de puerto predeterminado es el 3306.

  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

Si en esta etapa desea instalar SQL Server en el dispositivo desde el cual está instalando Kaspersky Security Center, debe detener la instalación y reiniciarla después de la instalación de SQL Server. Las versiones admitidas de SQL Server figuran en los requisitos del sistema.

Si está instalando SQL Server en un dispositivo remoto, no es preciso interrumpir el Asistente de Instalación de Kaspersky Security Center. Instale SQL Server y reanude la instalación de Kaspersky Security Center.

Paso 7. Selección de un modo de autenticación

Determine el modo de autenticación que se utilizará cuando el Servidor de administración se conecte SQL Server.

Según la base de datos seleccionada, puede elegir entre los siguientes modos de autenticación.

- Para SQL Express o Microsoft SQL Server seleccione una de las siguientes opciones:

  - **Modo de autenticación de Microsoft Windows**. La verificación de permisos utiliza la cuenta que se utiliza para iniciar el Servidor de administración.

  - **Modo de autenticación de SQL Server**. Si selecciona esta opción, se utiliza la cuenta especificada en la ventana para verificar los derechos de acceso. Rellene los campos **Cuenta** y **Contraseña**.

    Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

  Para ambos modos de autenticación, la aplicación verifica si la base de datos está disponible. Si la base de datos no está disponible, se muestra un mensaje de error y debe proporcionar las credenciales correctas.

  Si la base de datos del Servidor de administración se almacena en otro dispositivo y la cuenta del Servidor de administración no tiene acceso al servidor de la base de datos, debe usar el modo de autenticación de SQL Server al instalar o cambiar el Servidor de administración. Esto puede suceder cuando el dispositivo que almacena la base de datos está fuera del dominio o cuando el Servidor de administración está instalado en la cuenta del LocalSystem.

- Para el servidor MySQL o MariaDB, especifique la cuenta y la contraseña.

Paso 8. Desempaquetar e instalar archivos en el disco duro

Después de instalar los componentes de Kaspersky Security Center, puede empezar a instalar archivos en el disco duro.

Si la instalación requiere programas adicionales, el Asistente de Instalación se lo notificará, en la página **Instalando los requisitos previos**, antes de que comience la instalación de Kaspersky Security Center. Los programas requeridos se instalan automáticamente después de hacer clic en el botón **Siguiente**.

En la última página, puede seleccionar la consola para comenzar a trabajar con Kaspersky Security Center:

- **Iniciar Consola de administración basada en MMC**
- **Iniciar Kaspersky Security Center Web Console**

  Esta opción solo está disponible si optó por instalar Kaspersky Security Center 14 Web Console en uno de los pasos anteriores.

También puede hacer clic en **Finalizar** para cerrar el Asistente sin iniciar el trabajo con Kaspersky Security Center. Puede iniciar el trabajo más adelante en cualquier momento.

En el primer inicio de la Consola de administración o Kaspersky Security Center 14 Web Console, puede realizar la instalación inicial de la aplicación.

Cuando el Asistente de instalación finalice, se instalan los siguientes componentes de la aplicación en el disco duro en el que se ha instalado el sistema operativo:

- Servidor de administración (junto con la versión de servidor del Agente de red).
- Consola de administración basada en Microsoft Management Console.
- Kaspersky Security Center 14 Web Console (si decidiera instalarlo).
- Complementos de administración de aplicaciones disponibles en el kit de distribución.

Además, se instalará Microsoft Windows Installer 4.5 si no se ha instalado anteriormente.

Instalación personalizada

La instalación personalizada es una instalación del Servidor de administración durante la que se le solicita seleccionar qué componentes instalar y especificar la carpeta donde se debe instalar la aplicación.

Con este tipo de instalación, puede configurar la base de datos y el Servidor de administración, así como instalar componentes que no están incluidos en los complementos de instalación o administración estándar para varias aplicaciones de seguridad de Kaspersky. También puede activar la Administración de dispositivos móviles.

Para instalar el Servidor de administración de Kaspersky Security Center en un dispositivo local, siga estos pasos:

Ejecute el archivo ejecutable ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe.

Se abre una ventana que le solicita que seleccione las aplicaciones Kaspersky que desea instalar. En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar el Servidor de administración de Kaspersky Security Center 14** para iniciar el Asistente de instalación del Servidor de administración. Siga las instrucciones del Asistente.

Paso 1. Revisión del Contrato de licencia y la Política de privacidad

En este paso del Asistente de instalación, debe leer el Contrato de licencia, que se formaliza entre Kaspersky y usted, así como la Política de privacidad.

También es posible que se le solicite que consulte los Contratos de licencia y las Políticas de privacidad para los complementos de administración de aplicaciones disponibles en el kit de distribución de Kaspersky Security Center.

Lea detenidamente el siguiente Contrato de licencia y la Política de privacidad. Si acepta todas las condiciones del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido por completo, y que acepto lo siguiente**:

- **Los términos y condiciones de este EULA**
- **La Política de privacidad que describe la gestión de los datos**

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación de la aplicación haciendo clic en el botón **Cancelar**.

Paso 2. Selección de un método de instalación

En la ventana de selección del tipo de instalación, especifique **Personalizado**.

La instalación personalizada le permite modificar la configuración de Kaspersky Security Center, como la ruta a la carpeta compartida, las cuentas y los puertos para la conexión con el Servidor de administración y la configuración de la base de datos. La instalación personalizada le permite especificar qué complementos de administración de Kaspersky instalar. Durante la instalación personalizada, puede crear paquetes de instalación para dispositivos móviles al habilitar la opción correspondiente.

Paso 3. Seleccionar los componentes que desea instalar

Seleccione los componentes del Servidor de administración de Kaspersky Security Center que desee instalar:

- **Administración de dispositivos móviles**. Seleccione esta casilla si debe crear paquetes de instalación para dispositivos móviles cuando el Asistente de instalación de Kaspersky Security Center se está ejecutando. También puede crear paquetes de instalación para dispositivos móviles manualmente, tras la instalación del Servidor de administración, usando las herramientas de la Consola de administración.
- **Agente de SNMP**. Este componente recibe información estadística para el Servidor de administración a través del protocolo SNMP. El componente se encuentra disponible si la aplicación está instalada en un dispositivo con SNMP instalado.

  Una vez que Kaspersky Security Center esté instalado, los archivos .mib que se requieren para recibir estadísticas se encontrarán en la subcarpeta SNMP de la carpeta de instalación de la aplicación.

El Agente de red y la Consola de administración no aparecen en la lista de componentes. Estos componentes se instalan automáticamente y la instalación no se puede cancelar.

En este paso, debe especificar una carpeta de instalación de los componentes del Servidor de administración. De forma predeterminada, los componentes se instalan en <Unidad de disco>:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center. Si dicha carpeta no existe, la carpeta se crea automáticamente durante la instalación. Puede cambiar la carpeta de destino con el botón **Examinar**.

Paso 4. Instalar Kaspersky Security Center 14 Web Console

Este paso se muestra solo si está utilizando un sistema operativo de 64 bits. De lo contrario, este paso no se muestra, porque Kaspersky Security Center 14 Web Console no funciona con sistemas operativos de 32 bits.

De forma predeterminada, se instalarán tanto Kaspersky Security Center 14 Web Console como la consola de administración basada en MMC.

Si solo desea instalar Kaspersky Security Center 14 Web Console:

1. Seleccione **Instalar solo este**.
2. Elija la **consola basada en Web** en la lista desplegable.

La instalación de Kaspersky Security Center 14 Web Console se inicia automáticamente después de completar la instalación del Servidor de Administración.

Si quiere instalar solo la consola basada en MMC:

1. Seleccione **Instalar solo este**.
2. Elija la **consola basada en MMC** en la lista desplegable.

Paso 5. Selección del tamaño de la red

Especifique el tamaño de la red en la que se está instalando Kaspersky Security Center. Según el número de dispositivos en la red, el Asistente configura la instalación y el aspecto de la interfaz de la aplicación para que coincidan.

En la siguiente tabla se muestran los parámetros de instalación de la aplicación y los parámetros del aspecto de la interfaz que se ajustan según los distintos tamaños de red.

Dependencia de la configuración de instalación en la escala de red seleccionada

Configuración	1 a 100 dispositivos	101 a 1000 dispositivos	1001 a 5000 dispositivos	Más de 5000 dispositivos
Visualizar en el árbol de la consola el nodo de Servidores de administración esclavos y virtuales y todas las configuraciones relacionadas con los Servidores esclavos y virtuales	No disponible	No disponible	Disponible	Disponible
Visualizar las secciones **Seguridad** en las ventanas de propiedades del Servidor de	No disponible	No disponible	Disponible	Disponible

administración y los grupos de administración				
Distribución aleatoria del tiempo de inicio de la tarea de actualización en los dispositivos cliente	No disponible	Sobre un intervalo de 5 minutos	Sobre un intervalo de 10 minutos	Sobre un intervalo de 10 minutos

Si conecta el Servidor de administración a un servidor de bases de datos MySQL 5.7 o SQL Express, recomendamos que no use la aplicación para administrar más de 10 000 dispositivos. Para el sistema de administración de bases de datos MariaDB, el número máximo recomendado de dispositivos administrados es 20 000.

Paso 6. Selección de una base de datos

En este paso del Asistente, debe seleccionar el mecanismo [Microsoft SQL Server (SQL Express) o MySQL] que se utilizarán para almacenar la base de datos del Servidor de administración. La opción MySQL es relevante tanto para MySQL como para MariaDB.

Se recomienda instalar el Servidor de administración en un servidor dedicado, y no en un controlador de dominio. Sin embargo, si instala Kaspersky Security Center en un servidor que actúe como controlador de dominio de solo lectura (RODC), Microsoft SQL Server (SQL Express) no se debe instalar de manera local (en el mismo dispositivo). En este caso, le recomendamos que instale Microsoft SQL Server (SQL Express) de forma remota (en un dispositivo diferente), o que use MySQL o MariaDB si necesita instalar el DBMS de manera local.

La estructura de la base de datos del Servidor de administración se proporciona en el archivo klakdb.chm, que se encuentra en la carpeta de instalación de Kaspersky Security Center (este archivo también está disponible en el portal de Kaspersky: klakdb.zip).

Paso 7. Configuración de SQL Server

En este paso del Asistente se configura el SQL Server.

Según la base de datos que haya seleccionado, especifique los siguientes ajustes:

- Si ha seleccionado **Microsoft SQL Server (SQL Server Express)** en el paso anterior:
  - En el campo **Nombre de la instancia de SQL Server**, especifique el nombre del equipo de SQL Server en la red. Para ver una lista de todos los SQL Server instalados en la red, haga clic en el botón **Examinar**. Este campo está en blanco de forma predeterminada.

    Si se conecta a SQL Server a través de un puerto personalizado, junto con el nombre de host de SQL Server especifique el número de puerto separado con una coma, por ejemplo:

    ```
    SQL_Server_host_name,1433
    ```

    Si protege la comunicación entre el Servidor de administración y SQL Server por medio de un certificado, especifique en el campo **Nombre de instancia de SQL Server** el mismo nombre de host que se utilizó al generar del certificado. Si utiliza una instancia de SQL Server con nombre, junto con el nombre de host de SQL Server especifique el número de puerto separado con una coma, por ejemplo:

    ```
    SQL_Server_name,1433
    ```

Si usa varias instancias de SQL Server en el mismo host, especifique también el nombre de la instancia separado con una barra diagonal inversa, por ejemplo:

```
SQL_Server_name\SQL_Server_instance_name,1433
```

Si un SQL Server de la red empresarial tiene activada la función Always On, especifique el nombre del agente de escucha del grupo de disponibilidad en el campo **Nombre de la instancia de SQL Server**. Tenga en cuenta que el Servidor de administración solo admite el modo de disponibilidad de confirmación síncrona cuando la función Always On está activada.

- En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.
- Si ha seleccionado **MySQL** en el paso anterior:
  - En el campo **Nombre de la instancia de SQL Server**, especifique el nombre de la instancia de SQL Server. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.
  - En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con la base de datos de SQL Server. El número de puerto predeterminado es el 3306.
  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

Si en esta etapa desea instalar SQL Server en el dispositivo desde el cual está instalando Kaspersky Security Center, debe detener la instalación y reiniciarla después de la instalación de SQL Server. Las versiones admitidas de SQL Server figuran en los requisitos del sistema.

Si está instalando SQL Server en un dispositivo remoto, no es preciso interrumpir el Asistente de Instalación de Kaspersky Security Center. Instale SQL Server y reanude la instalación de Kaspersky Security Center.

Paso 8. Selección de un modo de autenticación

Determine el modo de autenticación que se utilizará cuando el Servidor de administración se conecte SQL Server.

Según la base de datos seleccionada, puede elegir entre los siguientes modos de autenticación.

- Para SQL Express o Microsoft SQL Server seleccione una de las siguientes opciones:
  - **Modo de autenticación de Microsoft Windows**. La verificación de permisos utiliza la cuenta que se utiliza para iniciar el Servidor de administración.
  - **Modo de autenticación de SQL Server**. Si selecciona esta opción, se utiliza la cuenta especificada en la ventana para verificar los derechos de acceso. Rellene los campos **Cuenta** y **Contraseña**.

    Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

  Para ambos modos de autenticación, la aplicación verifica si la base de datos está disponible. Si la base de datos no está disponible, se muestra un mensaje de error y debe proporcionar las credenciales correctas.

Si la base de datos del Servidor de administración se almacena en otro dispositivo y la cuenta del Servidor de administración no tiene acceso al servidor de la base de datos, debe usar el modo de autenticación de SQL Server al instalar o cambiar el Servidor de administración. Esto puede suceder cuando el dispositivo que almacena la base de datos está fuera del dominio o cuando el Servidor de administración está instalado en la cuenta del LocalSystem.

- Para el servidor MySQL o MariaDB, especifique la cuenta y la contraseña.

Paso 9. Selección de una cuenta para iniciar el Servidor de administración

Seleccione una cuenta que se utilizará para iniciar el Servidor de administración como un servicio.

- **Generar automáticamente la cuenta**. La aplicación crea una cuenta llamada KL-AK-* en la que se ejecutará el servicio kladminserver.

  Puede seleccionar esta opción si planea localizar la carpeta compartida y el DBMS en el mismo dispositivo que el Servidor de administración.

- **Seleccionar cuenta**. El servicio del Servidor de administración (kladminserver) se ejecutará en la cuenta seleccionada.

  Tendrá que seleccionar una cuenta de dominio si, por ejemplo, planea usar como DBMS una instancia de SQL Server de alguna versión, incluido SQL Express, que se encuentra en otro dispositivo o está planeando localizar la carpeta compartida en otro dispositivo.

  A partir de la versión 10 Service Pack 3, Kaspersky Security Center es compatible con cuentas de servicios administrados (MSA) y cuentas de servicios administrados en grupo (gMSA). Si estos tipos de cuentas se utilizan en su dominio, puede seleccionar una como la cuenta para el servicio del Servidor de administración.

  Antes de especificar MSA o gMSA, debe instalar la cuenta en el mismo dispositivo en el que desea instalar el Servidor de administración. Si la cuenta aún no está instalada, cancele la instalación del Servidor de administración, instale la cuenta y luego reinicie la instalación del Servidor de administración. Para obtener detalles sobre la instalación de cuentas de servicio administradas en un dispositivo local, consulte la documentación oficial de Microsoft.

  Para especificar MSA o gMSA:

  1. Haga clic en el botón **Examinar**.
  2. En la ventana que se abre, haga clic en el botón **Tipo de objeto**.
  3. Seleccione el tipo **Cuenta de servicios** y haga clic en **Aceptar**.
  4. Seleccione la cuenta correspondiente y haga clic en **Aceptar**.

La cuenta que seleccionó debe tener permisos diferentes, según el DBMS que planee utilizar.

Por razones de seguridad, no asigne el estado privilegiado a la cuenta en la que se ejecuta el Servidor de administración.

Si más adelante decide cambiar la cuenta del Servidor de administración, puede usar la utilidad de cambio de cuenta del Servidor de administración (klsrvswch).

Paso 10. Selección de una cuenta para ejecutar los servicios de Kaspersky Security Center

Seleccione la cuenta bajo la cual se ejecutarán los servicios de Kaspersky Security Center en este dispositivo:

- **Generar automáticamente la cuenta**. Kaspersky Security Center crea una cuenta local denominada KlScSvc en este dispositivo, dentro del grupo kladmins. Los servicios de Kaspersky Security Center se prestarán con la cuenta que se ha creado.
- **Seleccionar cuenta**. Los servicios de Kaspersky Security Center se ejecutarán en la cuenta que ha seleccionado.

  Tendrá que seleccionar una cuenta de dominio si, por ejemplo, tiene intención de guardar informes en una carpeta ubicada en un dispositivo diferente o si la directiva de seguridad de su organización le obliga a ello. También puede tener que seleccionar una cuenta de dominio si instala el Servidor de administración en un clúster de conmutación por error.

Por razones de seguridad, no conceda el estado privilegiado a la cuenta en la que se ejecutan los servicios.

El servicio del Servidor proxy de KSN (ksnproxy), el servicio del proxy de activación de Kaspersky (klactprx) y el servicio del portal de autenticación de Kaspersky (klwebsrv) se ejecutarán en la cuenta seleccionada.

Paso 11. Seleccionar la carpeta compartida

Defina la ubicación y el nombre de la carpeta compartida que se utilizará para hacer lo siguiente:

- Almacenar los archivos necesarios para la instalación remota de aplicaciones (los archivos se copian en el Servidor de administración durante la creación de los paquetes de instalación).
- Almacenar actualizaciones que se han descargado desde un origen de actualizaciones al Servidor de administración.

El uso compartido de archivos (solo lectura) se activará para todos los usuarios.

Puede seleccionar una de las siguientes opciones:

- **Crear una carpeta compartida**. Crear una carpeta nueva. En el cuadro de texto, especifique la ruta a la carpeta.
- **Seleccionar una carpeta compartida existente**. Permite seleccionar una carpeta compartida que ya existe.

La carpeta compartida puede ser una carpeta local en el dispositivo que se utiliza para la instalación o un directorio remoto en cualquier dispositivo cliente de la red corporativa. Si hace clic en el botón **Examinar**, puede seleccionar la carpeta compartida o especificarla manualmente introduciendo su ruta UNC (por ejemplo, \\server\Share) en el campo correspondiente.

De forma predeterminada, el instalador crea una subcarpeta Share local en la carpeta de la aplicación que contiene los componentes de Kaspersky Security Center.

Paso 12. Configuración de la conexión al Servidor de administración

Configure la conexión al Servidor de administración:

- **Puerto**

  El número de puerto utilizado para conectar con el Servidor de administración.

  El número de puerto predeterminado es el 14000.

- **Puerto SSL**

  Número de puerto SSL (capa de sockets seguros) que se utilizará para conectarse de forma segura al Servidor de administración mediante SSL.

  El número de puerto predeterminado es el 13000.

- **Longitud de la clave de cifrado**

  Seleccione la longitud de la clave de cifrado: 1024 bits o 2048 bits.

  Una clave de cifrado de 1024 bits aplica una carga más pequeña en la CPU, pero se considera obsoleta porque no puede proporcionar cifrado confiable debido a sus especificaciones técnicas. Además, el hardware existente probablemente resultará incompatible con certificados de SSL que presentan claves de 1024 bits.

  Una clave de cifrado de 2048 bits cumple todos los estándares del cifrado de última generación. Sin embargo, el uso de una clave de cifrado de 2048 bits puede añadir carga en la CPU.

  Por defecto, **2048 bits (mejor seguridad)** está seleccionado.

Si el Servidor de administración se instala en un equipo que ejecuta Microsoft Windows XP Service Pack 2, el Firewall incorporado al sistema bloque los puertos TCP 13000 y 14000. Por lo tanto, para permitir acceso al Servidor de administración en el dispositivo después de la instalación, debe abrir estos puertos manualmente.

Paso 13. Definición de la dirección del Servidor de administración

Especifique la dirección del Servidor de administración mediante uno de los siguientes métodos:

- **Nombre de dominio DNS**. Puede usar este método si la red incluye un servidor DNS y los dispositivos cliente pueden usarlo para recibir la dirección del Servidor de administración.
- **Nombre NetBIOS**. Puede usar este método si los dispositivos cliente reciben la dirección del Servidor de administración a través del protocolo NetBIOS o si el servidor WINS está disponible en la red.
- **Dirección IP**. Puede usar este método si el Servidor de administración tiene una dirección IP estática que no se cambiará posteriormente.

Si instala Kaspersky Security Center en el nodo activo del clúster de conmutación por error de Kaspersky y ha creado un adaptador de red virtual al preparar los nodos del clúster, especifique la dirección IP de este adaptador. De lo contrario, introduzca la dirección IP del equilibrador de carga de terceros que utilice.

Paso 14. Dirección externa del Servidor de administración para la conexión de dispositivos móviles

Este paso del Asistente de instalación se encuentra disponible si ha seleccionado la Administración de dispositivos móviles para la instalación.

En la ventana **Dirección para conectar dispositivos móviles**, especifique la dirección externa del Servidor de administración para la conexión de dispositivos móviles que están fuera de la red local. Puede especificar la dirección IP o el Sistema de nombres de dominio (DNS) del Servidor de administración.

Paso 15. Selección de los complementos de administración de aplicaciones

Seleccione los complementos de administración de aplicaciones que deben instalarse con Kaspersky Security Center.

Para facilitar las búsquedas, los complementos se dividen en grupos según el tipo de objetos protegidos.

Paso 16. Desempaquetar e instalar archivos en el disco duro

Después de instalar los componentes de Kaspersky Security Center, puede empezar a instalar archivos en el disco duro.

Si la instalación requiere programas adicionales, el Asistente de Instalación se lo notificará, en la página **Instalando los requisitos previos**, antes de que comience la instalación de Kaspersky Security Center. Los programas requeridos se instalan automáticamente después de hacer clic en el botón **Siguiente**.

En la última página, puede seleccionar la consola para comenzar a trabajar con Kaspersky Security Center:

- **Iniciar Consola de administración basada en MMC**
- **Iniciar Kaspersky Security Center Web Console**

  Esta opción solo está disponible si optó por instalar Kaspersky Security Center 14 Web Console en uno de los pasos anteriores.

También puede hacer clic en **Finalizar** para cerrar el Asistente sin iniciar el trabajo con Kaspersky Security Center. Puede iniciar el trabajo más adelante en cualquier momento.

En el primer inicio de la Consola de administración o Kaspersky Security Center 14 Web Console, puede realizar la instalación inicial de la aplicación.

Despliegue del clúster de conmutación por error de Kaspersky

Esta sección contiene tanto información general sobre el clúster de conmutación por error de Kaspersky, como las instrucciones sobre la preparación y despliegue del clúster de conmutación por error de Kaspersky en su red.

Escenario: despliegue de un clúster de conmutación por error de Kaspersky

Un clúster de conmutación por error de Kaspersky proporciona una alta disponibilidad de Kaspersky Security Center y minimiza el tiempo de inactividad del Servidor de administración en caso de fallo. El clúster de conmutación por error se basa en dos instancias idénticas de Kaspersky Security Center instaladas en dos equipos. Una de las instancias funciona como nodo activo y la otra, como un nodo pasivo. El nodo activo gestiona la protección de los dispositivos del cliente, mientras que el pasivo está preparado para asumir todas las funciones del nodo activo en caso de que este falle. Cuando se produce un fallo, el nodo pasivo pasa a ser activo y el nodo activo pasa a ser pasivo.

Requisitos previos

Dispone de un hardware que cumple los requisitos del clúster de conmutación por error.

Etapas

El despliegue de las aplicaciones de Kaspersky se realiza en etapas:

1. **Creación de una cuenta para los servicios de Kaspersky Security Center**

   Cree un nuevo grupo de dominio (en este escenario, se utiliza el nombre "KLAdmins" para este grupo) y conceda los permisos de administrador local al grupo en ambos nodos y en el servidor de archivos. A continuación, cree dos nuevas cuentas de usuario de dominio (en este escenario, se usan los nombres "ksc" y "rightless" para estas cuentas) y añada las cuentas al grupo de dominio KLAdmins.

   Añada la cuenta de usuario, en la cual se instalará Kaspersky Security Center, al grupo de dominio KLAdmins creado anteriormente.

2. **Preparación del servidor de archivos**

   Prepare el servidor de archivos para que funcione como componente del clúster de conmutación por error de Kaspersky. Asegúrese de que el servidor de archivos cumple los requisitos de hardware y software, cree dos carpetas compartidas para los datos de Kaspersky Security Center y configure los permisos para acceder a las carpetas compartidas.

   Instrucciones: preparación de un servidor de archivos para el clúster de conmutación por error de Kaspersky

3. **Preparación de los nodos activos y pasivos**

   Prepare dos equipos con hardware y software idénticos para que funcionen como nodos activo y pasivo.

   Instrucciones: preparación de los nodos para el clúster de conmutación por error de Kaspersky

4. **Instalación del sistema de administración de bases de datos (DBMS)**

   Seleccione cualquiera de los DBMS admitidos y, a continuación, instale el DBMS en un equipo dedicado.

5. **Instalación de Kaspersky Security Center**

   Instale Kaspersky Security Center en el modo de clúster de conmutación por error en ambos nodos. Primero debe instalar Kaspersky Security Center en el nodo activo y luego, en el pasivo.

   Instrucciones: Instalación de Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky

6. **Prueba del clúster de conmutación por error**

   Compruebe que ha configurado correctamente el clúster de conmutación por error y que funciona correctamente. Por ejemplo, puede detener uno de los servicios de Kaspersky Security Center en el nodo activo: kladminserver, klnagent, ksnproxy, klactprx o klwebsrv. Una vez detenido el servicio, la administración de la protección debe pasar automáticamente al nodo pasivo.

Resultados

El clúster de conmutación por error de Kaspersky está desplegado. Por favor, familiarícese con los eventos que conducen al cambio entre los nodos activos y pasivos.

Acerca del clúster de conmutación por error de Kaspersky

El clúster de conmutación por error de Kaspersky proporciona una alta disponibilidad de Kaspersky Security Center y minimiza el tiempo de inactividad del Servidor de administración en caso de fallo. El clúster de conmutación por error se basa en dos instancias idénticas de Kaspersky Security Center instaladas en dos equipos. Una de las instancias funciona como nodo activo y la otra, como un nodo pasivo. El nodo activo gestiona la protección de los dispositivos del cliente, mientras que el pasivo está preparado para asumir todas las funciones del nodo activo en caso de que este falle. Cuando se produce un fallo, el nodo pasivo pasa a ser activo y el nodo activo pasa a ser pasivo.

Requisitos de hardware y software

Para implementar un clúster de conmutación por error de Kaspersky, debe tener el siguiente hardware:

- Dos equipos con hardware y software idénticos. Estos equipos actuarán como nodos activos y pasivos.
- Un servidor de archivos compatible con el protocolo CIFS/SMB, versión 2.0 o posterior. Debe proporcionar un equipo dedicado que actúe como servidor de archivos.

  Asegúrese de que ha proporcionado un gran ancho de banda de red entre el servidor de archivos y los nodos activos y pasivos.

- Un equipo con Sistema de administración de Bases de Datos (DBMS).

Condiciones de los interruptores

El clúster de conmutación por error cambia la administración de la protección de los dispositivos cliente del nodo activo al nodo pasivo si se produce alguno de los siguientes eventos en el nodo activo:

- El nodo activo está roto debido a un fallo de software o hardware.
- El nodo activo se detuvo temporalmente por actividades de mantenimiento.
- Al menos uno de los servicios (o procesos) de Kaspersky Security Center falló o fue cancelado deliberadamente por el usuario. Los servicios de Kaspersky Security Center son los siguientes: kladminserver, klnagent, klactprx y klwebsrv.
- Se interrumpió o terminó la conexión de red entre el nodo activo y el almacenamiento en el servidor de archivos.

Preparación de un servidor de archivos para un clúster de conmutación por error de Kaspersky

Un servidor de archivos funciona como un componente necesario de un clúster de conmutación por error de Kaspersky.

Para preparar un servidor de archivos:

1. Asegúrese de que el servidor de archivos cumple los requisitos de hardware y software.
2. Asegúrese de que el servidor de archivos y ambos nodos (activo y pasivo) están incluidos en el mismo dominio o que el servidor de archivos es el controlador del dominio.
3. En el servidor de archivos, cree dos carpetas compartidas. Uno de ellos se utiliza para mantener la información sobre el estado del clúster de conmutación por error. El otro se utiliza para almacenar los datos y la configuración de Kaspersky Security Center. Usted especificará las rutas a las carpetas compartidas mientras configura la instalación de Kaspersky Security Center.
4. Conceda permisos de acceso total (tanto permisos de uso compartido como permisos NTFS) a las carpetas compartidas creadas para las siguientes cuentas y grupos de usuarios:
   - Grupo de dominios KLAdmins.
   - Cuentas de usuario $<node1> y $<node2>. Aquí, <node1> y <node2> son los nombres de los equipos de los nodos activos y pasivos.

El servidor de archivos está preparado. Para desplegar el clúster de conmutación por error de Kaspersky, siga las instrucciones de este escenario.

Preparación de nodos para un clúster de conmutación por error de Kaspersky

Prepare dos equipos para que funcionen como nodos activos y pasivos de un clúster de conmutación por error de Kaspersky.

Para preparar los nodos para un clúster de conmutación por error de Kaspersky:

1. Asegúrese de que tienes dos equipos que cumplen los requisitos de hardware y software. Estos equipos actuarán como nodos activos y pasivos del clúster de conmutación por error.
2. Asegúrese de que el servidor de archivos y ambos nodos están incluidos en el mismo dominio.
3. Realice una de las siguientes acciones:
   - En cada uno de los nodos, cree un adaptador de red virtual. Puede hacerlo mediante un software de terceros.

     Asegúrese de que se cumplen las siguientes condiciones:

     - Los adaptadores de red virtuales deben estar desactivados. Puede crear los adaptadores de red virtuales en estado desactivado o desactivarlos después de su creación.

- Los adaptadores de red virtuales de ambos nodos deben tener la misma dirección IP.

- Utilice un equilibrador de carga de terceros. Por ejemplo, puede utilizar un servidor nginx. En este caso, haga lo siguiente:

  a. Proporcione un equipo dedicado basado en Linux con nginx instalado.

  b. Configure el equilibrio de carga. Establezca el nodo activo como servidor principal y el nodo pasivo como servidor de reserva.

  c. En el servidor nginx, abra todos los puertos del Servidor de administración: TCP 13000, UDP 13000, TCP 13291, TCP 13299 y TCP 17000.

4. Reinicie ambos nodos y el servidor de archivos.

5. Asigne las dos carpetas compartidas, que creó durante el paso de preparación del servidor de archivos, a cada uno de los nodos. Debe asignar las carpetas compartidas como unidades de red. Al asignar las carpetas, puede seleccionar cualquier letra de unidad vacía. Para acceder a las carpetas compartidas, utilice las credenciales de la cuenta de usuario que creó durante el paso 1 del escenario.

Los nodos están preparados. Para desplegar el clúster de conmutación por error de Kaspersky, siga las instrucciones del escenario.

Instalación de Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky

Se instala Kaspersky Security Center en ambos nodos del clúster de conmutación por error de Kaspersky por separado. Primero se instala la aplicación en el nodo activo y luego en el pasivo. Durante la instalación, elige el nodo que será el activo y el que será el pasivo.

Solo un usuario del grupo de dominio KLAdmins puede instalar Kaspersky Security Center en cada nodo.

Para instalar Kaspersky Security Center en el nodo activo del clúster de conmutación por error de Kaspersky:

1. Ejecute el archivo ejecutable ksc_14.<número de compilación>_full_<idioma>.exe.

   Se abre una ventana y le solicita que seleccione las aplicaciones Kaspersky que desea instalar. En la ventana de selección de aplicación, haga clic en el enlace **Instalación del Servidor de administración de Kaspersky Security Center 14** para iniciar el Asistente de instalación del Servidor de administración. Siga las instrucciones del Asistente.

2. Lea detenidamente el siguiente Contrato de licencia y la Política de privacidad. Si acepta todas las condiciones del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido por completo, y que acepto lo siguiente**:

   - **Los términos y condiciones de este EULA**

   - **La Política de privacidad que describe la gestión de los datos**

   La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

   Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación de la aplicación haciendo clic en el botón **Cancelar**.

3. Seleccione **Nodo principal del clúster de Kaspersky Failover** para instalar la aplicación en el nodo activo.

4. En la ventana **Carpeta compartida**, debe hacer lo siguiente:

   - En los campos **Estado compartido** y **Datos compartidos**, especifique las rutas de las carpetas compartidas que creó en el servidor de archivos durante su preparación.
   - En los campos **Unidad de estado compartido** y **Unidad de datos compartidos**, seleccione las unidades de red a las que asignó las carpetas compartidas durante la preparación de los nodos.
   - Seleccione el modo de conectividad del clúster: mediante un adaptador de red virtual o un equilibrador de carga de terceros.

5. Realice los demás pasos de la instalación personalizada, comenzando por el paso 3.

   En el paso 13, especifique la dirección IP de un adaptador de red virtual si ha creado un adaptador al preparar los nodos del clúster. De lo contrario, introduzca la dirección IP del equilibrador de carga de terceros que utilice.

Kaspersky Security Center se ha instalado en el nodo activo.

Para instalar Kaspersky Security Center en el nodo pasivo del clúster de conmutación por error de Kaspersky:

1. Ejecute el archivo ejecutable ksc_14.<número de compilación>_full_<idioma>.exe.

   Se abre una ventana y le solicita que seleccione las aplicaciones Kaspersky que desea instalar. En la ventana de selección de aplicación, haga clic en el enlace **Instalación del Servidor de administración de Kaspersky Security Center 14** para iniciar el Asistente de instalación del Servidor de administración. Siga las instrucciones del Asistente.

2. Lea detenidamente el siguiente Contrato de licencia y la Política de privacidad. Si acepta todas las condiciones del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido por completo, y que acepto lo siguiente**:

   - **Los términos y condiciones de este EULA**
   - **La Política de privacidad que describe la gestión de los datos**

   La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

   Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación de la aplicación haciendo clic en el botón **Cancelar**.

3. Seleccione **Nodo secundario del clúster de Kaspersky Failover** para instalar la aplicación en el nodo pasivo.

4. En la ventana **Carpeta compartida**, en el campo **Estado compartido**, especifique una ruta a la carpeta compartida con información sobre el estado del clúster que creó en el servidor de archivos durante su preparación.

5. Haga clic en el botón **Instalar**. Cuando termine la instalación, haga clic en el botón **Finalizar**.

Kaspersky Security Center se ha instalado en el nodo pasivo. Ahora, puede probar el clúster de conmutación por error de Kaspersky para asegurarse de que lo configuró correctamente y de que el clúster funciona bien.

Inicio y detención manual de nodos del clúster

Es posible que tenga que detener todo el clúster de conmutación por error de Kaspersky o separar temporalmente uno de los nodos del clúster para su mantenimiento. En este caso, siga las instrucciones de esta sección. No intente iniciar o detener los servicios o procesos relacionados con el clúster de conmutación por error con cualquier otro medio. Esto puede causar la pérdida de datos.

Inicio y detención de todo el clúster de conmutación por error para su mantenimiento detención

Para iniciar o detener todo el clúster de conmutación por error:

1. En el nodo activo, vaya a <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Abra la línea de comandos y ejecute uno de los siguientes comandos:
   - Para detener el clúster, ejecute: `klfoc -stopcluster --stp klfoc`
   - Para iniciar el clúster, ejecute: `klfoc -startcluster --stp klfoc`

Se inicia o se detiene el clúster de conmutación por error, dependiendo del comando que se ejecute.

Mantenimiento de uno de los nodos

Para el mantenimiento de uno de los nodos:

1. En el nodo activo, detenga el clúster de conmutación por error con el comando `klfoc -stopcluster --stp klfoc`.
2. En el nodo que desea mantener, vaya a <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Abra la línea de comandos y, a continuación, separe el nodo del clúster con el comando `detach_node.cmd`.
4. En el nodo activo, inicie el clúster de conmutación por error con el comando `klfoc -startcluster --stp klfoc`.
5. Actividades de mantenimiento.
6. En el nodo activo, detenga el clúster de conmutación por error con el comando `klfoc -stopcluster --stp klfoc`.
7. En el nodo que se actualizó, vaya a <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
8. Abra la línea de comandos y, a continuación, adjunte el nodo al clúster ejecutando el comando `attach_node.cmd`.
9. En el nodo activo, inicie el clúster de conmutación por error con el comando `klfoc -startcluster --stp klfoc`.

El nodo se mantiene y se adjunta al clúster de conmutación por error.

Instalación del Servidor de administración en un clúster de conmutación por error de Microsoft

El procedimiento de instalación del Servidor de administración en un clúster de conmutación por error difiere de la instalación estándar y personalizada en un dispositivo independiente.

Realice el procedimiento descrito en esta sección en el nodo que contiene un almacenamiento de datos común del clúster.

Para instalar el Servidor de administración de Kaspersky Security Center en un clúster:

Ejecute el archivo ejecutable ksc_<número de versión>.<número de compilación>_full_<idioma de localización>.exe.

Se abre una ventana que le solicita que seleccione las aplicaciones Kaspersky que desea instalar. En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar el Servidor de administración de Kaspersky Security Center 14** para iniciar el Asistente de instalación del Servidor de administración. Siga las instrucciones del Asistente.

Paso 1. Revisión del Contrato de licencia y la Política de privacidad

En este paso del Asistente de instalación, debe leer el Contrato de licencia, que se formaliza entre Kaspersky y usted, así como la Política de privacidad.

También es posible que se le solicite que consulte los Contratos de licencia y las Políticas de privacidad para los complementos de administración de aplicaciones disponibles en el kit de distribución de Kaspersky Security Center.

Lea detenidamente el siguiente Contrato de licencia y la Política de privacidad. Si acepta todas las condiciones del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido por completo, y que acepto lo siguiente**:

- **Los términos y condiciones de este EULA**
- **La Política de privacidad que describe la gestión de los datos**

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

Si no acepta el Contrato de licencia o la Política de privacidad, cancele la instalación de la aplicación haciendo clic en el botón **Cancelar**.

Paso 2. Seleccionar el tipo de instalación en un clúster

Seleccione el tipo de instalación en el clúster:

- **Clúster (instalar en todos los nodos del clúster)**

  Esta es la opción recomendada. Si selecciona esta opción, el Servidor de administración se instalará al mismo tiempo en todos los nodos del clúster.

- **Localmente (instalar solo en este dispositivo)**

  Si selecciona esta opción, el Servidor de administración se instalará solo en el nodo actual, como si fuera un servidor independiente, y el Servidor de administración no funcionará como una aplicación compatible con clústeres. Por ejemplo, es posible que desee elegir esta opción para ahorrar espacio de almacenamiento compartido, si la tolerancia a fallos no es necesaria para el Servidor de administración. En caso de falla del nodo en uso, deberá instalar el Servidor de administración en otro nodo y restaurar el estado del Servidor de administración desde una copia de seguridad.

  Los siguientes pasos son los mismos que cuando utiliza el método de instalación estándar o personalizado, comenzando desde el paso de selección del método de instalación.

Paso 3. Especificar el nombre del Servidor de administración virtual

Especifique el nombre de red del nuevo Servidor de administración virtual. Podrá utilizar este nombre para conectar la Consola de administración o Kaspersky Security Center 14 Web Console al Servidor de administración.

El nombre que especifique debe se diferente del nombre del clúster.

Paso 4. Especificar los detalles de la red del Servidor de administración virtual

Para especificar los detalles de la red de la nueva instancia del Servidor de administración virtual:

1. En **Red para usar**, seleccione la red de dominio a la que está conectado el nodo del clúster en uso.
2. Realice una de las siguientes acciones:
   - Si en la red seleccionada se usa DHCP para asignar direcciones IP, seleccione la opción **Usar DHCP**.
   - Si no se utiliza DHCP en la red seleccionada, especifique la dirección IP requerida.

     La dirección IP que especifique debe ser diferente de la dirección IP del clúster.
3. Haga clic en **Agregar** para aplicar la configuración especificada.

Podrá utilizar la dirección IP asignada automáticamente o la especificada para conectar la Consola de administración o Kaspersky Security Center Web Console al Servidor de administración.

Paso 5. Especificar un grupo de clústeres

Un grupo de clústeres es una función especial de clúster de conmutación por error que contiene recursos comunes para todos los nodos. Tiene dos opciones:

- Crear un nuevo grupo de clústeres.

  Esta opción se recomienda en la mayoría de los casos. El nuevo grupo de clústeres contendrá todos los recursos comunes relacionados con la instancia del Servidor de administración.

- Seleccionar un grupo de clústeres existente.

Seleccione esta opción si desea utilizar un recurso común que ya está asociado con un grupo de clústeres existente. Por ejemplo, es posible que desee utilizar esta opción si desea utilizar un almacenamiento asociado con un grupo de clústeres existente y si no hay otro almacenamiento disponible para un nuevo grupo de clústeres.

Paso 6. Seleccionar un almacenamiento de datos de clúster

Para seleccionar un almacenamiento de datos de clúster:

1. En **Repositorios disponibles**, seleccione el almacenamiento de datos en el que se instalarán los recursos comunes de la instancia del Servidor de administración virtual.
2. Si el almacenamiento de datos seleccionado contiene varios volúmenes, en **Secciones disponibles en la unidad de disco**, seleccione el volumen requerido.
3. En **Ruta de instalación**, ingrese la ruta del almacenamiento de datos común en el que se instalarán los recursos de la instancia del Servidor de administración virtual.

El almacenamiento de datos queda seleccionado.

Paso 7. Especificar una cuenta para la instalación remota

Especifique el nombre de usuario y la contraseña que se utilizarán para la instalación remota de la instancia del Servidor de administración virtual en un nodo pasivo del clúster.

La cuenta que especifique debe tener privilegios administrativos en todos los nodos del clúster.

Paso 8. Seleccionar los componentes que desea instalar

Seleccione los componentes del Servidor de administración de Kaspersky Security Center que desee instalar:

- **Administración de dispositivos móviles**. Seleccione esta casilla si debe crear paquetes de instalación para dispositivos móviles cuando el Asistente de instalación de Kaspersky Security Center se está ejecutando. También puede crear paquetes de instalación para dispositivos móviles manualmente, tras la instalación del Servidor de administración, usando las herramientas de la Consola de administración.
- **Agente de SNMP**. Este componente recibe información estadística para el Servidor de administración a través del protocolo SNMP. El componente se encuentra disponible si la aplicación está instalada en un dispositivo con SNMP instalado.

  Una vez que Kaspersky Security Center esté instalado, los archivos .mib que se requieren para recibir estadísticas se encontrarán en la subcarpeta SNMP de la carpeta de instalación de la aplicación.

El Agente de red y la Consola de administración no aparecen en la lista de componentes. Estos componentes se instalan automáticamente y la instalación no se puede cancelar.

En este paso, debe especificar una carpeta de instalación de los componentes del Servidor de administración. De forma predeterminada, los componentes se instalan en <Unidad de disco>:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center. Si dicha carpeta no existe, la carpeta se crea automáticamente durante la instalación. Puede cambiar la carpeta de destino con el botón **Examinar**.

Paso 9. Selección del tamaño de la red

Especifique el tamaño de la red en la que se está instalando Kaspersky Security Center. Según el número de dispositivos en la red, el Asistente configura la instalación y el aspecto de la interfaz de la aplicación para que coincidan.

En la siguiente tabla se muestran los parámetros de instalación de la aplicación y los parámetros del aspecto de la interfaz que se ajustan según los distintos tamaños de red.

Dependencia de la configuración de instalación en la escala de red seleccionada

Configuración	1 a 100 dispositivos	101 a 1000 dispositivos	1001 a 5000 dispositivos	Más de 5000 dispositivos
Visualizar en el árbol de la consola el nodo de Servidores de administración esclavos y virtuales y todas las configuraciones relacionadas con los Servidores esclavos y virtuales	No disponible	No disponible	Disponible	Disponible
Visualizar las secciones **Seguridad** en las ventanas de propiedades del Servidor de administración y los grupos de administración	No disponible	No disponible	Disponible	Disponible
Distribución aleatoria del tiempo de inicio de la tarea de actualización en los dispositivos cliente	No disponible	Sobre un intervalo de 5 minutos	Sobre un intervalo de 10 minutos	Sobre un intervalo de 10 minutos

Si conecta el Servidor de administración a un servidor de bases de datos MySQL 5.7 o SQL Express, recomendamos que no use la aplicación para administrar más de 10 000 dispositivos. Para el sistema de administración de bases de datos MariaDB, el número máximo recomendado de dispositivos administrados es 20 000.

Paso 10. Seleccionar una base de datos

En este paso del Asistente, debe seleccionar el mecanismo [Microsoft SQL Server (SQL Express) o MySQL] que se utilizarán para almacenar la base de datos del Servidor de administración. La opción MySQL es relevante tanto para MySQL como para MariaDB.

Se recomienda instalar el Servidor de administración en un servidor dedicado, y no en un controlador de dominio. Sin embargo, si instala Kaspersky Security Center en un servidor que actúe como controlador de dominio de solo lectura (RODC), Microsoft SQL Server (SQL Express) no se debe instalar de manera local (en el mismo dispositivo). En este caso, le recomendamos que instale Microsoft SQL Server (SQL Express) de forma remota (en un dispositivo diferente), o que use MySQL o MariaDB si necesita instalar el DBMS de manera local.

La estructura de la base de datos del Servidor de administración se proporciona en el archivo klakdb.chm, que se encuentra en la carpeta de instalación de Kaspersky Security Center (este archivo también está disponible en el portal de Kaspersky: klakdb.zip).

Paso 11. Configuración de SQL Server

En este paso del Asistente se configura el SQL Server.

Según la base de datos que haya seleccionado, especifique los siguientes ajustes:

- Si ha seleccionado **Microsoft SQL Server (SQL Server Express)** en el paso anterior:

  - En el campo **Nombre de la instancia de SQL Server**, especifique el nombre del equipo de SQL Server en la red. Para ver una lista de todos los SQL Server instalados en la red, haga clic en el botón **Examinar**. Este campo está en blanco de forma predeterminada.

    Si se conecta a SQL Server a través de un puerto personalizado, junto con el nombre de host de SQL Server especifique el número de puerto separado con una coma, por ejemplo:

    ```
    SQL_Server_host_name,1433
    ```

    Si protege la comunicación entre el Servidor de administración y SQL Server por medio de un certificado, especifique en el campo **Nombre de instancia de SQL Server** el mismo nombre de host que se utilizó al generar del certificado. Si utiliza una instancia de SQL Server con nombre, junto con el nombre de host de SQL Server especifique el número de puerto separado con una coma, por ejemplo:

    ```
    SQL_Server_name,1433
    ```

    Si usa varias instancias de SQL Server en el mismo host, especifique también el nombre de la instancia separado con una barra diagonal inversa, por ejemplo:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

Si un SQL Server de la red empresarial tiene activada la función Always On, especifique el nombre del agente de escucha del grupo de disponibilidad en el campo **Nombre de la instancia de SQL Server**. Tenga en cuenta que el Servidor de administración solo admite el modo de disponibilidad de confirmación síncrona cuando la función Always On está activada.

- En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

- Si ha seleccionado **MySQL** en el paso anterior:

  - En el campo **Nombre de la instancia de SQL Server**, especifique el nombre de la instancia de SQL Server. De forma predeterminada, el nombre es la dirección IP del dispositivo en el cual se debe instalar Kaspersky Security Center.

  - En el campo **Puerto**, especifique el puerto para la conexión del Servidor de administración con la base de datos de SQL Server. El número de puerto predeterminado es el 3306.

  - En el campo **Nombre de la base de datos**, especifique el nombre de la base de datos que se creará para almacenar los datos del Servidor de administración. El valor predeterminado es *KAV*.

Si en esta etapa desea instalar SQL Server en el dispositivo desde el cual está instalando Kaspersky Security Center, debe detener la instalación y reiniciarla después de la instalación de SQL Server. Las versiones admitidas de SQL Server figuran en los requisitos del sistema.

Si está instalando SQL Server en un dispositivo remoto, no es preciso interrumpir el Asistente de Instalación de Kaspersky Security Center. Instale SQL Server y reanude la instalación de Kaspersky Security Center.

Paso 12. Selección de un modo de autenticación

Determine el modo de autenticación que se utilizará cuando el Servidor de administración se conecte SQL Server.

Según la base de datos seleccionada, puede elegir entre los siguientes modos de autenticación.

- Para SQL Express o Microsoft SQL Server seleccione una de las siguientes opciones:

  - **Modo de autenticación de Microsoft Windows**. La verificación de permisos utiliza la cuenta que se utiliza para iniciar el Servidor de administración.

  - **Modo de autenticación de SQL Server**. Si selecciona esta opción, se utiliza la cuenta especificada en la ventana para verificar los derechos de acceso. Rellene los campos **Cuenta** y **Contraseña**.

    Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

  Para ambos modos de autenticación, la aplicación verifica si la base de datos está disponible. Si la base de datos no está disponible, se muestra un mensaje de error y debe proporcionar las credenciales correctas.

  Si la base de datos del Servidor de administración se almacena en otro dispositivo y la cuenta del Servidor de administración no tiene acceso al servidor de la base de datos, debe usar el modo de autenticación de SQL Server al instalar o cambiar el Servidor de administración. Esto puede suceder cuando el dispositivo que almacena la base de datos está fuera del dominio o cuando el Servidor de administración está instalado en la cuenta del LocalSystem.

- Para el servidor MySQL o MariaDB, especifique la cuenta y la contraseña.

Paso 13. Selección de una cuenta para iniciar el Servidor de administración

Seleccione una cuenta que se utilizará para iniciar el Servidor de administración como un servicio.

- **Generar automáticamente la cuenta**. La aplicación crea una cuenta llamada KL-AK-* en la que se ejecutará el servicio kladminserver.

  Puede seleccionar esta opción si planea localizar la carpeta compartida y el DBMS en el mismo dispositivo que el Servidor de administración.

- **Seleccionar cuenta**. El servicio del Servidor de administración (kladminserver) se ejecutará en la cuenta seleccionada.

  Tendrá que seleccionar una cuenta de dominio si, por ejemplo, planea usar como DBMS una instancia de SQL Server de alguna versión, incluido SQL Express, que se encuentra en otro dispositivo o está planeando localizar la carpeta compartida en otro dispositivo.

  A partir de la versión 10 Service Pack 3, Kaspersky Security Center es compatible con cuentas de servicios administrados (MSA) y cuentas de servicios administrados en grupo (gMSA). Si estos tipos de cuentas se utilizan en su dominio, puede seleccionar una como la cuenta para el servicio del Servidor de administración.

  Antes de especificar MSA o gMSA, debe instalar la cuenta en el mismo dispositivo en el que desea instalar el Servidor de administración. Si la cuenta aún no está instalada, cancele la instalación del Servidor de administración, instale la cuenta y luego reinicie la instalación del Servidor de administración. Para obtener detalles sobre la instalación de cuentas de servicio administradas en un dispositivo local, consulte la documentación oficial de Microsoft.

Para especificar MSA o gMSA:

1. Haga clic en el botón **Examinar**.
2. En la ventana que se abre, haga clic en el botón **Tipo de objeto**.
3. Seleccione el tipo **Cuenta de servicios** y haga clic en **Aceptar**.
4. Seleccione la cuenta correspondiente y haga clic en **Aceptar**.

La cuenta que seleccionó debe tener permisos diferentes, según el DBMS que planee utilizar.

Por razones de seguridad, no asigne el estado privilegiado a la cuenta en la que se ejecuta el Servidor de administración.

Si más adelante decide cambiar la cuenta del Servidor de administración, puede usar la utilidad de cambio de cuenta del Servidor de administración (klsrvswch).

Paso 14. Selección de una cuenta para ejecutar los servicios de Kaspersky Security Center

Seleccione la cuenta bajo la cual se ejecutarán los servicios de Kaspersky Security Center en este dispositivo:

- **Generar automáticamente la cuenta**. Kaspersky Security Center crea una cuenta local denominada KlScSvc en este dispositivo, dentro del grupo kladmins. Los servicios de Kaspersky Security Center se prestarán con la cuenta que se ha creado.
- **Seleccionar cuenta**. Los servicios de Kaspersky Security Center se ejecutarán en la cuenta que ha seleccionado.

  Tendrá que seleccionar una cuenta de dominio si, por ejemplo, tiene intención de guardar informes en una carpeta ubicada en un dispositivo diferente o si la directiva de seguridad de su organización le obliga a ello. También puede tener que seleccionar una cuenta de dominio si instala el Servidor de administración en un clúster de conmutación por error.

Por razones de seguridad, no conceda el estado privilegiado a la cuenta en la que se ejecutan los servicios.

El servicio del Servidor proxy de KSN (ksnproxy), el servicio del proxy de activación de Kaspersky (klactprx) y el servicio del portal de autenticación de Kaspersky (klwebsrv) se ejecutarán en la cuenta seleccionada.

Paso 15. Seleccionar la carpeta compartida

Defina la ubicación y el nombre de la carpeta compartida que se utilizará para hacer lo siguiente:

- Almacenar los archivos necesarios para la instalación remota de aplicaciones (los archivos se copian en el Servidor de administración durante la creación de los paquetes de instalación).

- Almacenar actualizaciones que se han descargado desde un origen de actualizaciones al Servidor de administración.

El uso compartido de archivos (solo lectura) se activará para todos los usuarios.

Puede seleccionar una de las siguientes opciones:

- **Crear una carpeta compartida**. Crear una carpeta nueva. En el cuadro de texto, especifique la ruta a la carpeta.
- **Seleccionar una carpeta compartida existente**. Permite seleccionar una carpeta compartida que ya existe.

La carpeta compartida puede ser una carpeta local en el dispositivo que se utiliza para la instalación o un directorio remoto en cualquier dispositivo cliente de la red corporativa. Si hace clic en el botón **Examinar**, puede seleccionar la carpeta compartida o especificarla manualmente introduciendo su ruta UNC (por ejemplo, \\server\Share) en el campo correspondiente.

De forma predeterminada, el instalador crea una subcarpeta Share local en la carpeta de la aplicación que contiene los componentes de Kaspersky Security Center.

Paso 16. Configuración de la conexión al Servidor de administración

Configure la conexión al Servidor de administración:

- **Puerto**

  El número de puerto utilizado para conectar con el Servidor de administración.

  El número de puerto predeterminado es el 14000.

- **Puerto SSL**

  Número de puerto SSL (capa de sockets seguros) que se utilizará para conectarse de forma segura al Servidor de administración mediante SSL.

  El número de puerto predeterminado es el 13000.

- **Longitud de la clave de cifrado**

  Seleccione la longitud de la clave de cifrado: 1024 bits o 2048 bits.

  Una clave de cifrado de 1024 bits aplica una carga más pequeña en la CPU, pero se considera obsoleta porque no puede proporcionar cifrado confiable debido a sus especificaciones técnicas. Además, el hardware existente probablemente resultará incompatible con certificados de SSL que presentan claves de 1024 bits.

  Una clave de cifrado de 2048 bits cumple todos los estándares del cifrado de última generación. Sin embargo, el uso de una clave de cifrado de 2048 bits puede añadir carga en la CPU.

  Por defecto, **2048 bits (mejor seguridad)** está seleccionado.

Si el Servidor de administración se instala en un equipo que ejecuta Microsoft Windows XP Service Pack 2, el Firewall incorporado al sistema bloque los puertos TCP 13000 y 14000. Por lo tanto, para permitir acceso al Servidor de administración en el dispositivo después de la instalación, debe abrir estos puertos manualmente.

Paso 17. Definición de la dirección del Servidor de administración

Especifique la dirección del Servidor de administración. Puede seleccionar una de las siguientes opciones:

- **Nombre de dominio DNS**. Puede usar este método si la red incluye un servidor DNS y los dispositivos cliente pueden usarlo para recibir la dirección del Servidor de administración.
- **Nombre NetBIOS**. Puede usar este método si los dispositivos cliente reciben la dirección del Servidor de administración a través del protocolo NetBIOS o si el servidor WINS está disponible en la red.
- **Dirección IP**. Puede usar este método si el Servidor de administración tiene una dirección IP estática que no se cambiará posteriormente.

Paso 18. Dirección externa del Servidor de administración para la conexión de dispositivos móviles

Este paso del Asistente de instalación se encuentra disponible si ha seleccionado la Administración de dispositivos móviles para la instalación.

En la ventana **Dirección para conectar dispositivos móviles**, especifique la dirección externa del Servidor de administración para la conexión de dispositivos móviles que están fuera de la red local. Puede especificar la dirección IP o el Sistema de nombres de dominio (DNS) del Servidor de administración.

Paso 19. Desempaquetar e instalar archivos en el disco duro

Después de instalar los componentes de Kaspersky Security Center, puede empezar a instalar archivos en el disco duro.

Si la instalación requiere programas adicionales, el Asistente de Instalación se lo notificará, en la página **Instalando los requisitos previos**, antes de que comience la instalación de Kaspersky Security Center. Los programas requeridos se instalan automáticamente después de hacer clic en el botón **Siguiente**.

En la última página, puede seleccionar la consola para comenzar a trabajar con Kaspersky Security Center:

- **Iniciar Consola de administración basada en MMC**
- **Iniciar Kaspersky Security Center Web Console**

  Esta opción solo está disponible si optó por instalar Kaspersky Security Center 14 Web Console en uno de los pasos anteriores.

También puede hacer clic en **Finalizar** para cerrar el Asistente sin iniciar el trabajo con Kaspersky Security Center. Puede iniciar el trabajo más adelante en cualquier momento.

En el primer inicio de la Consola de administración o Kaspersky Security Center 14 Web Console, puede realizar la instalación inicial de la aplicación.

Instalación del Servidor de administración en modo silencioso

El Servidor de administración se puede instalar en modo silencioso; es decir, sin la introducción interactiva de los parámetros de instalación.

Para instalar el Servidor de administración en un dispositivo local en modo no interactivo:

1. Lea el Contrato de licencia de usuario final. Utilice el siguiente comando solo si comprende y acepta las condiciones del Contrato de licencia de usuario final.

2. Lea la Política de privacidad. Solo use el siguiente comando si entiende y está de acuerdo con que sus datos serán manejados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad.

3. Ejecute el comando
   ```
   setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"
   ```

donde `setup_parameters` es una lista de parámetros de configuración y sus respectivos valores separados por espacios (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). El archivo setup.exe se ubica en la carpeta Servidor, que es parte del kit de distribución de Kaspersky Security Center.

Los nombres y valores posibles para los parámetros que se pueden utilizar al instalar el Servidor de administración en modo silencioso figuran en la tabla siguiente.

Parámetros de la instalación del Servidor de administración en modo no interactivo

Nombre del parámetro	Descripción del parámetro	Valores disponibles
EULA	Aceptación de las condiciones del Contrato de licencia.	• 1: He leído, y entiendo y acepto todas las condiciones del Contrato de licencia de usuario final. • Otro valor o sin valor: no acepto las condiciones del Contrato de licencia (no se realiza la instalación).
PRIVACYPOLICY	Aceptación de las condiciones de la Política de privacidad.	• 1: Entiendo y acepto que todos mis datos serán manejados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad. Confirmo que he leído y entendido completamente la Política de privacidad. • Otro valor o sin valor: No acepto las condiciones de la

		Política de privacidad (no se realiza la instalación).
INSTALLATIONMODETYPE	Tipo de instalación del Servidor de administración.	• Estándar: instalación estándar. • Personalizado: instalación personalizada.
INSTALLDIR	Ruta a la carpeta de instalación del Servidor de administración.	Valor de cadena.
ADDLOCAL	Lista de los componentes del Servidor de administración (separados por comas) que se deben instalar.	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Lista mínima de componentes suficientes para la instalación apropiada del Servidor de administración: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.`
NETRANGETYPE	Tamaño de la red (número de dispositivos en la red).	• NRT_1_100: de 1 a 100 dispositivos. • NRT_100_1000: De 101 a 1000 dispositivos. • NRT_GREATER_1000: más de 1000 dispositivos.
SRV_ACCOUNT_TYPE	Modo de especificación de una cuenta bajo la que el Servidor de administración se ejecutará como un servicio.	• SrvAccountDefault: la cuenta se crea automáticamente. • SrvAccountUser: la cuenta se define manualmente. En este caso, debe especificar valores para los parámetros SERVERACCOUNTNAME y SERVERACCOUNTPWD.
SERVERACCOUNTNAME	Modo de especificación de una cuenta con la que el Servidor de administración se ejecutará como servicio. Debe especificar un valor para el parámetro si SRV_ACCOUNT_TYPE=SrvAccountUser.	Valor de cadena.
SERVERACCOUNTPWD	Contraseña de la cuenta que se utilizará para iniciar el Servidor de administración como un servicio. Debe especificar un	Valor de cadena.

	valor para el parámetro si SRV_ACCOUNT_TYPE=SrvAccountUser.	
SERVERCER	Tamaño de la clave del certificado del Servidor de administración (bits).	• 1: tamaño de la clave del certificado del Servidor de administración es de 2.048 bits. • Sin valor: El tamaño de la clave del certificado del Servidor de administración es de 1.024 bits.
DBTYPE	Tipo de base de datos que se utilizará para almacenar la base de datos del Servidor de administración. Este parámetro es obligatorio.	• MySQL: se usará una base de datos MySQL o MariaDB; en este caso, debe especificar los valores para los parámetros MYSQLSERVERNAME, MYSQLSERVERPORT, MYSQLDBNAME, MYSQLACCOUNTNAME, y MYSQLACCOUNTPWD. • MSSQL: se utilizará una base de datos Microsoft SQL Server (SQL Express). En este caso, debe especificar valores para los parámetros MSSQLSERVERNAME, MSSQLDBNAME y MSSQLAUTHTYPE.
MYSQLSERVERNAME	Nombre completo del SQL Server. Debe especificar un valor para el parámetro si DBTYPE=MySQL.	Valor de cadena.
MYSQLSERVERPORT	Número del puerto para conectar al SQL Server. Debe especificar un valor para el parámetro si DBTYPE=MySQL.	Valor numérico.
MYSQLDBNAME	Nombre de la base de datos que se creará para almacenar datos del Servidor de administración. Debe especificar un valor para el parámetro si DBTYPE=MySQL.	Valor de cadena.
MYSQLACCOUNTNAME	Nombre de la cuenta para conexión a la base de datos. Debe especificar un valor para el parámetro si DBTYPE=MySQL.	Valor de cadena.
MYSQLACCOUNTPWD	Contraseña de la cuenta para conexión a la base de datos. Debe especificar un valor para el parámetro si DBTYPE=MySQL.	Valor de cadena.
MSSQLSERVERNAME	Nombre completo del SQL Server. Debe especificar un valor para el parámetro si DBTYPE=MSSQL.	Valor de cadena.
MSSQLDBNAME	Nombre de la base de datos. Debe	Valor de cadena.

	especificar un valor para el parámetro si DBTYPE=MSSQL.	
MSSQLAUTHTYPE	Tipo de autorización al conectar al SQL Server. Debe especificar un valor para el parámetro si DBTYPE=MSSQL	• Windows: modo de autenticación de Microsoft Windows. • SQLServer: modo de autenticación de SQL Server. En este caso, debe especificar valores para los parámetros MSSQLACCOUNTNAME y MSSQLACCOUNTPWD.
MSSQLACCOUNTNAME	Nombre de la cuenta para conexión con el SQL Server. Debe especificar un valor para el parámetro si MSSQLAUTHTYPE=SQLServer.	Valor de cadena.
MSSQLACCOUNTPWD	Contraseña de la cuenta para conexión con el SQL Server. Debe especificar un valor para el parámetro si MSSQLAUTHTYPE=SQLServer.	Valor de cadena.
CREATE_SHARE_TYPE	Método de especificación de la carpeta compartida.	• Create: Cree una nueva carpeta compartida. En este caso, debe especificar valores para los parámetros SHARELOCALPATH y SHAREFOLDERNAME. • ChooseExisting: seleccione una carpeta existente. En este caso, debe especificar un valor para el parámetro EXISTSHAREFOLDERNAME.
SHARELOCALPATH	Ruta a una carpeta local. Debe especificar un valor para el parámetro si CREATE_SHARE_TYPE=Create	Valor de cadena.
SHAREFOLDERNAME	Nombre de red de una carpeta compartida. Debe especificar un valor para el parámetro si CREATE_SHARE_TYPE=Create.	Valor de cadena.
EXISTSHAREFOLDERNAME	Ruta completa a una carpeta compartida existente. Debe especificar un valor para el parámetro si CREATE_SHARE_TYPE=ChooseExisting.	Valor de cadena.
SERVERPORT	Número de puerto para conectar con el Servidor de administración.	Valor numérico.
SERVERSSLPORT	Número del puerto para conexión cifrada al Servidor de administración usando el protocolo SSL.	Valor numérico.

SERVERADDRESS	Dirección de Servidor de administración.	Valor de cadena.
MOBILESERVERADDRESS	Dirección externa del Servidor de administración para la conexión de dispositivos móviles.	Valor de cadena.

Para obtener una descripción detallada de los parámetros de instalación del Servidor de administración, consulte la sección Instalación personalizada.

Instalación de la Consola de administración en la estación de trabajo del administrador

Puede instalar la Consola de administración en la estación de trabajo del administrador por separado y administrar el Servidor de administración en la red con esa consola.

Para instalar la Consola de administración en la estación de trabajo del administrador:

1. Ejecute el archivo ejecutable setup.exe.

   Se abre una ventana que le solicita que seleccione las aplicaciones Kaspersky que desea instalar.

2. En la ventana de selección de aplicaciones, haga clic en el enlace **Instalar solo la Consola de administración de Kaspersky Security Center 14** para iniciar el Asistente de instalación de la Consola de administración. Siga las instrucciones del Asistente.

3. Seleccionar la carpeta de destino. De forma predeterminada, la carpeta de destino será <Unidad de disco>:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center Console. Si la carpeta no existe, se crea automáticamente durante la instalación. Puede cambiar la carpeta de destino con el botón **Examinar**.

4. En la última página del Asistente de instalación, haga clic en el botón **Iniciar** para comenzar la instalación de la Consola de administración.

Cuando el Asistente termina, la Consola de administración se instala en la estación de trabajo del administrador.

Para instalar la Consola de administración en la estación de trabajo del administrador en modo no interactivo:

1. Lea el Contrato de licencia de usuario final. Utilice el siguiente comando solo si comprende y acepta las condiciones del Contrato de licencia de usuario final.

2. En la carpeta `Distrib\Console` del kit de distribución de Kaspersky Security Center, ejecute el archivo setup.exe utilizando el siguiente comando:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Si desea instalar todos los complementos de administración de la carpeta `Distrib\Console\Plugins` junto con la Consola de administración, ejecute el siguiente comando:

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Si desea especificar qué complementos de administración instalar desde la carpeta `Distrib\Console\Plugins` junto con la Consola de administración, especifique los complementos después de la clave "/p" y sepárelos con un punto y coma:

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   donde `P1`, `P2`, `P3` son nombres de complementos que corresponden a los nombres de las carpetas de complementos en la carpeta `Distrib\Console\Plugins`. Por ejemplo:

```
setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
```

La Consola de administración y los complementos de administración (si los hubiera) se instalarán en la estación de trabajo del administrador.

Después de instalar la Consola de administración, debe conectarse al Servidor de administración. Para ello, ejecute la Consola de administración y, en la ventana que se abre, especifique el nombre o la dirección IP del dispositivo en el que está instalado el Servidor de administración y la configuración de la cuenta de usuario a la que conectarse. Una vez que se establece la conexión al Servidor de administración, puede administrar el sistema de protección antivirus mediante la Consola de administración.

Puede quitar la Consola de administración con herramientas estándar de adición y eliminación de Microsoft Windows.

Cambios en el sistema después de la instalación de Kaspersky Security Center

Icono de la Consola de administración

Después de haber instalado la Consola de administración en su dispositivo, aparecerá el icono que se usa para iniciar la Consola de administración. Puede encontrar la Consola de administración en el menú **Iniciar** → **Programas** → **Kaspersky Security Center**.

Servicios del Servidor de administración y del Agente de red

El Servidor de administración y el Agente de red se instalan en el dispositivo como servicios con las propiedades que se enumeran a continuación. La tabla también contiene atributos u otros servicios que se aplican en el dispositivo después de la instalación del Servidor de administración.

Propiedades de los servicios de Kaspersky Security Center

Componente	Nombre de servicio	Nombre de servicio mostrado	Cuenta
Servidor de administración	kladminserver	Servidor de administración de Kaspersky Security Center	Cuenta no privilegiada dedicada o definida por el usuario en formato KL-AK-* creada durante la instalación
Agente de red	klnagent	Agente de red de Kaspersky Security Center	Sistema local
Servidor Web para acceder a Kaspersky Security Center 14 Web Console y administrar la intranet de la organización	klwebsrv	Servidor web de Kaspersky	Cuenta especializada no privilegiada de KlScSvc
Servidor proxy de activación	klactprx	Proxy de activación de Kaspersky	Cuenta especializada no privilegiada de KlScSvc
Servidor proxy de KSN.	ksnproxy	Servidor proxy de Kaspersky	Cuenta especializada no privilegiada de KlScSvc

		Security Network	

Servicios de Kaspersky Security Center 14 Web Console

Si instala Kaspersky Security Center 14 Web Console en el dispositivo, se desplegarán los siguientes servicios (consulte la tabla a continuación):

Servicios de Kaspersky Security Center 14 Web Console

Nombre de servicio mostrado	Cuenta
Kaspersky Security Center Service Console	Cuenta especializada no privilegiada de KlScSvc
Kaspersky Security Center Web Console	Servicio de red
Servicio del complemento de Kaspersky Security Center	Cuenta especializada no privilegiada de KlScSvc
Kaspersky Security Center Web Console Management Service	Sistema local
Cola de mensajes de Kaspersky Security Center Web Console	Cuenta especializada no privilegiada de KlScSvc

Versión del servidor del Agente de red

La versión de servidor del Agente de red se instalará en el dispositivo junto con el Servidor de administración. La versión de servidor del Agente de red es parte del Servidor de administración, se instala y se elimina junto con el Servidor de administración y puede interactuar con un solo Servidor de administración instalado localmente. No tiene que configurar la conexión del Agente de red al Servidor de administración: la configuración se implementa mediante funciones del programa, porque los componentes se instalan en el mismo dispositivo. La versión de servidor del Agente de red se instala con las mismas propiedades como Agente de red estándar y ejecuta las mismas funciones de administración de aplicaciones. Esta versión se administrará por la directiva del grupo de administración al cual pertenece el dispositivo cliente del Servidor de administración. Para la versión de servidor del Agente de red, se crean todas las tareas de la cobertura proporcionada para el Servidor de administración, a excepción de la tarea de cambio de servidor.

El Agente de red no se puede instalar por separado en un dispositivo que ya tiene instalado el Servidor de administración.

Puede consultar las propiedades de cada servicio del Servidor de administración y el Agente de red, además de supervisar su funcionamiento mediante las herramientas de administración estándar de Microsoft Windows: Administración de equipos\Servicios. La información sobre la actividad del servicio del Servidor de administración de Kaspersky se almacena en el registro del sistema Microsoft Windows en una rama de registro de eventos de Kaspersky en el dispositivo donde está instalado el Servidor de administración.

Recomendamos que evite iniciar y detener servicios manualmente y que no cambie las cuentas de servicio en la configuración del servicio. Si es necesario, puede modificar la cuenta de servicio del Servidor de administración utilizando la utilidad klsrvswch.

Cuentas de usuario y grupos de usuarios

El programa de instalación del Servidor de administración creó las siguientes cuentas de forma predeterminada:

- KL-AK-*: Cuenta de servicio del Servidor de administración.
- KlScSvc: Cuenta para otros servicios desde el conjunto del Servidor de administración.
- KlPxeUser: Cuenta para el despliegue de sistemas operativos.

Si ha seleccionado otras cuentas para el servicio del Servidor de administración y otros servicios mientras ejecuta el programa de instalación, se utilizarán las cuentas especificadas.

Los grupos de seguridad locales denominados KLAdmins y KLOperators con sus respectivos conjuntos de derechos también se crean automáticamente en el dispositivo que tiene el Servidor de administración instalado.

No se recomienda instalar el Servidor de administración en un controlador de dominio, pero si lo hace, debe iniciar el instalador con los derechos del administrador del dominio. En este caso, el instalador crea automáticamente los grupos de seguridad de dominio llamados KLAdmins y KLOperators. Si instala el Servidor de administración en un equipo que no sea el controlador de dominio, debe iniciar el instalador con los derechos del administrador local. En este caso, el instalador crea automáticamente los grupos de seguridad locales llamados KLAdmins y KLOperators.

Al configurar notificaciones del correo electrónico, es posible que tenga que crear una cuenta en el servidor de correo para la autenticación ESMTP.

Quitando la aplicación

Puede quitar Kaspersky Security Center con herramientas estándar de adición y eliminación de Microsoft Windows. La eliminación de la aplicación requiere iniciar un Asistente que elimina del dispositivo todos los componentes de la aplicación (incluidos los complementos). El Asistente hace que su navegador predeterminado abra una página web con una encuesta donde puede decirnos por qué decidió dejar de usar Kaspersky Security Center. Si no ha seleccionado la eliminación de la carpeta compartida (Share) durante el funcionamiento del Asistente, puede quitarla manualmente cuando finalicen todas las tareas relacionadas.

Después de eliminarse la aplicación, algunos de sus archivos podrían permanecer en la carpeta temporal del sistema.

El Asistente de eliminación de aplicaciones le sugerirá almacenar una copia de seguridad del Servidor de administración.

Al eliminar la aplicación de Microsoft Windows 7 y Microsoft Windows 2008, se puede producir el cierre prematuro del Asistente de eliminación. Esto se puede evitar desactivando el Control de cuenta de usuario (UAC) en el sistema operativo y reiniciando la eliminación de la aplicación.

Acerca del proceso de actualización de Kaspersky Security Center

Esta sección contiene información sobre cómo actualizar Kaspersky Security Center desde una versión anterior. Puede actualizar Kaspersky Security Center de diferentes maneras, dependiendo de si Kaspersky Security Center se instaló de forma local o en los nodos de clúster de conmutación por error de Kaspersky.

Durante la actualización, se prohíbe estrictamente que el Servidor de administración y otra aplicación hagan uso concurrente de la DBMS.

Al actualizar Kaspersky Security Center desde una versión anterior, se conservan todos los complementos instalados de las aplicaciones de Kaspersky compatibles. El complemento del Servidor de administración y el complemento del Agente de red se actualizan automáticamente (tanto para la Consola de administración como para Kaspersky Security Center 14 Web Console).

Actualización de Kaspersky Security Center desde una versión anterior

Puede instalar la versión 14 del Servidor de administración en un dispositivo que tenga una versión anterior del Servidor de administración instalada (a partir de la versión 10 Service Pack 1). Al actualizar a la versión 14, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Si se presentan problemas durante la instalación del Servidor de administración, puede restaurar la versión anterior del Servidor de administración usando la copia de seguridad de los datos del Servidor de administración creada antes de la actualización.

Si se ha instalado al menos un Servidor de administración de la nueva versión en la red, puede actualizar otros Servidores de administración en la red mediante la tarea de instalación remota que utiliza el paquete de instalación del Servidor de administración.

Si ha implementado el clúster de conmutación por error de Kaspersky, también puede actualizar Kaspersky Security Center en sus nodos.

Para actualizar una versión anterior del Servidor de administración a la versión 14, realice lo siguiente:

1. Ejecute el archivo de instalación ksc_14_<número de compilación>_full_<idioma>.exe para la versión 14 (puede descargar este archivo del sitio web de Kaspersky).

2. En la ventana que se abre, haga clic en el enlace **Instalar Kaspersky Security Center 14** para iniciar el Asistente de instalación del Servidor de administración. Siga las instrucciones del Asistente.

3. Lea el Contrato de licencia y la Política de privacidad. Si acepta todas las condiciones del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido por completo, y que acepto lo siguiente**:

   - **Los términos y condiciones de este EULA**

   - **La Política de privacidad que describe la gestión de los datos**

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas. El Asistente de instalación le solicita que cree una copia de seguridad de los datos del Servidor de administración para la versión anterior.

Kaspersky Security Center admite la recuperación de datos de una copia de seguridad creada con una versión anterior del Servidor de administración.

4. Si desea crear una copia de seguridad de los datos del Servidor de administración, especifíquelo en la ventana **Copia de seguridad del Servidor de administración** que se abre.

   La utilidad klbackup crea una copia de seguridad. Esta utilidad se incluye en el kit de distribución y se encuentra en la raíz de la carpeta de instalación de Kaspersky Security Center.

5. Instale la versión 14 del Servidor de administración, siguiendo las instrucciones del Asistente de instalación.

   Si aparece un mensaje de que el servicio de Kaspersky Security Center 14 Web Console está ocupado, haga clic en el botón **Ignorar** de la ventana del Asistente.

   Le recomendamos que evite cancelar la operación del Asistente de instalación. Si cancela la actualización durante el paso de instalación del Servidor de administración puede provocar el fallo de la versión actualizada de Kaspersky Security Center.

6. Para dispositivos que tienen instalada una versión posterior del Agente de red, cree y ejecute la tarea de instalación remota para la nueva versión del Agente de red.

   Al completarse la tarea de instalación remota, se actualiza la versión del Agente de red.

Actualizar Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky

Puede instalar la versión 14 del Servidor de administración en cada nodo del clúster de conmutación por error de Kaspersky que tenga instalada una versión anterior del Servidor de administración (a partir de la versión 13.2). Al actualizar a la versión 14, se conservan todos los datos y configuraciones de la versión anterior del Servidor de administración.

Si ya instaló de forma local Kaspersky Security Center en los dispositivos, también puede actualizar Kaspersky Security Center en estos dispositivos.

Para actualizar Kaspersky Security Center en los nodos del clúster de conmutación por error de Kaspersky:

1. Detenga el clúster.

2. Realice las siguientes acciones en el nodo activo del clúster:

   a. Ejecute el archivo ejecutable ksc_14.<número de compilación>_full_<idioma>.exe.

      Se abre una ventana y le solicita que seleccione las aplicaciones Kaspersky que desea actualizar. En la ventana de selección de aplicación, haga clic en el enlace **Instalación del Servidor de administración de Kaspersky Security Center 14** para iniciar el Asistente de instalación del Servidor de administración. Siga las instrucciones del Asistente.

   b. Lea el Contrato de licencia y la Política de privacidad. Si acepta todas las condiciones del Contrato de licencia y la Política de privacidad, seleccione las casillas siguientes en la sección **Confirmo que he leído y comprendido por completo, y que acepto lo siguiente**:

- **Los términos y condiciones de este EULA**
- **La Política de privacidad que describe la gestión de los datos**

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas casillas.

Si no acepta el Contrato de licencia o la Política de privacidad, haga clic en el botón **Cancelar** para cancelar la actualización.

c. En la ventana **Tipo de instalación en el clúster**, seleccione el nodo en el que está realizando la actualización.

A continuación, el instalador configura y finaliza la actualización del Servidor de administración. Durante la actualización, no puede cambiar los ajustes del Servidor de administración que haya configurado antes de la actualización.

3. En el nodo pasivo del clúster de conmutación por error de Kaspersky, realice las mismas acciones que en el nodo activo. Si elige la opción **Clúster (instalar en todos los nodos del clúster)** en la ventana **Tipo de instalación en el clúster**, no necesita ejecutar el instalador y realizar el paso actual.

4. Inicie el clúster.

Como resultado, usted ha instalado la última versión del Servidor de administración en los nodos del clúster de conmutación por error de Kaspersky.

Configuración inicial de Kaspersky Security Center

Esta sección describe los pasos que debe seguir después de la instalación de Kaspersky Security Center para realizar su configuración inicial.

Asistente de inicio rápido del Servidor de administración

Esta sección proporciona información sobre del Asistente de inicio rápido del Servidor de administración.

Acerca del Asistente de inicio rápido

Esta sección proporciona información sobre del Asistente de inicio rápido del Servidor de administración.

Asistente de inicio rápido del Servidor de administración le permite crear un mínimo de tareas y directivas necesarias, ajustar un mínimo de configuraciones, descargar e instalar complementos para aplicaciones administradas de Kaspersky y crear paquetes de instalación de aplicaciones administradas de Kaspersky. Cuando el Asistente se está ejecutando, puede realizar los siguientes cambios en la aplicación:

- Descargue e instale complementos para aplicaciones administradas. Una vez que el Asistente de inicio rápido ha finalizado, la lista de complementos de administración instalados se muestra en la sección **Avanzado** → **Detalles de los complementos de administración de aplicaciones instalados** de la ventana de propiedades del Servidor de administración.

- Crear paquetes de instalación para aplicaciones administradas de Kaspersky. Una vez finalizado el Asistente de inicio rápido, los paquetes de instalación del Agente de red para Windows y las aplicaciones administradas de Kaspersky se muestran en la lista **Servidor de administración** → **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

- Añadir archivos claves o ingresar códigos de activación que se pueden distribuir automáticamente a los dispositivos de grupos de administración. Una vez finalizado el Asistente de inicio rápido, se muestra información sobre las claves de licencia en el **Servidor de administración** → Lista de **Licencias de Kaspersky** y en la sección **Claves de licencia** de la ventana de propiedades del Servidor de administración.

- Configurar la interacción con Kaspersky Security Network (KSN).

- Configurar el envío de notificaciones por correo electrónico sobre eventos que tienen lugar durante el funcionamiento del Servidor de administración y las aplicaciones administradas (para que el envío de notificaciones sea correcto, el servicio de mensajería se debe ejecutar en el Servidor de administración y en todos los dispositivos destinatarios). Una vez que el Asistente de inicio rápido ha finalizado, la configuración de notificaciones por correo electrónico se muestra en la sección **Notificación** de la ventana de propiedades del Servidor de administración.

- Ajustar la configuración de la actualización y de la reparación de la vulnerabilidad de las aplicaciones instaladas en los dispositivos.

- Crear una directiva de protección para estaciones de trabajo y servidores, así como tareas del análisis antivirus, tareas de descarga de actualizaciones y tareas de copia de seguridad de datos, para el nivel superior de la jerarquía de dispositivos administrados. Una vez finalizado el Asistente de inicio rápido, las tareas creadas se muestran en la lista **Servidor de administración** → **Tareas**, las directivas correspondientes a los complementos para aplicaciones administradas se muestran en la lista **Servidor de administración** → **Directivas**.

El Asistente de inicio rápido crea directivas para las aplicaciones administradas, como Kaspersky Endpoint Security para Windows, a menos que dichas directivas ya se creen para el grupo de **dispositivos administrados**. El Asistente de inicio rápido crea tareas si no existen tareas con los mismos nombres para el grupo de **dispositivos administrados**.

En la Consola de administración, Kaspersky Security Center le solicita automáticamente que ejecute el Asistente de inicio rápido después de haberlo iniciado por primera vez. También puede iniciar el Asistente de inicio rápido manualmente en cualquier momento.

Iniciar el Asistente de inicio rápido del Servidor de administración

La aplicación automáticamente solicita que se ejecute el Asistente de inicio rápido tras la instalación del Servidor de administración la primera vez que se realiza la conexión con él. También puede iniciar el Asistente de inicio rápido manualmente en cualquier momento.

Para iniciar manualmente el Asistente de inicio rápido, haga lo siguiente:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.

2. En el menú contextual del nodo, seleccione **Todas las tareas** → **Asistente de inicio rápido del Servidor de administración**.

   El Asistente le solicita a realizar la configuración inicial del Servidor de administración. Siga las instrucciones del Asistente.

Si vuelve a iniciar el Asistente de inicio rápido, las tareas y directivas creadas en la ejecución anterior del Asistente no podrán crearse de nuevo.

Paso 1. Configuración de un servidor proxy

Especifique la configuración de acceso a Internet para el Servidor de administración. Debe configurar el acceso a Internet para usar Kaspersky Security Network y descargar actualizaciones de bases de datos antivirus para Kaspersky Security Center y las aplicaciones administradas de Kaspersky.

Seleccione la opción **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si esta casilla está seleccionada, los campos están disponibles para introducir la configuración. Especifique la configuración siguiente para la conexión con el servidor proxy:

- **Dirección**

  Dirección del servidor proxy utilizado para la conexión de Kaspersky Security Center con Internet.

- **Número de puerto**

  Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

- **No utilizar el servidor proxy para direcciones locales**

  No se utilizará un servidor proxy para conectarse a los dispositivos de la red local.

- **Autenticación del servidor proxy**

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Este campo de entrada está disponible si la casilla **Usar servidor proxy** está seleccionada.

- **Nombre de usuario**

  La cuenta de usuario en la que se establece la conexión al servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

- **Contraseña**

  La contraseña configurada por el usuario bajo cuya cuenta se establece la conexión del servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

  Para ver la contraseña introducida, mantenga pulsado el botón **Mostrar** todo el tiempo que sea necesario.

Paso 2. Selección del método de activación de la aplicación

Seleccione una de las siguientes opciones de activación de Kaspersky Security Center:

- **Inserte su código de activación**

El *código de activación* es una secuencia única de 20 caracteres alfanuméricos. Introduzca un código de activación para añadir una clave que active Kaspersky Security Center. Recibirá el código de activación a través de la dirección de correo electrónico que especificó después de adquirir Kaspersky Security Center.

Para activar la aplicación con un código de activación, necesita disponer de acceso a Internet a fin de establecer conexión con los servidores de activación de Kaspersky.

Si ha seleccionado esta opción de activación, puede activar la opción **Desplegar clave de licencia automáticamente en dispositivos administrados**.

Si esta opción está activada, la clave de licencia se desplegará automáticamente en los dispositivos administrados.

Si esta opción está desactivada, puede desplegar después la clave de licencia en los dispositivos administrados en el nodo **Licencias de Kaspersky** del árbol de la Consola de administración.

- Especifique un archivo clave

  Un *archivo clave* es un archivo con la extensión .key que Kaspersky le proporciona. Sirve para añadir archivo clave que active la aplicación.

  Recibirá su archivo clave a través de la dirección de correo electrónico que especificó después de adquirir Kaspersky Security Center.

  Para activar la aplicación con un archivo clave, no hace falta conectarse a los servidores de activación de Kaspersky.

  Si ha seleccionado esta opción de activación, puede activar la opción **Desplegar clave de licencia automáticamente en dispositivos administrados**.

  Si esta opción está activada, la clave de licencia se desplegará automáticamente en los dispositivos administrados.

  Si esta opción está desactivada, puede desplegar después la clave de licencia en los dispositivos administrados en el nodo **Licencias de Kaspersky** del árbol de la Consola de administración.

- Posponer la activación de aplicaciones

  La aplicación funcionará con una funcionalidad básica, sin Administración de dispositivos móviles y sin administración de vulnerabilidades y parches.

Si decide posponer la activación de la aplicación, puede añadir una clave de licencia más adelante en cualquier momento.

Paso 3. Selección de los alcances y plataformas de protección

Seleccione los alcances de protección y las plataformas que están en uso en su red. Cuando selecciona estas opciones, especifica los filtros para los complementos de administración de aplicaciones y los paquetes de distribución en los servidores de Kaspersky que puede descargar para instalar en los dispositivos cliente en su red. Seleccione las opciones:

- Áreas

Puede seleccionar los siguientes alcances de protección:

- **Estaciones de trabajo**. Seleccione esta opción si desea proteger las estaciones de trabajo en su red. La estación de trabajo está seleccionada de forma predeterminada.
- **Servidores de archivos y almacenamiento**. Seleccione esta opción si desea proteger los servidores de archivos en su red.
- **Dispositivos móviles**. Seleccione esta opción si desea proteger los dispositivos móviles pertenecientes a la empresa o a los empleados de la empresa. Si selecciona esta opción pero no ha proporcionado una licencia con la función de administración de dispositivos móviles, se muestra un mensaje que le informa sobre la necesidad de proporcionar una licencia con la función de administración de dispositivos móviles. Si no proporciona una licencia, no podrá usar la función de dispositivo móvil.
- **Virtualización**. Seleccione esta opción si desea proteger las máquinas virtuales en su red.
- **Kaspersky Anti-Spam**. Seleccione esta opción si desea proteger los servidores de correo electrónico de su organización del correo no deseado, el fraude y la entrega de malware.

- **Sistemas operativos**

  Puede seleccionar las siguientes plataformas:
  - Microsoft Windows
  - Linux
  - macOS
  - Android

Después de seleccionar los alcances y plataformas de protección, los complementos de administración y los paquetes de distribución para las aplicaciones de Kaspersky comenzarán a descargarse automáticamente.

Paso 4. Selección de complementos para las aplicaciones administradas

Seleccione complementos para instalar aplicaciones administradas. Se muestra una lista de complementos ubicados en los servidores de Kaspersky. La lista se filtra de acuerdo con las opciones seleccionadas en el paso anterior del Asistente. Por defecto, una lista completa incluye complementos de todos los idiomas. Para mostrar solo el complemento de un idioma específico, seleccione el idioma de la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**. La lista de complementos incluye las siguientes columnas:

- **Nombre de la aplicación**

  Se seleccionan los complementos que dependen de los componentes y las plataformas que haya seleccionado en el paso anterior.

- **Versión de la aplicación**

  La lista incluye complementos de todas las versiones colocadas en los servidores de Kaspersky. De forma predeterminada, se seleccionan los complementos de las últimas versiones.

- Idioma de localización

  De forma predeterminada, el idioma de localización de un complemento está definido por el idioma de Kaspersky Security Center que ha seleccionado en la instalación. Puede especificar otros idiomas en la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**.

Después de seleccionar los complementos, su instalación comienza automáticamente en una ventana separada. Para instalar algunos complementos, debe aceptar las condiciones del EULA. Lea el texto del EULA, seleccione la opción **Acepto los términos del Contrato de licencia** y haga clic en el botón **Instalar**. Si no acepta las condiciones del EULA, el complemento no se instala.

Una vez completada la instalación, cierre la ventana de instalación.

Paso 5. Descargar los paquetes de distribución y crear los paquetes de instalación

Kaspersky Endpoint Security para Windows incluye una herramienta de cifrado para la información almacenada en los dispositivos cliente. Para descargar un paquete de distribución de Kaspersky Endpoint Security para Windows válido para las necesidades de su organización, consulte la legislación del país donde se encuentran los dispositivos cliente de su organización. En la ventana **Tipo de cifrado**, seleccione uno de los siguientes tipos de cifrado:

- Cifrado fuerte. Este tipo de cifrado utiliza una longitud de clave de 256 bits.
- Cifrado ligero. Este tipo de cifrado utiliza una longitud de clave de 56 bits.

La ventana **Tipo de cifrado** se muestra solo si ha seleccionado **Estaciones de trabajo** como cobertura de protección y **Microsoft Windows** como plataforma.

Después de seleccionar un tipo de cifrado, se muestra una lista de paquetes de distribución de ambos tipos de cifrado. En la lista, se selecciona un paquete de distribución con el tipo de cifrado seleccionado. El idioma del paquete de distribución corresponde al idioma de Kaspersky Security Center. Si no existe un paquete de distribución de Kaspersky Endpoint Security para Windows para el idioma de Kaspersky Security Center, se selecciona el paquete de distribución en inglés.

En la lista, puede seleccionar los idiomas del paquete de distribución mediante la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**.

Las actualizaciones de aplicaciones administradas pueden requerir la instalación de una versión mínima específica de Kaspersky Security Center.

En la lista, puede seleccionar paquetes de distribución de cualquier tipo de cifrado, diferentes de los que ha seleccionado en la ventana **Tipo de cifrado**. Después de haber seleccionado un paquete de distribución para Kaspersky Endpoint Security para Windows, comienza la descarga de los paquetes de distribución, correspondientes a los componentes y plataformas. Puede controlar el progreso de la descarga en la columna **Estado de la descarga**. Una vez finalizado el Asistente de inicio rápido, los paquetes de instalación del Agente de red para Windows y las aplicaciones administradas de Kaspersky se muestran en la lista **Servidor de administración → Avanzado → Instalación remota → Paquetes de instalación**.

Para finalizar la descarga de algunos paquetes de distribución, debe aceptar el EULA. Cuando hace clic en el botón **Aceptar**, se muestra el texto del EULA. Para continuar con el siguiente paso del Asistente, debe aceptar las condiciones del EULA y las condiciones de la Política de privacidad de Kaspersky. Seleccione las opciones relacionadas con el EULA y la Política de privacidad de Kaspersky y haga clic en el botón **Aceptar todos**. Si no acepta las condiciones, se cancela la descarga del paquete.

Después de haber aceptado las condiciones del EULA y las condiciones de la Política de privacidad de Kaspersky, la descarga de los paquetes de distribución continúa. Cuando finaliza la descarga, se muestra el estado **Se ha creado el paquete de instalación**. Más tarde, usará paquetes de instalación para implementar aplicaciones de Kaspersky en dispositivos cliente.

Si prefiere no ejecutar el Asistente, puede crear paquetes de instalación manualmente en el nodo **Servidor de administración** → **Avanzado** → **Instalación remota** → **Paquetes de instalación** en el árbol de la Consola de administración.

Paso 6. Configuración del uso de Kaspersky Security Network

Lea la declaración de Kaspersky Security Network (KSN), que se muestra en la ventana. Especifique la configuración para transmitir la información sobre las operaciones de Kaspersky Security Center a la base de conocimientos de Kaspersky Security Network. Seleccione una de las siguientes opciones:

- **Acepto& usar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos cliente transferirán automáticamente su información de operación a Kaspersky Security Network. La participación en Kaspersky Security Network garantiza actualizaciones más rápidas de bases de datos que contienen información sobre virus y otras amenazas, y asegura una respuesta más rápida ante amenazas de seguridad emergentes.

- **No acepto usar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se desactivará el uso de Kaspersky Security Network.

Si ha descargado el complemento de Kaspersky Endpoint Security para Windows, se muestran las dos declaraciones de KSN: la declaración de KSN para Kaspersky Security Center y la declaración de KSN para Kaspersky Endpoint Security para Windows. Las declaraciones de KSN para otras aplicaciones Kaspersky administradas, cuyos complementos se descargaron, se muestran en ventanas separadas y usted debe aceptar (o no) cada una de las declaraciones por separado.

Paso 7. Configuración de notificaciones por correo electrónico

Configure el envío de notificaciones sobre eventos registrados durante el funcionamiento de aplicaciones Kaspersky en los dispositivos administrados. Estos parámetros servirán de configuración predeterminada para el Servidor de administración.

Para configurar la entrega de notificaciones sobre eventos que ocurren en aplicaciones de Kaspersky, use la configuración siguiente:

- **Destinatarios (correo electrónico)**

Las direcciones de correo electrónico de usuarios a quien la aplicación enviará notificaciones. Puede introducir una o más direcciones; si introduce más de una dirección, sepárelas con un punto y coma.

- **Servidores SMTP**

  La dirección o direcciones de los servidores de correo de su organización.

  Si introduce más de una dirección, sepárelas con un punto y coma. Puede usar los siguientes valores:

  - Dirección IPv4 o IPv6
  - Nombre de la red de Windows (nombre NetBIOS) del dispositivo
  - Nombre DNS del servidor SMTP

- **Puerto del servidor SMTP**

  Número del puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

- **Utilizar autenticación ESMTP**

  Activa la compatibilidad con autenticación de ESMTP. Cuando la casilla está seleccionada, en los campos **Nombre de usuario** y **Contraseña**, puede especificar la configuración de la autorización de ESMTP. De forma predeterminada, esta casilla está vacía y los parámetros de autenticación ESMTP no están disponibles.

- **Configuración de TLS para el servidor SMTP**

Especifique la configuración de TLS para el servidor SMTP:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de TLS para el servidor SMTP

Puede especificar la configuración de TLS para el servidor SMTP:

Puede desactivar el uso de TLS, usar TLS si el servidor SMTP admite este protocolo o puede forzar el uso de solo TLS. Si elige usar solo TLS, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, si elige usar solo TLS, puede especificar un certificado para la autenticación de clientes en el servidor SMTP.

- Busque un archivo de certificado para el servidor SMTP:

Puede recibir un archivo con la lista de certificados de las autoridades de certificación confiables y cargar el archivo en Kaspersky Security Center. Kaspersky Security Center verifica si el certificado del servidor del sistema SIEM también está firmado por autoridades de certificación confiables o no. Si el certificado del servidor del sistema SIEM no se recibe de las autoridades de certificación confiables, Kaspersky Security Center no podrá conectarse al servidor del sistema SIEM.

- Busque un archivo de certificado para el cliente:

Puede utilizar un certificado que haya recibido de cualquier fuente, por ejemplo, de cualquier autoridad de certificación confiable. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Ambos archivos no dependen el uno del otro y, por ende, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

- Contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y su clave privada. Cuando se cargue el archivo, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

Puede probar la nueva configuración de la notificación por correo electrónico haciendo clic en el botón **Enviar mensaje de prueba**.

Paso 8. Configuración de la administración de actualizaciones

Ajuste la configuración para administrar actualizaciones de aplicaciones instaladas en dispositivos cliente.

Solo puede configurar estos ajustes si ha proporcionado una clave de licencia con la opción de Administración de vulnerabilidades y parches.

En el grupo de configuración **Buscar actualizaciones e instalarlas**, puede seleccionar un modo de búsqueda e instalación de actualizaciones para Kaspersky Security Center:

- **Buscar las actualizaciones requeridas**

  La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea.

  Esta opción está seleccionada de forma predeterminada.

- **Buscar e instalar las actualizaciones requeridas**

  Las tareas *Buscar vulnerabilidades y actualizaciones requeridas* y *Instalar actualizaciones requeridas y reparar vulnerabilidades* se crean automáticamente, si no tiene ninguna.

En el grupo de configuración **Servicio de Windows Server Update** puede seleccionar el método de sincronización de actualizaciones:

- **Usar fuentes de actualización definidas en la directiva de dominio**

  Los dispositivos cliente descargarán las actualizaciones de Windows Update de acuerdo con la configuración de su directiva de dominio. La directiva del Agente de red se crea automáticamente si no tiene una.

- **Utilizar el Servidor de administración como servidor WSUS**

  Los dispositivos cliente descargarán las actualizaciones de Windows Update del Servidor de administración. La tarea *Realizar la sincronización de Windows Update* y la directiva del Agente de red se crean automáticamente, si no tiene ninguna.

Paso 9. Creación de una configuración de protección inicial

La ventana **Configurar la protección inicial** muestra una lista de directivas y tareas creadas automáticamente. Se crean las siguientes directivas y tareas:

- Directiva del Agente de red de Kaspersky Security Center
- Directivas para aplicaciones de Kaspersky administradas
- Tarea Mantenimiento del Servidor de administración
- Tarea Copia de seguridad de los datos del Servidor de administración
- Tarea Descargar actualizaciones en el repositorio del Servidor de administración
- Tarea Buscar vulnerabilidades y actualizaciones requeridas
- Tarea Instalar actualización

Espere a que se complete la creación de directivas y tareas antes de ir al paso siguiente del Asistente.

Si ha descargado e instalado el complemento para Kaspersky Endpoint Security para Windows 10 Service Pack 1 y versiones posteriores hasta 11.0.1, durante la creación de directivas y tareas, se abre una ventana para la configuración inicial de la zona de confianza de Kaspersky Endpoint Security para Windows. La aplicación le solicitará añadir proveedores verificados por Kaspersky en la zona de confianza con el fin de excluir sus aplicaciones de los análisis para impedir que se bloqueen por accidente. Puede crear exclusiones recomendadas ahora o crear una lista de exclusiones más adelante al seleccionar lo siguiente en el árbol de consola: **Directivas** → Menú de propiedades de Kaspersky Endpoint Security → **Protección avanzada contra amenazas** → **Zona de confianza** → **Configuración** → **Agregar**. La lista de exclusiones de análisis está disponible para modificarse en cualquier momento al usar la aplicación.

Las operaciones en la zona de confianza se realizan mediante las herramientas integradas en Kaspersky Endpoint Security para Windows. Si desea obtener instrucciones detalladas sobre cómo realizar cifrados, así como una descripción de las funciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows.

Para terminar la configuración inicial de la zona de confianza y volver al Asistente, haga clic en **Aceptar**.

Haga clic en **Siguiente**. Este botón se vuelve disponible después de que todas las directivas y tareas necesarias se hayan creado.

Paso 10. Conexión de dispositivos móviles

Si ha activado previamente la cobertura de protección **Dispositivos móviles** en la configuración del Asistente, especifique la configuración para la conexión de dispositivos móviles corporativos de la organización administrada. Si no activó la cobertura de protección **Dispositivos móviles**, este paso se omite.

En este paso del Asistente, hace lo siguiente:

- Configurar puertos para la conexión de dispositivos móviles.
- Configurar la autenticación del Servidor de administración.
- Crear o administrar certificados.
- Configurar la emisión, la actualización automática y el cifrado de certificados de tipo general.
- Crear una regla de movimiento para dispositivos móviles.

Para configurar los puertos para la conexión de dispositivos móviles:

1. Haga clic en el botón **Configurar** a la derecha del campo **Conexión de dispositivos móviles**.
2. En la lista desplegable, seleccione **Configurar puertos**.
   Se abre la ventana de propiedades del Servidor de administración que muestra la sección **Puertos adicionales**.
3. En la sección **Puertos adicionales**, puede especificar la configuración de conexión del dispositivo móvil:
   - **Puerto SSL para el servidor proxy de activación**

     Número de un puerto SSL para conectar Kaspersky Endpoint Security para Windows a los servidores de activación de Kaspersky.

     El número de puerto predeterminado es el 17000.

- **Abrir puerto para dispositivos móviles**

  Se abre un puerto para que los dispositivos móviles se conecten al Servidor de licencias. Puede definir el número de puerto y otra configuración en los campos a continuación.

  Esta opción está activada de forma predeterminada.

- **Puerto para la sincronización de dispositivos móviles**

  El número del puerto a través del cual los dispositivos móviles se conectarán al Servidor de administración e intercambiarán datos con él. El número de puerto predeterminado es el 13292.

  Puede asignar un puerto diferente si el puerto 13292 se está utilizando para otros fines.

- **Puerto para la activación de dispositivos móviles**

  Puerto para conectar Kaspersky Endpoint Security for Android a los servidores de activación de Kaspersky.

  El número de puerto predeterminado es el 17100.

- **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

  Los dispositivos con protección de UEFI pueden conectarse al Servidor de administración.

- **Puerto para estos dispositivos**

  Puede cambiar el número de puerto si la opción **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS** está activada. El número de puerto predeterminado es el 13294.

4. Haga clic **Aceptar** para guardar los cambios y vuelva al Asistente de inicio rápido.

Tendrá que configurar la autenticación del Servidor de administración por dispositivos móviles y autenticación de dispositivos móviles por el Servidor de administración. Si lo desea, puede configurar la autenticación más adelante, en forma aislada del Asistente de inicio rápido.

Para configurar la autenticación del Servidor de administración por dispositivos móviles:

1. Haga clic en el botón **Configurar** a la derecha del campo **Conexión de dispositivos móviles**.

2. En la lista desplegable, seleccione **Configurar autenticación**.

   Se abre la ventana de propiedades del Servidor de administración que muestra la sección **Certificados**.

3. Seleccione la opción de autenticación para dispositivos móviles en el grupo de configuraciones **Autenticación del Servidor de administración por dispositivos móviles** y seleccione la opción de autenticación para dispositivos con protección de UEFI en el grupo de configuraciones **Autenticación del Servidor de administración por dispositivos con protección de UEFI**.

   Cuando el Servidor de administración intercambia datos con dispositivos cliente, se autentica a través del uso de un certificado.

   De forma predeterminada, el Servidor de administración usa el certificado que se creó durante la instalación del Servidor de administración. Si lo desea, puede añadir un nuevo certificado.

Para añadir un nuevo certificado (opcional):

1. Seleccionar **Otro certificado**.

   Aparece el botón **Examinar**.

2. Haga clic en el botón **Examinar**.

3. En la ventana que se abre, especifique la configuración del certificado:

   - Tipo de certificado

     Puede seleccionar un tipo de certificado de la lista desplegable:

     - **Certificado X.509**. Si se selecciona esta opción, debe especificar la clave privada de un certificado y un certificado abierto:
       - **Clave privada (.prk, .pem)**. En este campo, haga clic en el botón **Examinar** para especificar la clave privada de un certificado en formato PKCS #8 (*.prk).
       - **Clave pública (.cer)**. En este campo, haga clic en el botón **Examinar** para especificar una clave pública en formato PEM (*.cer).
     - **Contenedor PKCS #12**. Si selecciona esta opción, puede especificar un archivo de certificado en formato P12 o PFX haciendo clic en el botón **Examinar** y completando el campo **Archivo de certificado**.

   - Hora de activación:

     - Inmediatamente

       El certificado actual se reemplazará inmediatamente con el nuevo después de que haga clic en **Aceptar**.

       Los dispositivos móviles anteriormente conectados no se podrán conectar al Servidor de administración.

     - Después de que este periodo venza, días

       Si selecciona esta opción, se generará un certificado de reserva. El certificado actual se reemplazará por el nuevo en el número especificado de días. La fecha de entrada en vigor del certificado de reserva se muestra en la sección **Certificados**.

       Se recomienda planificar la reemisión con anticipación. El certificado de reserva debe descargarse a los dispositivos móviles antes de que caduque el período especificado. Después de que el certificado actual se reemplace por el nuevo, los dispositivos móviles anteriormente conectados que no tengan el certificado de reserva no se podrán conectar al Servidor de administración.

4. Haga clic en el botón **Propiedades** para ver la configuración del certificado del Servidor de administración seleccionado.

Para volver a emitir un certificado emitido a través del Servidor de administración, haga lo siguiente:

1. Seleccionar **Certificado emitido a través del Servidor de administración**.

2. Haga clic en el botón **Reemitir**.

3. En la ventana que se abre, especifique la siguiente configuración:

   - Dirección de conexión:

     - **Utilizar dirección de conexión antigua**

       La dirección del Servidor de administración a la cual los dispositivos móviles se conectan permanece sin alterar.

       Esta opción está seleccionada de forma predeterminada.

     - **Cambiar dirección de conexión a**

       Si desea que dispositivos móviles se conecten a una dirección diferente, especifique la dirección relevante en este campo.

       Si la dirección de conexión de dispositivos móviles ha cambiado, debe emitirse un nuevo certificado. El certificado anterior se vuelve no válido en todos los dispositivos móviles conectados. Los dispositivos anteriormente conectados no podrán conectarse al Servidor de administración y, por tanto, se volverán no administrados.

   - Hora de activación:

     - **Inmediatamente**

       El certificado actual se reemplazará inmediatamente con el nuevo después de que haga clic en **Aceptar**.

       Los dispositivos móviles anteriormente conectados no se podrán conectar al Servidor de administración.

     - **Después de que este periodo venza, días**

       Si selecciona esta opción, se generará un certificado de reserva. El certificado actual se reemplazará por el nuevo en el número especificado de días. La fecha de entrada en vigor del certificado de reserva se muestra en la sección **Certificados**.

       Se recomienda planificar la reemisión con anticipación. El certificado de reserva debe descargarse a los dispositivos móviles antes de que caduque el período especificado. Después de que el certificado actual se reemplace por el nuevo, los dispositivos móviles anteriormente conectados que no tengan el certificado de reserva no se podrán conectar al Servidor de administración.

4. Haga clic **Aceptar** para guardar los cambios y vuelva a la ventana **Certificados**.

5. Haga clic **Aceptar** para guardar los cambios y vuelva al Asistente de inicio rápido.

Para configurar la emisión, la actualización automática y el cifrado de certificados de tipo general para la identificación de dispositivos móviles por Servidor de administración:

1. Haga clic en el botón **Configurar** a la derecha del campo **Autenticación de dispositivos móviles**.

   Se abre la ventana **Reglas de emisión de certificados**, que muestra la sección **Emisión de certificados móviles**.

2. Si es necesario, ajuste la configuración siguiente en la sección **Configuración de emisión**:

- **Vida útil del certificado, días**

  Duración del certificado en días. La vida útil predeterminada de un certificado es 365 días. Cuando este período expire, el dispositivo móvil no podrá conectarse al Servidor de administración.

- **Origen del certificado**

  Seleccione el origen de los certificados de tipo general para dispositivos móviles: los certificados son emitidos por el Servidor de administración o bien se especifican manualmente.

  Puede modificar las plantillas del certificado si la integración con la infraestructura de claves públicas (PKI) se ha configurado en la sección **Integración con la PKI**. En este caso, los campos de selección de plantilla siguientes están disponibles:

- **Plantilla predeterminada**

  Use un certificado emitido por un origen de externo (centro de certificación) bajo la plantilla predeterminada.

  Esta opción está seleccionada de forma predeterminada.

- **Otra plantilla**

  Seleccione una plantilla utilizada para emitir certificados. Puede especificar las plantillas de certificados en el dominio. El botón **Actualizar lista** actualiza la lista de plantillas de certificados.

3. Si es necesario, especifique la configuración siguiente para la emisión automática de certificados en la sección **Configuración de las actualizaciones automáticas**:

   - **Renovar el certificado cuando para que caduque falten (días)**

     El número de días restantes hasta que caduque el certificado actual durante el cual el Servidor de administración debe emitir un nuevo certificado. Por ejemplo, si el valor del campo es 4, el Servidor de administración emitirá un nuevo certificado cuatro días antes de que el certificado actual caduque. El valor predeterminado es 7.

   - **Reemitir el certificado automáticamente siempre que sea posible**

     Seleccione esta opción para volver a emitir un certificado automáticamente por el número de días especificado en el campo **Renovar el certificado cuando para que caduque falten (días)**. Si un certificado se definió manualmente, no se puede renovar automáticamente y la opción activada no funcionará.

     Esta opción está desactivada de forma predeterminada.

   El centro de certificación reemite los certificados automáticamente.

4. Si es necesario, en la sección de configuración **Protección de contraseñas**, especifique la configuración para descifrar certificados durante la instalación.

   Seleccione la opción **Solicitar contraseña durante la instalación del certificado** para solicitar al usuario que escriba la contraseña cuando se instale el certificado en un dispositivo móvil. La contraseña solo se utiliza una vez, que es durante la instalación del certificado en el dispositivo móvil.

La contraseña será automáticamente generada por el Servidor de administración y se enviará a la dirección de correo electrónico que especificó. Puede especificar la dirección de correo electrónico del usuario o su propia dirección de correo electrónico si desea usar otro método para reenviar la contraseña al usuario.

Puede usar el control deslizante para especificar el número de caracteres en la contraseña de descifrado del certificado.

La opción de solicitud de la contraseña se requiere, por ejemplo, para proteger un certificado compartido en un paquete de instalación de Kaspersky Endpoint Security for Android independiente. La protección con contraseña impedirá a un intruso obtener el acceso al certificado compartido mediante el robo del paquete de instalación independiente desde el Servidor web de Kaspersky Security Center.

Si esta opción está desactivada, el certificado automáticamente se descifrará durante la instalación y no se solicitará al usuario que escriba una contraseña. Esta opción está desactivada de forma predeterminada.

5. Haga clic **Aceptar** para guardar los cambios y vuelva a la ventana del Asistente de inicio rápido.

   Haga clic en el botón **Cancelar** para volver al Asistente de inicio rápido sin guardar ninguno de los cambios.

Para activar la función para mover dispositivos móviles a un grupo de administración que elija,

En el campo **Mover automáticamente dispositivos móviles**, seleccione la opción **Crear una regla de movimiento para dispositivos móviles**.

Si la opción **Crear una regla de movimiento para dispositivos móviles** está seleccionada, la aplicación automáticamente crea una regla de movimiento que mueve los dispositivos con Android e iOS al grupo **Dispositivos administrados**:

- Con sistemas operativos Android en los cuales se haya instalado Kaspersky Endpoint Security for Android y un certificado móvil
- Con sistemas operativos iOS en los cuales se haya instalado el perfil de MDM para iOS con un certificado compartido

Si tal regla ya existe, la aplicación no la crea de nuevo.

Esta opción está desactivada de forma predeterminada.

Kaspersky ya no admite Kaspersky Safe Browser.

Paso 11. Descargar actualizaciones

Las actualizaciones de las bases de datos antivirus para Kaspersky Security Center y las aplicaciones administradas de Kaspersky se descargan automáticamente. Las actualizaciones se descargan de los servidores de Kaspersky.

Paso 12. Detección de dispositivos

La ventana **Sondeo de la red** muestra la información sobre el estado del sondeo de la red realizada por el Servidor de administración.

Puede ver los dispositivos de la red detectados por el Servidor de administración y recibir ayuda sobre el funcionamiento con la ventana **Detección de dispositivos** haciendo clic en los vínculos de la parte inferior de la ventana.

Paso 13. Cierre el Asistente de inicio rápido

En la ventana de finalización del Asistente de inicio rápido, seleccione la opción **Ejecutar el Asistente de instalación remota** si desea iniciar la instalación automática de aplicaciones antivirus y/o el Agente de red en dispositivos en su red.

Para completar el Asistente, haga clic en el botón **Finalizar**.

Configuración de la conexión de la Consola de administración al Servidor de administración

En versiones anteriores de Kaspersky Security Center, la Consola de administración se conectaba al Servidor de administración mediante el puerto SSL TCP 13291, así como el puerto SSL TCP 13000. Desde Kaspersky Security Center 10 Service Pack 2, los puertos SSL usados por la aplicación se separan de forma estricta y cualquier uso indebido de puertos es imposible:

- El puerto SSL TCP 13291 solo puede ser utilizado por la Consola de administración y los objetos de automatización klakaut.
- El puerto SSL TCP 13000 solo puede ser utilizado por el Agente de red, un Servidor de administración secundario y el Servidor de administración principal en DMZ.

El puerto TCP 14000 solo puede ser utilizado para conectar la Consola de administración, los puntos de distribución, los Servidores de administración secundarios y los objetos de automatización klakaut, así como para recibir datos desde dispositivos cliente.

En algunos casos, puede que la Consola de administración deba conectarse mediante el puerto SSL 13000:

- Si es probable que un puerto SSL único se utilice tanto para la Consola de administración como para otras actividades (recepción de datos desde dispositivos cliente, conexión de puntos de distribución o conexión de Servidores de administración secundarios).
- Si un objeto de automatización klakaut no se conecta al Servidor de administración directamente sino mediante un punto de distribución en DMZ.

Para permitir la conexión de la Consola de administración mediante el puerto 13000:

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).
2. Vaya al siguiente subárbol:
   - Para un sistema de 64 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - Para un sistema de 32 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Para la clave LP_ConsoleMustUsePort13291 (DWORD), establezca 00000000 como valor.

   El valor predeterminado especificado para esta clave es 1.

4. Reinicie el servicio del Servidor de administración.

Podrá conectar la Consola de administración al Servidor de administración mediante el puerto 13000.

Conexión de dispositivos fuera de la oficina

Esta sección describe cómo conectar los dispositivos fuera de la oficina (es decir, los dispositivos administrados que se encuentran fuera de la red principal) al Servidor de administración.

Escenario: conexión de dispositivos fuera de la oficina a través de una puerta de enlace de conexión

Este escenario describe cómo conectar dispositivos administrados que se encuentran fuera de la red principal al Servidor de administración.

Requisitos previos

El escenario tiene los siguientes requisitos previos:

- Una zona desmilitarizada (DMZ) está organizada en la red de su organización.
- El Servidor de administración de Kaspersky Security Center está desplegado en la red corporativa.

Etapas

Este escenario avanza en etapas:

1. **Seleccionar un dispositivo cliente en la DMZ**

   Este dispositivo se utilizará como puerta de enlace de conexión. El dispositivo que seleccione debe cumplir los requisitos de las puertas de enlace de conexión.

2. **Instalación de Agente de red con la función de puerta de enlace de conexión**

   Le recomendamos que utilice una instalación local para instalar el Agente de red en el dispositivo seleccionado.

   De forma predeterminada, el archivo de instalación se encuentra en: \\<server name>\KLSHARE\PkgInst\NetAgent_<version number>

   En la ventana **Puerta de enlace de conexión** del Asistente de instalación del Agente de red, seleccione **Usar el Agente de red como puerta de enlace de conexión en DMZ**. Este modo activa simultáneamente la función de puerta de enlace de conexión e indica al Agente de red que espere las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración.

   También puede instalar el Agente de red en un dispositivo Linux y configurar el Agente de red para que funcione como puerta de enlace de conexión, pero preste atención a la lista de limitaciones del Agente de red que se ejecuta en dispositivos Linux.

3. **Permitir conexiones en firewalls en la puerta de enlace de conexión**

Para asegurarse de que el Servidor de administración pueda realmente conectarse a la puerta de enlace de conexión en la DMZ, permita conexiones al puerto TCP 13000 en todos los firewalls entre el Servidor de administración y la puerta de enlace de conexión.

Si la puerta de enlace de conexión no tiene una dirección IP real en Internet, sino que se encuentra detrás de Network Address Translation (NAT), configure una regla para reenviar las conexiones a través de NAT.

4. **Creación de un grupo de administración para dispositivos externos**

   Cree un nuevo grupo en el grupo de **Dispositivos administrados**. Este grupo nuevo contendrá dispositivos administrados externos.

5. **Conexión de la puerta de enlace de conexión a un Servidor de administración.**

   La puerta de enlace de conexión que ha configurado queda a la espera de que el Servidor de administración se conecte. Sin embargo, el Servidor de administración no enumera el dispositivo con la puerta de enlace de conexión entre los dispositivos administrados. Esto se debe a que la puerta de enlace de conexión no ha intentado establecer una conexión con el Servidor de administración. Por lo tanto, necesita un procedimiento especial para asegurarse de que el Servidor de administración inicie una conexión con la puerta de enlace de conexión.

   Haga lo siguiente:

   1. Añada la puerta de enlace de conexión como punto de distribución.
   2. Mueva la puerta de enlace de conexión del grupo **Dispositivos no asignados** al grupo que ha creado para dispositivos externos.

   La puerta de enlace de conexión queda conectada y configurada.

6. **Conexión de equipos de escritorio externos al Servidor de administración:**

   Por lo general, los equipos de escritorio externos no se mueven dentro del perímetro. Por lo tanto, debe configurarlos para que se conecten al Servidor de administración a través de la puerta de enlace al instalar el Agente de red.

7. **Configuración de actualizaciones para equipos de escritorio externos**

   Si las actualizaciones de las aplicaciones de seguridad están configuradas para descargarse del Servidor de administración, los equipos externos descargan las actualizaciones a través de la puerta de enlace de conexión. Esto tiene dos desventajas:

   - Se trata de tráfico innecesario, que ocupa el ancho de banda del canal de comunicación de Internet de la empresa.
   - Esta no es necesariamente la forma más rápida de obtener actualizaciones. Es muy probable que sea más barato y rápido que los equipos externos reciban actualizaciones de los servidores de actualización de Kaspersky.

   Haga lo siguiente:

   1. Mueva todos los equipos externos al grupo de administración independiente que ha creado.
   2. Excluya al grupo con dispositivos externos de la tarea de actualización.
   3. Cree una tarea de actualización aparte para el grupo con dispositivos externos.

8. **Conexión de equipos portátiles que viajan al Servidor de administración**

   Los equipos portátiles que viajan a veces están dentro de la red, y otras fuera. Para una gestión eficaz, necesita que se conecten al Servidor de administración de forma diferente según su ubicación. Para un uso eficiente del tráfico, también necesitan recibir actualizaciones de diferentes fuentes según su ubicación.

Necesita configurar reglas para usuarios fuera de la oficina: perfiles de conexión y descripciones de ubicación de red. Cada regla define la instancia del Servidor de administración al que deben conectarse los equipos portátiles que viajan, según su ubicación y según el Servidor de administración desde el cual deben recibir actualizaciones.

Acerca de la conexión de dispositivos fuera de la oficina

Algunos de los dispositivos administrados que siempre están fuera de la red principal (por ejemplo, los equipos en las sucursales regionales de una empresa; quioscos, cajeros automáticos y terminales instalados en varios puntos de venta; equipos en las oficinas en casa de los empleados) no se pueden conectar directamente al Servidor de administración. Algunos dispositivos viajan fuera del perímetro de vez en cuando (por ejemplo, ordenadores portátiles de usuarios que visitan sucursales regionales o la oficina de un cliente).

Con todo, es necesario monitorizar y gestionar la protección de los dispositivos fuera de la oficina: recibir información real sobre su estado de protección y mantener actualizadas las aplicaciones de seguridad. Esto es necesario porque, por ejemplo, si un dispositivo de este tipo se ve comprometido mientras está lejos de la red principal, podría convertirse en una plataforma para propagar amenazas tan pronto como se conecte a la red principal. Para conectar dispositivos fuera de la oficina al Servidor de administración, puede utilizar dos métodos:

- Puerta de enlace de conexión en la zona desmilitarizada (DMZ)

  Consulte el esquema de tráfico de datos: Servidor de administración en LAN, dispositivos administrados en Internet, puerta de enlace de conexión en uso

- Servidor de administración en DMZ

  Consulte el esquema de tráfico de datos: Servidor de administración en DMZ, dispositivos administrados en Internet

Una puerta de enlace de conexión en la DMZ

Un método recomendado para conectar dispositivos fuera de la oficina al Servidor de administración es organizar una DMZ en la red de la organización e instalar una puerta de enlace de conexión en la DMZ. Los dispositivos externos se conectarán a la puerta de enlace de conexión y el Servidor de administración dentro de la red iniciará la conexión con los dispositivos a través de la puerta de enlace de conexión.

En comparación con el otro método, este es más seguro:

- No es necesario abrir el acceso al Servidor de administración desde fuera de la red.
- Una puerta de enlace de conexión comprometida no representa un alto riesgo para la seguridad de los dispositivos de red. Una puerta de enlace de conexión en realidad no administra nada por sí misma y no establece ninguna conexión.

Además, una puerta de enlace de conexión no requiere muchos recursos de hardware.

Sin embargo, este método tiene un proceso de configuración más complicado:

- Para hacer que un dispositivo actúe como puerta de enlace de conexión en la DMZ, debe instalar el Agente de red y conectarlo al Servidor de administración de una manera específica.
- No podrá utilizar la misma dirección para conectarse al Servidor de administración en todas las situaciones. Desde fuera del perímetro, no solo deberá utilizar una dirección diferente (dirección de puerta de enlace de conexión), sino también un modo de conexión diferente: a través de una puerta de enlace de conexión.

- También debe definir diferentes configuraciones de conexión para ordenadores portátiles en diferentes ubicaciones.

Servidor de administración en la DMZ

Otro método es instalar un único Servidor de administración en la DMZ.

Esta configuración es menos segura que el otro método. Para administrar ordenadores portátiles externos en este caso, el Servidor de administración debe aceptar conexiones desde cualquier dirección en Internet. Seguirá administrando todos los dispositivos en la red interna, pero desde la DMZ. Por lo tanto, un servidor comprometido podría causar una enorme cantidad de daños, a pesar de la baja probabilidad de que ocurra tal evento.

El riesgo se reduce en gran medida si el Servidor de administración en la DMZ no administra dispositivos en la red interna. Una configuración de este tipo puede utilizarla, por ejemplo, un proveedor de servicios para administrar los dispositivos de los clientes.

Es posible que desee utilizar este método en los siguientes casos:

- Si está familiarizado con la instalación y configuración del Servidor de administración y no desea realizar otro procedimiento para instalar y configurar una puerta de enlace de conexión.
- Si necesita gestionar más dispositivos. La capacidad máxima del Servidor de administración es de 100.000 dispositivos, mientras que una puerta de enlace de conexión puede admitir hasta 10.000 dispositivos.

Esta solución también tiene posibles dificultades:

- El Servidor de administración requiere más recursos de hardware y una base de datos más.
- La información sobre los dispositivos se almacenará en dos bases de datos no relacionadas (para el Servidor de administración dentro de la red y otra en la DMZ), lo que complica el la monitorización.
- Para administrar todos los dispositivos, el Servidor de administración debe ser parte de una jerarquía, lo que complica no solo la monitorización, sino también la administración. Una instancia del Servidor de administración secundario impone limitaciones a las posibles estructuras de los grupos de administración. Debe decidir cómo y qué tareas y directivas distribuir a una instancia del Servidor de administración secundario.
- Configurar dispositivos externos para usar el Servidor de administración en la DMZ desde afuera y usar el Servidor de administración principal desde adentro no es más simple que configurarlos para usar una conexión condicional a través de una puerta de enlace.
- Altos riesgos de seguridad. Una instancia del Servidor de administración comprometida hace más fácil comprometer ordenadores portátiles administrados. Si esto sucede, los piratas informáticos solo necesitan esperar a que uno de los ordenadores portátiles regrese a la red corporativa para poder continuar con su ataque contra la red de área local.

Conexión de equipos de escritorio externos al Servidor de administración:

Los equipos de escritorio que siempre están fuera de la red principal (por ejemplo, los equipos en las sucursales regionales de la empresa; quioscos, cajeros automáticos y terminales instalados en varios puntos de venta; equipos en las oficinas en casa de los empleados) no se pueden conectar directamente al Servidor de administración. Deben conectarse al Servidor de administración a través de una puerta de enlace de conexión que esté instalada en la zona desmilitarizada (DMZ). Esta configuración se realiza al instalar el Agente de red en esos equipos.

Para conectar equipos de escritorio externos al Servidor de administración:

1. Cree un paquete nuevo de instalación personalizada para el Agente de red.
2. Abra las propiedades del paquete de instalación creado y vaya a la sección **Avanzado**; luego, elija la opción **Conectar con el Servidor de administración usando una puerta de enlace de conexión**.

   El ajuste **Conectar con el Servidor de administración usando una puerta de enlace de conexión** es incompatible con el ajuste **Usar el Agente de red como puerta de enlace de conexión en DMZ**. No puede habilitar estas dos configuraciones al mismo tiempo.

3. En **Dirección de la puerta de enlace de conexión**, especifique la dirección pública de la puerta de enlace de conexión.

   Si la puerta de enlace de conexión se encuentra detrás de un sistema de traducción de direcciones de red (NAT) y no tiene su propia dirección pública, configure una regla de puerta de enlace NAT para reenviar conexiones desde la dirección pública a la dirección interna de la puerta de enlace de conexión.

4. Cree un paquete de instalación independiente basado en el paquete de instalación creado.
5. Entregue el paquete de instalación independiente a los equipos de destino de forma electrónica o mediante una unidad extraíble.
6. Instale Agente de red desde el paquete independiente.

Los equipos de escritorio externos quedan conectados al Servidor de administración.

Acerca de los perfiles de conexión para usuarios fuera de la oficina

Puede que los usuarios "fuera de la oficina" de equipos portátiles (en adelante, también denominados "dispositivos") deban cambiar el método de conexión a un Servidor de administración o cambiar entre Servidores de administración según la ubicación actual del dispositivo en la red empresarial.

Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

Uso de diferentes direcciones de un único Servidor de administración

El siguiente procedimiento se aplica únicamente a Kaspersky Security Center 10 Service Pack 1 y versiones posteriores.

Los dispositivos con el Agente de red instalado pueden conectarse al Servidor de administración ya sea mediante la intranet de la organización o por Internet. Esta situación puede requerir que el Agente de red utilice direcciones diferentes para la conexión con el Servidor de administración: la dirección del Servidor de administración externa para la conexión a Internet y la dirección del Servidor de administración interna para la conexión a la intranet.

Para esto, debe añadir un perfil (para la conexión con el Servidor de administración de Internet) a la directiva del Agente de red. Añada el perfil en las propiedades de la directiva (sección **Conectividad**, subsección **Perfiles de conexión**). En la ventana de creación de perfil, debe desactivar la opción **Usar solo para recibir actualizaciones** y seleccionar la opción **Sincronizar la configuración de la conexión con la configuración del Servidor de administración especificada para este perfil**. Si usa una puerta de enlace de conexión para acceder al Servidor de administración (por ejemplo, en una configuración de Kaspersky Security Center como la que se describe en Acceso a Internet: el Agente de red como puerta de enlace en DMZ), debe especificar la dirección de la puerta de enlace de conexión en el campo correspondiente del perfil de conexión.

Cambio entre Servidores de administración según la red actual

El siguiente procedimiento se aplica únicamente a Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 y versiones posteriores.

Si la organización tiene varias oficinas con Servidores de administración diferentes y algunos de los dispositivos con el Agente de red instalado se mueven entre ellas, necesita el Agente de red para la conexión con el Servidor de administración de la red local en la oficina donde se ubica el dispositivo actualmente.

En este caso, debe crear un perfil para la conexión con el Servidor de administración en las propiedades de la directiva del Agente de red para cada una de las oficinas, excepto la oficina principal donde se ubica el Servidor de administración principal. Debe especificar las direcciones de los Servidores de administración en los perfiles de conexión y activar o desactivar la opción **Usar solo para recibir actualizaciones**:

- Seleccione la opción si necesita que el Agente de red se sincronice con el Servidor de administración principal, mientras el Servidor local se usa solo para descargar actualizaciones.
- Desactive esta opción si es necesario que el Agente de red sea completamente administrado por el Servidor de administración local.

Después de esto, debe configurar las condiciones de conmutación a los perfiles recientemente creados: al menos, una condición para cada una de las oficinas, excepto la oficina principal. El objetivo de cada condición consiste en la detección de elementos que sean específicos del entorno de red de una oficina. Si una condición es verdadera, se activa el perfil correspondiente. Si ninguna de las condiciones es verdadera, el Agente de red cambia al Servidor de administración principal.

Creación de un perfil de conexión para usuarios fuera de la oficina

El perfil de conexión del Servidor de Administración sólo está disponible en dispositivos con Windows y macOS.

Para crear un perfil que permita a los usuarios fuera de la oficina conectar el Agente de red al Servidor de administración:

1. En el árbol de consola, seleccione el grupo de administración que contiene los dispositivos cliente para los que necesita crear un perfil de conexión del Agente de red al Servidor de administración.
2. Realice una de las siguientes acciones:
   - Si desea crear un perfil de conexión para todos los dispositivos del grupo, seleccione una directiva del Agente de red en el espacio de trabajo del grupo, en la ficha **Directivas**. Abra la ventana de propiedades de la directiva seleccionada.

- Si necesita crear un perfil de conexión para un dispositivo en un grupo, seleccione este dispositivo en el espacio de trabajo del grupo, en la ficha **Dispositivos**, y realice las siguientes acciones:

  a. Abra la ventana de propiedades del dispositivo seleccionado.

  b. En la sección **Aplicaciones** de la ventana de propiedades del dispositivo, seleccione el Agente de red.

  c. Abra la ventana de propiedades del Agente de red.

3. En la ventana de propiedades, en la sección **Conectividad** seleccione la subsección **Perfiles de conexión**.

4. En el grupo de configuración **Perfiles de conexión al Servidor de administración**, haga clic en el botón **Agregar**.

   De forma predeterminada, la lista de perfiles de conexión contiene los perfiles <Modo sin conexión> y <Servidor de administración principal>. No se puede modificar ni eliminar el perfiles.

   El perfil <Modo sin conexión> no especifica ningún Servidor para la conexión. Por lo tanto, el Agente de red, cuando se cambia a ese perfil, no intenta conectarse a ningún Servidor de administración mientras las aplicaciones instaladas en dispositivos cliente se ejecutan bajo directivas fuera de la oficina. El perfil <Modo sin conexión> puede utilizarse si los dispositivos están desconectados de la red.

   El perfil <Servidor de administración principal> especifica la conexión para el Servidor de administración que se seleccionó durante la instalación del Agente de red. El perfil <Servidor de administración principal> se aplica cuando un dispositivo se conecta de nuevo al Servidor de administración maestro después de que se ejecutara en una red externa durante algún tiempo.

5. En la ventana **Perfil nuevo** que se abre, configure el perfil de conexión:

   - Nombre del perfil

     En el campo de entrada se puede ver o cambiar el nombre del perfil de conexión.

   - Servidor de administración

     La Dirección del Servidor de administración al cual el dispositivo cliente debe conectarse durante la activación del perfil.

   - Puerto

     Número de puerto que se utiliza en la conexión.

   - Puerto SSL

     Número de puerto para la conexión mediante el protocolo SSL.

   - Utilizar SSL

     Si esta opción está activada, la conexión se establece a través de un puerto seguro, utilizando el protocolo SSL.

     Esta opción está activada de forma predeterminada. Le recomendamos que no desactive esta opción para que su conexión siga siendo segura.

- Haga clic en el enlace **Configurar la conexión mediante el servidor proxy** para configurar la conexión a través de un servidor proxy. Seleccione la opción **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si esta opción está seleccionada, los campos están disponibles para introducir la configuración. Especifique la configuración siguiente para la conexión con el servidor proxy:

  - Dirección del servidor proxy

    Dirección del servidor proxy utilizado para la conexión de Kaspersky Security Center con Internet.

  - Número de puerto

    Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

  - Autenticación del servidor proxy

    Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

    Este campo de entrada está disponible si la casilla **Usar servidor proxy** está seleccionada.

  - Nombre de usuario (este campo está disponible si la opción **Autenticación del servidor proxy** está seleccionada)

    La cuenta de usuario en la que se establece la conexión al servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

  - Contraseña (este campo está disponible si la opción **Autenticación del servidor proxy** está seleccionada)

    La contraseña configurada por el usuario bajo cuya cuenta se establece la conexión del servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

    Para ver la contraseña introducida, mantenga pulsado el botón **Mostrar** todo el tiempo que sea necesario.

- Configuración de la puerta de enlace de conexión

  Dirección de la puerta de enlace a través de la que se conectan los dispositivos cliente al Servidor de administración.

- Activar modo Fuera de la oficina

  Si se selecciona esta opción y en el caso de que la conexión se realice con este perfil, las aplicaciones instaladas en el dispositivo cliente utilizan los perfiles de directivas para dispositivos en modo fuera de la oficina, además de directivas fuera de la oficina. Si no se ha definido una directiva fuera de la oficina en la aplicación, se utilizará la directiva activa.

  Si esta opción está desactivada, las aplicaciones utilizarán las directivas activas.

  Esta opción está desactivada de forma predeterminada.

- Usar solo para recibir actualizaciones

Si esta opción está activada, el perfil lo utilizarán las aplicaciones instaladas en el dispositivo cliente solo para descargar actualizaciones. Para otras operaciones, la conexión al Servidor de administración será establecida con los parámetros de conexión iniciales definidos durante la instalación del Agente de red.

Esta opción está activada de forma predeterminada.

- Sincronizar la configuración de la conexión con la configuración del Servidor de administración especificada para este perfil

  Si esta opción está activada, el Agente de red se conecta al Servidor de administración usando la configuración especificada en las propiedades del perfil.

  Si esta opción está desactivada, el Agente de red se conectará al Servidor de administración usando la configuración original especificada durante la instalación.

  Esta opción está disponible si la opción **Usar para recibir actualizaciones solamente** está desactivada.

  Esta opción está desactivada de forma predeterminada.

6. Seleccione la opción **Activar modo Fuera de la oficina cuando el Servidor de administración no está disponible** para permitir que las aplicaciones instaladas en un dispositivo cliente usen perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas fuera de la oficina, en cualquier intento de conexión si el Servidor de administración no está disponible. Si no se ha definido una directiva fuera de la oficina en la aplicación, se utilizará la directiva activa.

Se crea un perfil para la conexión del Agente de red al Servidor de administración para usuarios fuera de la oficina. Cuando el Agente de red se conecta al Servidor de administración con este perfil, las aplicaciones instaladas en un dispositivo cliente utilizarán las directivas para estos dispositivos en modo fuera de la oficina, o bajo directivas fuera de la oficina.

Acerca del cambio del Agente de red a otro Servidor de administración

Kaspersky Security Center ofrece la opción de cambiar el Agente de red de un dispositivo cliente a otros Servidores de administración si cambian los siguientes parámetros de la red:

- **Dirección predeterminada de la puerta de enlace de conexión**: si cambia la dirección de la puerta de enlace principal de la red.
- **Dirección del servidor DHCP**: si cambia la dirección IP del servidor Protocolo de configuración dinámica de host (DHCP) de la red.
- **Dominio DNS**: si cambia el sufijo DNS de la subred.
- **Dirección del servidor DNS**: si cambia la dirección IP del servidor DNS de la red.
- **Accesibilidad del dominio de Windows (solo para Windows)**: cambia el estado del dominio de Windows al que está conectado un dispositivo cliente. Esta configuración solo está disponible para dispositivos que ejecutan Windows.
- **Subred**: cambia la dirección de la subred y la máscara.
- **Dirección del servidor WINS (solo para Windows)**: si cambia la dirección IP del servidor WINS de la red. Esta configuración solo está disponible para dispositivos que ejecutan Windows.

- **Capacidad de resolución de nombres** - Si cambia el nombre DNS o NetBIOS del dispositivo cliente.

- **Disponibilidad de la dirección de conexión SSL** - El dispositivo cliente puede o no puede (según la opción que seleccione) establecer una conexión SSL con un servidor específico (nombre:puerto). Para cada servidor, puede especificar adicionalmente un certificado SSL. En este caso, el Agente de red verifica el certificado del servidor además de verificar la capacidad de conexión SSL. Si el certificado no coincide, la conexión falla.

Esta función solo es compatible con los Agentes de red instalados en dispositivos que ejecutan Windows o macOS.

Los parámetros iniciales de la conexión del Agente de red al Servidor de administración se definen durante la instalación del Agente de red. A continuación, si se han creado las reglas de cambio del Agente de red a otros Servidores de administración, el Agente de red responde a los cambios en la configuración de red del siguiente modo:

- Si la configuración de la red cumple con una de las reglas creadas, el Agente de red se conecta con el Servidor de administración que se especifique en ella. Las aplicaciones instaladas en los dispositivos cliente cambian a las directivas fuera de la oficina siempre y cuando así lo contemple una regla.

- Si ninguna de las reglas es aplicable, el Agente de red restaura la configuración predeterminada de la conexión al Servidor de administración especificado durante la instalación. Las aplicaciones instaladas en los dispositivos cliente restablecen las directivas activas.

- Si no se puede acceder al Servidor de administración, el Agente de red utiliza las directivas fuera de la oficina.

El Agente de red cambia a la directiva fuera de la oficina solo si la opción **Activar modo Fuera de la oficina cuando el Servidor de administración no está disponible** está activada en la configuración de la directiva del Agente de red.

Los parámetros de conexión del Agente de red al Servidor de administración se guardan en un perfil de conexión. En el perfil de conexión, puede crear reglas de cambio de dispositivos cliente a directivas fuera de la oficina, así como configurar el perfil de modo que pueda utilizarse únicamente para descargar actualizaciones.

Creación de una regla de cambio de Agente de red por ubicación de red

El cambio de Agente de red por ubicación de red está disponible solo en dispositivos que ejecutan Windows y macOS.

Para crear una regla de cambio del Agente de red de un Servidor de administración a otro si la configuración de red cambia:

1. En el árbol de consola, seleccione el grupo de administración que contenga los dispositivos para los que necesita crear una regla de cambio del Agente de red en función de la descripción de la ubicación de la red.

2. Realice una de las siguientes acciones:

   - Si desea crear una regla para todos los dispositivos del grupo, en el espacio de trabajo del grupo seleccione una directiva del Agente de red en la ficha **Directivas**. Abra la ventana de propiedades de la directiva seleccionada.

   - Si desea crear una regla para un dispositivo seleccionado en un grupo, vaya al espacio de trabajo del grupo, seleccione el dispositivo en la ficha **Dispositivos** y realice las siguientes acciones:

a. Abra la ventana de propiedades del dispositivo seleccionado.

b. En la sección **Aplicaciones** de la ventana de propiedades del dispositivo, seleccione el Agente de red.

c. Abra la ventana de propiedades del Agente de red.

3. En la ventana de propiedades que se abre, en la sección **Conectividad** seleccione la subsección **Perfiles de conexión**.

4. En la sección **Configuración de la ubicación de red**, haga clic en el botón **Agregar**.

5. En la ventana **Descripción nueva** que se abre, configure la descripción de la ubicación de la red y la regla de cambio. Especifique la configuración de la descripción de la ubicación de la red siguiente:

   - Nombre de la descripción de la ubicación de la red

     El nombre de una descripción de la ubicación de la red no puede contener más de 255 caracteres, ni contener símbolos especiales, como ("*<>?\/:|).

   - Utilizar perfil de conexión

     En la lista desplegable se puede especificar el perfil de conexión que utiliza un Agente de red para conectarse al Servidor de administración. Este perfil se utilizará cuando las condiciones de la descripción de la ubicación de la red se cumplan. El perfil de conexión contiene la configuración para la conexión de Agente de red con el Servidor de administración; también define cuando los dispositivos cliente deben cambiar a directivas fuera de la oficina. El perfil solo se utiliza para descargar actualizaciones.

6. En la sección **Cambiar condiciones**, haga clic en el botón **Agregar** para crear una lista de condiciones de descripción de la ubicación de la red.

   Las condiciones de una regla se combinan mediante el operador lógico AND. Para activar una regla de cambio por la descripción de la ubicación de la red, se deben cumplir todas las condiciones de cambio de reglas.

7. En la lista desplegable, seleccione el valor correspondiente al cambio de características de la red en la que está conectado el dispositivo cliente:

   - **Dirección predeterminada de la puerta de enlace de conexión**: si cambia la dirección de la puerta de enlace principal de la red.
   - **Dirección del servidor DHCP**: si cambia la dirección IP del servidor Protocolo de configuración dinámica de host (DHCP) de la red.
   - **Dominio DNS**: si cambia el sufijo DNS de la subred.
   - **Dirección del servidor DNS**: si cambia la dirección IP del servidor DNS de la red.
   - **Accesibilidad del dominio de Windows (solo para Windows)**: cambia el estado del dominio de Windows al que está conectado un dispositivo cliente. Use esta configuración solo para dispositivos que ejecutan Windows.
   - **Subred**: cambia la dirección de la subred y la máscara.
   - **Dirección del servidor WINS (solo para Windows)**: si cambia la dirección IP del servidor WINS de la red. Use esta configuración solo para dispositivos que ejecutan Windows.

- **Capacidad de resolución de nombres** - Si cambia el nombre DNS o NetBIOS del dispositivo cliente.

- **Disponibilidad de la dirección de conexión SSL** - El dispositivo cliente puede o no puede (según la opción que seleccione) establecer una conexión SSL con un servidor específico (nombre:puerto). Para cada servidor, puede especificar adicionalmente un certificado SSL. En este caso, el Agente de red verifica el certificado del servidor además de verificar la capacidad de conexión SSL. Si el certificado no coincide, la conexión falla.

8. En la ventana que se abre, se puede especificar la condición para que el Agente de red cambie a otro Servidor de administración. El nombre de la ventana depende del valor seleccionado en el paso anterior. Especifique la configuración siguiente de la condición de cambio:

   - Valor

     Para crear la condición, se pueden añadir en el campo uno o varios valores.

   - Coincide con al menos un valor de la lista

     Si se selecciona esta opción, la condición se cumplirá sin tener en cuenta ninguno de los valores especificados en la lista **Valor**.

     Esta opción está seleccionada de forma predeterminada.

   - No coincide con ninguno de los valores en la lista

     Si se selecciona esta opción, la condición se cumplirá si el valor no está en la lista **Valor**.

9. En la ventana **Descripción nueva**, seleccione la opción **Descripción activada** para activar el uso de la nueva descripción de la ubicación de la red.

Se creará una nueva regla de cambio por la descripción de la ubicación de la red, según la cual, siempre que se cumplan las condiciones, el Agente de red utilizará el perfil de conexión especificado en la regla para conectarse al Servidor de administración.

Se comprueba la coincidencia de las descripciones de la ubicación de la red con el esquema de red en el orden de aparición en la lista. Si una red coincide con diferentes descripciones, se utilizará la primera. Puede cambiar el orden de las reglas en la lista usando el botón **Arriba** (↑) y **Abajo** (↓).

Cifrar la comunicación con SSL/TLS

Para corregir vulnerabilidades en la red corporativa de su organización, puede habilitar el cifrado de tráfico mediante SSL/TLS. Puede habilitar SSL / TLS en el Servidor de administración y el Servidor de MDM para iOS. Kaspersky Security Center admite SSL v3 y Transport Layer Security (TLS v1.0, 1.1 y 1.2). Puede seleccionar el protocolo de cifrado y las suites de cifrado. Kaspersky Security Center utiliza certificados autofirmados. No se requiere configuración adicional de los dispositivos iOS. También puede utilizar sus propios certificados. Los especialistas de Kaspersky recomiendan utilizar certificados emitidos por autoridades de certificación de confianza.

Servidor de administración

Para configurar los protocolos de cifrado permitidos y las suites de cifrado en el Servidor de administración:

1. Use la utilidad klscflag para configurar los protocolos de cifrado permitidos y las suites de cifrado en el Servidor de administración. Introduzca el siguiente comando en el símbolo del sistema de Windows, usando derechos de administrador:
   `klscflag -fset -pv “.core/.independent” -s Transport -n SrvUseStrictSslSettings -v <value> -t d`

   Especifique el parámetro <value> del comando:

   - `0`: Todos los protocolos de cifrado y suites de cifrado admitidos están activados
   - `1`: SSL v2 está desactivado

     Suites de cifrado:

     - AES256-GCM-SHA384
     - AES256-SHA256
     - AES256-SHA
     - CAMELLIA256-SHA
     - AES128-GCM-SHA256
     - AES128-SHA256
     - AES128-SHA
     - SEED-SHA
     - CAMELLIA128-SHA
     - IDEA-CBC-SHA
     - RC4-SHA
     - RC4-MD5
     - DES-CBC3-SHA
   - `2`: SSL v2 y SSL v3 se activan (valor predeterminado)

     Suites de cifrado:

     - AES256-GCM-SHA384
     - AES256-SHA256
     - AES256-SHA
     - CAMELLIA256-SHA
     - AES128-GCM-SHA256
     - AES128-SHA256

- AES128-SHA
- SEED-SHA
- CAMELLIA128-SHA
- IDEA-CBC-SHA
- RC4-SHA
- RC4-MD5
- DES-CBC3-SHA

- 3: solo TLS v1.2.
  Suites de cifrado:
  - AES256-GCM-SHA384
  - AES256-SHA256
  - AES256-SHA
  - CAMELLIA256-SHA
  - AES128-GCM-SHA256
  - AES128-SHA256
  - AES128-SHA
  - CAMELLIA128-SHA

2. Reinicie los siguientes servicios de Kaspersky Security Center 14:
   - Servidor de administración
   - Servidor Web
   - Proxy de activación

Servidor de MDM para iOS

La conexión entre los dispositivos iOS y el Servidor de MDM para iOS está encriptada por defecto.

Para configurar los protocolos de cifrado permitidos y las suites de cifrado en el Servidor de MDM para iOS:

1. Abra el registro del sistema del dispositivo cliente que tiene instalado el Servidor de MDM para iOS (por ejemplo, localmente, usando el comando regedit en el menú **Inicio** → **Ejecutar**).
2. Vaya al siguiente subárbol:
   - Para un sistema de 64 bits:
     `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOS`

- Para un sistema de 32 bits:
  `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\`

3. Cree una clave con el nombre `StrictSslSettings`.
4. Especifique `DWORD` como tipo de clave.
5. Configure el valor de clave:
   - `2`: SSL v3 se desactiva (están permitidos TLS 1.0, TLS 1.1 y TLS 1.2)
   - `3`: solo TLS 1.2 (valor predeterminado)
6. Reiniciar el servicio del Servidor de MDM para iOS de Kaspersky Security Center 14.

Notificaciones de eventos

Esta sección describe cómo seleccionar un método para enviar notificaciones del administrador sobre eventos en dispositivos cliente, y cómo ajustar la configuración de las notificaciones de eventos.

También describe cómo probar la distribución de notificaciones de eventos usando el virus de prueba Eicar.

Configuración de notificación de eventos

Kaspersky Security Center le permite seleccionar un método para notificar al administrador los eventos que tienen lugar en los dispositivos cliente, así como configurar la notificación:

- Correo electrónico. Cuando se produce un evento, la aplicación envía una notificación a las direcciones de correo electrónico especificadas. Puede editar el texto de la notificación.
- SMS. Cuando se produce un evento, la aplicación envía una notificación a los números de teléfono especificados. Puede configurar las notificaciones por SMS para que se envíen a través de la puerta de enlace de correo.
- Archivo ejecutable. Cuando se produce un evento en un dispositivo, el archivo ejecutable se inicia en la estación de trabajo del administrador. Mediante el archivo ejecutable, el administrador puede recibir los parámetros de cualquier evento ocurrido.

Para configurar las notificaciones de los eventos sucedidos en los dispositivos cliente:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. Haga clic en el enlace **Configurar las notificaciones y la exportación de eventos** y seleccione el valor **Configurar notificaciones** en la lista desplegable.

   De este modo, se abre la ventana **Propiedades: Eventos**.
4. En la sección **Notificación**, seleccione un método de notificación (por correo electrónico, SMS o un archivo ejecutable) y defina la configuración de la notificación:

- Correo electrónico

La ficha **Correo electrónico** le permite configurar las notificaciones de correo electrónico para eventos.

En el campo **Destinatarios (correo electrónico)**, especifique las direcciones de correo electrónico a las cuales la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolos con punto y coma. Puede usar los siguientes valores:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

Si activa la opción **Buscar registros MX por DNS**, puede utilizar varios registros MX de las direcciones IP para el mismo nombre DNS del servidor SMTP. El mismo nombre DNS puede tener varios registros MX con diferentes valores de prioridad de recepción de mensajes de correo electrónico. El Servidor de administración intenta enviar notificaciones del correo electrónico al servidor SMTP en orden ascendente de prioridad de registros MX. Esta opción está desactivada de forma predeterminada.

Si activa la opción **Buscar registros MX por DNS** y no activa el uso de la configuración de TLS, le recomendamos que use la configuración de DNSSEC en el dispositivo de su servidor como medida adicional de protección para el envío de notificaciones del correo electrónico.

Haga clic en el enlace **Configuración** para definir ajustes de notificación adicionales:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de autenticación ESMTP

Debe especificar una cuenta para la autenticación en un servidor SMTP si la opción de autenticación ESMTP está activada para el servidor SMTP.

- Configuración de TLS para el servidor SMTP:
  - **Do not use TLS**

    Puede seleccionar esta opción si desea desactivar el cifrado de mensajes de correo electrónico.
  - **Use TLS if supported by SMTP server**

    Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.
  - **Always use TLS, check the server certificate for validity**

    Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse con el servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si elige el valor **Always use TLS, check the server certificate for validity**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

Puede especificar la configuración de TLS para un servidor SMTP:

- Busque un archivo de certificado para el servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo en el Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

- Busque un archivo de certificado para el cliente:

Puede utilizar un certificado que haya recibido de cualquier fuente, por ejemplo, de cualquier autoridad de certificación confiable. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Ambos archivos no dependen el uno del otro y, por ende, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

- Contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y su clave privada. Cuando se cargue el archivo, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

El campo **Mensaje de notificación** contiene el texto estándar con información sobre el evento que la aplicación envía cuando un evento ocurre. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje añadiendo otros parámetros sustitutos con detalles más relevantes del evento. La lista de parámetros sustitutos está disponible haciendo clic en el botón a la derecha del campo.

Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que escribir dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

Haga clic en el enlace **Configurar límite numérico de notificaciones**, para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en el botón **Enviar mensaje de prueba** para verificar si ha configurado las notificaciones correctamente. La aplicación debería enviar una notificación de prueba a las direcciones de correo electrónico que ha especificado.

- SMS

La ficha **SMS** le permite configurar la transmisión de notificaciones por SMS de varios eventos a un teléfono celular. Los mensajes SMS se enviarán a través de una puerta de enlace de correo.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las cuales la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma. Las notificaciones se transmitirán a los números de teléfono asociados con las direcciones de correo electrónico especificadas.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolos con punto y coma. Puede usar los siguientes valores:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

Haga clic en el enlace **Configuración** para definir ajustes de notificación adicionales:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de autenticación ESMTP

En caso de ser necesario, puede especificar una cuenta para la autenticación en un servidor SMTP si la opción de autenticación ESMTP está activada para el servidor SMTP.

- Configuración de TLS para un servidor SMTP

Puede desactivar el uso de TLS, usar TLS si el servidor SMTP admite este protocolo o forzar el uso de TLS únicamente. Si elige usar solo TLS, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, si elige usar solo TLS, puede especificar un certificado para la autenticación de clientes en el servidor SMTP.

- Busque un archivo de certificado para el servidor SMTP

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo en Kaspersky Security Center. Kaspersky Security Center verifica si el certificado del servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado del servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

Debe cargar un solo archivo que contenga el certificado y su clave privada. Cuando se cargue el archivo, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede estar vacía si la clave privada no está cifrada. El campo **Mensaje de notificación** contiene el texto estándar con información sobre el evento que la aplicación envía cuando un evento ocurre. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje añadiendo otros parámetros sustitutos con detalles más relevantes del evento. La lista de parámetros sustitutos está disponible haciendo clic en el botón a la derecha del campo.

Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que escribir dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

Haga clic en el enlace **Configurar límite numérico de notificaciones** para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en el botón **Enviar mensaje de prueba** para comprobar si ha configurado correctamente las notificaciones. La aplicación debería enviar una notificación de prueba al destinatario que ha especificado.

- Archivo ejecutable para lanzar

  Si se selecciona este método de notificación, en el campo de entrada puede especificar la aplicación que se iniciará cuando ocurra un evento.

  Al hacer clic en el enlace **Configurar límite numérico de notificaciones**, puede especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

  Al hacer clic en el botón **Enviar mensaje de prueba** le permite verificar si ha configurado las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que ha especificado.

5. En el campo **Mensaje de notificación**, introduzca el texto que la aplicación enviará cuando se produzca un evento.

   Puede usar la lista desplegable a la derecha del campo del texto para agregar los parámetros de sustitución con detalles del evento (por ejemplo, la descripción del evento o la hora en que ocurrió).

   Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que especificar dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

6. Haga clic en el botón **Enviar mensaje de prueba** para comprobar si la notificación se ha configurado correctamente.

   La aplicación envía una notificación de prueba al usuario especificado.

7. Haga clic en **Aceptar** para guardar los cambios.

Los parámetros reajustados de la notificación se aplicarán a todos los eventos que tengan lugar en los dispositivos cliente.

Puede anular la configuración de notificación para ciertos eventos en la sección **Configuración de eventos** de la Configuración del Servidor de administración, de una configuración de directiva o de una configuración de aplicación.

Comprobación de notificaciones

Para comprobar si se han enviado las notificaciones del evento, la aplicación utiliza la notificación de la detección de "virus" de prueba EICAR en los dispositivos cliente.

Para comprobar el envío de notificaciones de eventos:

1. Detenga la tarea de protección del sistema de archivos en tiempo real en un dispositivo cliente y copie el "virus" de prueba EICAR en ese equipo. A continuación, vuelva a activar la protección en tiempo real del sistema de archivos.

2. Ejecute una tarea de análisis para los dispositivos cliente en un grupo de administración o para dispositivos específicos, incluido uno que tenga el "virus" EICAR.

   Si la tarea de análisis se ha configurado correctamente, se detectará el "virus" de prueba. Si las notificaciones se han configurado correctamente, recibirá una notificación sobre la detección de un virus.

   En el espacio de trabajo del nodo **Servidor de administración**, en la ficha **Eventos**, la selección de **Eventos recientes** muestra un registro de detección de un "virus".

El “virus” de prueba EICAR no contiene código que pueda dañar su dispositivo. Sin embargo, la mayoría de fabricantes de aplicaciones de seguridad identifican este archivo como un virus. Puede descargar el "virus" de prueba desde el sitio web oficial de EICAR.

Notificaciones de eventos mostradas mediante archivos ejecutables

Kaspersky Security Center puede informar al administrador sobre los eventos de los dispositivos cliente mediante la ejecución de un archivo ejecutable. El archivo ejecutable debe contener otro archivo ejecutable con los marcadores de posición del evento que se transferirá al administrador.

Marcadores de posición para describir un evento

Marcador de posición	Descripción del marcador de posición
%SEVERITY%	Nivel de importancia del evento
%COMPUTER%	Nombre del dispositivo en el que ocurrió el evento
%DOMAIN%	Dominio
%EVENT%	Evento
%DESCR%	Descripción de eventos
%RISE_TIME%	Hora de creación
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nombre de la tarea
%KL_PRODUCT%	Agente de red de Kaspersky Security Center
%KL_VERSION%	Número de versión del Agente de red
%HOST_IP%	Dirección IP
%HOST_CONN_IP%	Dirección IP de conexión

Ejemplo:
Las notificaciones de eventos se envían por medio de un archivo ejecutable (como script1.bat), dentro del cual se inicia otro archivo ejecutable (como script2.bat) con el marcador de posición %COMPUTER%. Cuando ocurre un evento, el archivo script1.bat se abre en el dispositivo del administrador, que a su vez abre el archivo script2.bat con el marcador de posición %COMPUTER%. El administrador recibe el nombre del dispositivo en el que ha ocurrido el evento.

Configuración de la interfaz

Puede configurar la interfaz de Kaspersky Security Center para:

- Mostrar y ocultar objetos en el árbol de la consola, el espacio de trabajo y las ventanas de propiedades de los objetos (carpetas, secciones), según las funciones que se utilicen.
- Mostrar y ocultar elementos de la ventana principal (por ejemplo, el árbol de la consola o menús estándar como **Acciones** y **Ver**).

Para configurar la interfaz de Kaspersky Security Center de acuerdo con el conjunto de funciones utilizado actualmente:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. En la barra de menús de la ventana principal de la aplicación, seleccione **Ver** → **Configuración de la interfaz**.
3. En la ventana **Configuración de la interfaz** que se abre, configure la visualización de los elementos de la interfaz con las siguientes casillas de verificación:

- Mostrar Administración de vulnerabilidades y parches

  Si esta opción está activada, la carpeta **Instalación remota** muestra la subcarpeta **Desplegar imágenes de dispositivos** y la carpeta **Repositorios** muestra la subcarpeta **Hardware**.

  Esta opción está desactivada de forma predeterminada si el Asistente de inicio rápido no ha finalizado. Esta opción está activada de forma predeterminada una vez finalizado el Asistente de inicio rápido.

- Mostrar Protección y cifrado de datos

  Si esta opción está activada, el árbol de la consola muestra la carpeta **Protección y cifrado de datos**.

  Esta opción está activada de forma predeterminada.

- Mostrar Configuración de Control de Endpoint

  Si esta opción está activada, las siguientes subsecciones se muestran en la sección **Controles de seguridad** de la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows:
  - **Control de aplicaciones**
  - **Monitor de vulnerabilidades**
  - **Control de dispositivos**
  - **Control web**

  Si esta opción está desactivada, estas subsecciones no se muestran en la sección **Controles de seguridad**.

  Esta opción está activada de forma predeterminada.

- Mostrar Administración de dispositivos móviles

  Si esta opción está activada, la función **Administración de dispositivos móviles** está disponible. Después de reiniciar la aplicación, el árbol de la consola muestra la carpeta **Dispositivos móviles**.

  Esta opción está activada de forma predeterminada.

- Mostrar Servidores de administración secundarios

Si la casilla de verificación está seleccionada, el árbol de la consola muestra los nodos de los Servidores de administración secundarios y virtuales dentro de los grupos de administración. Están disponible las características conectadas con los Servidores de administración secundarios y virtuales, por ejemplo, la creación de tareas para la instalación remota de aplicaciones en Servidores de administración secundarios.

De forma predeterminada, esta casilla está en blanco.

- Mostrar secciones de configuración de seguridad

  Si esta opción está activada, la sección **Seguridad** se muestra en la ventana de propiedades del Servidor de administración, los grupos de administración y otros objetos. Esta opción le permite conceder a los usuarios y grupos de usuarios permisos personalizados para trabajar con objetos.

  Esta opción está desactivada de forma predeterminada.

4. Haga clic en **Aceptar**.

Para aplicar algunos de los cambios, debe cerrar la ventana principal de la aplicación y volver a abrirla.

Para configurar la visualización de elementos en la ventana principal de la aplicación:

1. En la barra de menús de la ventana principal de la aplicación, seleccione **Ver** → **Configurar**.
2. En la ventana **Configurar vista** que se abre, configure la visualización de los elementos de la ventana principal mediante las casillas de verificación.
3. Haga clic en **Aceptar**.

Detección de dispositivos en red

Esta sección describe los pasos que debe seguir después de la instalación de Kaspersky Security Center.

Escenario: Detección de dispositivos en red

Debe realizar la detección de dispositivos antes de instalar las aplicaciones de seguridad. Cuando se detecten todos los dispositivos en red, puede obtener información sobre ellos y administrarlos a través de directivas. Se necesitan sondeos de red regulares para detectar si hay dispositivos nuevos y si los dispositivos detectados todavía están en la red.

La detección de dispositivos en red se realiza en etapas:

1. **Detección inicial de dispositivos**

   El Asistente de inicio rápido le guía a través de la detección inicial de dispositivos y lo ayuda a encontrar dispositivos en red, como ordenadores, tabletas y teléfonos móviles. También puede realizar la detección de dispositivos manualmente.

2. **Configuración de futuros sondeos**

Decida qué tipo(s) de detección desea utilizar regularmente. Asegúrese de que este tipo esté habilitado y que el calendario de sondeo cumpla con las necesidades de su organización. Al configurar el horario de sondeo, utilice las recomendaciones para la red de frecuencia de sondeo.

3. **La configuración de reglas para agregar dispositivos detectados a grupos de administración (opcional)**

   Si aparecen nuevos dispositivos de la red, que se detectan durante las sondeos regulares y se incluyen automáticamente en el grupo **Dispositivos no asignados**. Si lo desea, puede configurar las reglas para automático el traslado de estos dispositivos al grupo **Dispositivos administrados**. También puede configurar reglas de retención.

   Si omite este paso que configura la regla, todos los dispositivos recién detectados van al grupo **Dispositivos no asignados** y se quedan allí. Si lo desea, puede mover estos dispositivos al grupo de **Dispositivos administrados** manualmente. Si mueve estos dispositivos manualmente al grupo **Dispositivos administrados**, puede analizar la información sobre cada dispositivo y decidir si desea moverlo a un grupo de administración y, de ser así, a qué grupo.

Resultados

Al completar el escenario se obtienen los siguientes resultados:

- El Servidor de administración de Kaspersky Security Center detecta los dispositivos que están en la red y le proporciona información sobre ellos.
- Los sondeos futuros se configuran y funcionan de acuerdo con el calendario programado.
- Los dispositivos recién descubiertos se arreglan según las reglas configuradas. (O, si no se configura ninguna regla, los dispositivos se quedan en el grupo **Dispositivos no asignados**).

Dispositivos no asignados

Esta sección proporciona información sobre cómo administrar dispositivos en una red empresarial si no están incluidos en un grupo de administración.

Detección de dispositivos

Esta sección describe los tipos de detección de dispositivos disponibles en Kaspersky Security Center y proporciona información sobre cómo usar cada tipo.

El Servidor de administración recibe la información sobre la estructura de la red y sus dispositivos mediante sondeos periódicos. La información se registra en la base de datos del Servidor de administración. El Servidor de administración puede utilizar los siguientes tipos de sondeo:

- **Sondeo de la red de Windows**. El Servidor de administración puede realizar dos tipos de sondeo de red de Windows: rápido y completo. Durante un sondeo rápido, el Servidor de administración únicamente recopilará la información de los dispositivos de la lista de nombre NetBIOS de todos los dominios y grupos de trabajo de la red. Durante un sondeo completo, se solicita más información de cada dispositivo cliente, como nombre del sistema operativo, dirección IP, nombre DNS y nombre NetBIOS. De forma predeterminada, tanto el sondeo rápido como el sondeo completo están habilitados. El sondeo de la red de Windows puede no detectar dispositivos, por ejemplo, si los puertos UDP 137, UDP 138, TCP 139 están cerrados en el enrutador o por el firewall.

- **Sondeo de Active Directory**. El Servidor de administración recopila información de la estructura de la unidad de Active Directory y de los nombres DNS de los dispositivos de los grupos de Active Directory. Este tipo de sondeo está habilitado de forma predeterminada. Le recomendamos que utilice el sondeo de Active Directory si utiliza el directorio Activo; de lo contrario, el Servidor de administración no detecta ningún dispositivo. Si usa Active Directory pero algunos de los dispositivos en red no están listados como miembros, estos dispositivos no pueden ser detectados por el sondeo de Active Directory.

- **Sondeo de rangos IP**. El Servidor de administración sondea los rangos IP especificados utilizando paquetes ICMP o el protocolo NBNS y recopila un conjunto completo de datos en los dispositivos de esos rangos IP. Este tipo de sondeo está deshabilitado de forma predeterminada. No se recomienda usar este tipo de sondeo si usa el sondeo de red de Windows y / o el sondeo de Active Directory.

- **Sondeo de Zeroconf**. Un punto de distribución que sondea la red IPv6 mediante el uso de una red de configuración cero (también denominada *Zeroconf*). Este tipo de sondeo está deshabilitado de forma predeterminada. Puede usar el sondeo de Zeroconf si el punto de distribución ejecuta Linux.

Si configura y activa reglas de movimiento del dispositivo, los dispositivos recién descubiertos automáticamente se incluyen en el grupo de **Dispositivos administrados**. Si ninguna regla de movimiento se ha activado, los dispositivos recién descubiertos automáticamente se incluyen en el grupo de **Dispositivos no asignados**.

Puede modificar la configuración de detección de dispositivos para cada tipo. Por ejemplo, es posible que desee modificar la programación de sondeo o establecer si desea sondar todo el bosque de Active Directory o solo un dominio específico.

Sondeo de la red de Windows

Acerca del sondeo de la red de Windows

Durante un sondeo rápido, el Servidor de administración únicamente recopilará la información de los dispositivos de la lista de nombre NetBIOS de todos los dominios y grupos de trabajo de la red. Durante un sondeo completo, en cada dispositivo cliente se solicita la siguiente información:

- Nombre del sistema operativo
- Dirección IP
- Nombre DNS
- Nombre NetBIOS

Tanto el sondeo rápido como el sondeo completo requieren lo siguiente:

- Los puertos UDP 137/138, TCP 139, UDP 445 y TCP 445 deben estar disponibles en la red.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo del navegador principal debe estar activado en el Servidor de administración.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo del navegador principal debe estar activado en los dispositivos cliente:
  - En al menos un dispositivo, si el número de dispositivos en red no supera 32.
  - En al menos un dispositivo por cada 32 dispositivos en red.

El sondeo completo solo puede ejecutarse si el sondeo rápido se ha ejecutado al menos una vez.

Visualización y modificación de los parámetros para el sondeo de la red de Windows

Para modificar los parámetros para el sondeo de la red de Windows, realice lo siguiente:

1. En el árbol de consola, en la carpeta **Detección de dispositivos**, seleccione la subcarpeta **Dominios**.

   Puede ir de la carpeta **Dispositivos no asignados** a la carpeta **Detección de dispositivos** haciendo clic en el botón **Sondear ahora**.

   En el espacio de trabajo de la subcarpeta **Dominios**, se muestra la lista de los dispositivos.

2. Haga clic en **Sondear ahora**.

   Se abre la ventana de propiedades del dominio. Si lo desea, modifique la configuración del sondeo de la red Windows:

   - Permitir el sondeo de las redes de Windows

     Esta opción está seleccionada de forma predeterminada. Si no desea realizar un sondeo de la red de Windows (por ejemplo, si cree que el sondeo de Active Directory es suficiente), puede deseleccionar esta opción.

   - Programar un sondeo rápido

El intervalo predeterminado es de 15 minutos.

Durante un sondeo rápido, el Servidor de administración únicamente recopilará la información de los dispositivos de la lista de nombre NetBIOS de todos los dominios y grupos de trabajo de la red.

Los datos recibidos en el siguiente sondeo reemplazan completamente los datos antiguos.

Las siguientes opciones de programación del sondeo están disponibles:

- **Cada N días**

  El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

  De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.

- **Cada N minutos**

  El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.

  De forma predeterminada, el sondeo se ejecuta cada cinco minutos, a partir de la hora actual del sistema.

- **Por días de la semana**

  El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.

  De forma predeterminada, el sondeo se realiza todos los viernes a las 6:00:00 p.m.

- **Cada mes, en días concretos de las semanas seleccionadas**

  El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 6:00:00 p.m.

- **Ejecutar tareas no realizadas**

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de que se encienda o esperar a la próxima vez que se programe el sondeo.

  Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de que se encienda.

  Si esta opción está desactivada, el Servidor de administración espera a la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

- **Programar un sondeo completo**

El periodo predeterminado es de una hora. Los datos recibidos en el siguiente sondeo reemplazan completamente los datos antiguos.

Las siguientes opciones de programación del sondeo están disponibles:

- **Cada N días**

  El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

  De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.

- **Cada N minutos**

  El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.

  De forma predeterminada, el sondeo se ejecuta cada cinco minutos, a partir de la hora actual del sistema.

- **Por días de la semana**

  El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.

  De forma predeterminada, el sondeo se realiza todos los viernes a las 6:00:00 p.m.

- **Cada mes, en días concretos de las semanas seleccionadas**

  El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 6:00:00 p.m.

- **Ejecutar tareas no realizadas**

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de que se encienda o esperar a la próxima vez que se programe el sondeo.

  Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de que se encienda.

  Si esta opción está desactivada, el Servidor de administración espera a la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

Si desea realizar el sondeo de inmediato, haga clic en **Sondear ahora**. Ambos tipos de sondeos comenzarán.

En el Servidor de administración virtual, puede ver y editar la configuración de sondeo de la red Windows en la ventana de propiedades del punto de distribución, en la sección **Detección de dispositivos**.

Sondeo de Active Directory

Use el sondeo de Active Directory si usa Active Directory; de lo contrario, se recomienda utilizar otros tipos de sondeo. Si usa Active Directory pero algunos de los dispositivos en red no están listados como miembros, estos dispositivos no pueden ser detectados por el sondeo de Active Directory.

Visualización y modificación de los parámetros para el sondeo de Active Directory

Para ver y modificar los parámetros para realizar sondeos en los grupos de Active Directory:

1. En el árbol de consola, en la carpeta **Detección de dispositivos**, seleccione la subcarpeta **Active Directory**.

   De forma alternativa, puede ir desde la carpeta **Dispositivos no asignados** a la carpeta **Detección de dispositivos** haciendo clic en el botón **Sondear ahora**.

2. Haga clic en **Configurar sondeo**.

   Se abrirá la ventana de propiedades de Active Directory. Si lo desea, modifique la configuración del sondeo del grupo de Active Directory:

   - **Permitir sondeo de Active Directory**

     Esta opción está seleccionada de forma predeterminada. Sin embargo, si no utiliza Active Directory, el sondeo no recupera ningún resultado. En este caso, puede deseleccionar esta opción.

   - **Programar sondeo**

El periodo predeterminado es de una hora. Los datos recibidos en el siguiente sondeo reemplazan completamente los datos antiguos.

Las siguientes opciones de programación del sondeo están disponibles:

- **Cada N días**

  El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

  De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.

- **Cada N minutos**

  El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.

  De forma predeterminada, el sondeo se ejecuta cada cinco minutos, a partir de la hora actual del sistema.

- **Por días de la semana**

  El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.

  De forma predeterminada, el sondeo se realiza todos los viernes a las 6:00:00 p.m.

- **Cada mes, en días concretos de las semanas seleccionadas**

  El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 6:00:00 p.m.

- **Ejecutar tareas no realizadas**

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de que se encienda o esperar a la próxima vez que se programe el sondeo.

  Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de que se encienda.

  Si esta opción está desactivada, el Servidor de administración espera a la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

- **Avanzado**

Puede seleccionar qué dominios de Active Directory sondear:

- El dominio de Active Directory al cual Kaspersky Security Center pertenece.
- El bosque de dominio al cual Kaspersky Security Center pertenece.
- Lista especificada de dominios de Active Directory.

  Si selecciona esta opción, puede añadir dominios a la cobertura de sondeo:

  - Haga clic en el botón **Agregar**.
  - En los campos correspondientes, especifique la dirección del controlador de dominio, el nombre y la contraseña de la cuenta para acceder a él.
  - Haga clic en **Aceptar** para guardar los cambios.

  Puede seleccionar la dirección del controlador de dominio en la lista y hacer clic en los **botones Modificar** o **Eliminar** para modificarla o eliminarla.
- Haga clic en **Aceptar** para guardar los cambios.

Si desea realizar el sondeo de inmediato, haga clic en el botón **Sondear ahora**.

En el Servidor de administración virtual, puede ver y editar la configuración de sondeo de los grupos de Active Directory en la ventana de propiedades del punto de distribución, en la sección **Detección de dispositivos**.

Sondeo de rangos IP

El Servidor de administración sondea los rangos IP especificados utilizando paquetes ICMP o el protocolo NBNS y recopila un conjunto completo de datos en los dispositivos de esos rangos IP. Este tipo de sondeo está deshabilitado de forma predeterminada. No se recomienda usar este tipo de sondeo si usa el sondeo de red de Windows y / o el sondeo de Active Directory.

Visualización y modificación de los parámetros para el sondeo de rangos IP

Para ver y modificar los parámetros para realizar sondeos en los grupos del rango IP:

1. En el árbol de consola, en la carpeta **Detección de dispositivos**, seleccione la subcarpeta **Rangos IP**.

   Puede proceder desde la carpeta **Dispositivos no asignados** a la carpeta **Detección de dispositivos** haciendo clic en **Sondear ahora**.
2. Si lo desea, en la subcarpeta **Rangos IP**, haga clic en **Agregar subred** para añadir un rango IP para el sondeo y después haga clic en **Aceptar**.
3. Haga clic en **Configurar sondeo**.

   Se abre la ventana de propiedades de rango de IP. Si lo desea, puede modificar la configuración del sondeo del rango IP:

   - Activar sondeos de rangos IP

Esta opción no está seleccionada de forma predeterminada. No se recomienda usar este tipo de sondeo si usa el sondeo de red de Windows y/o el sondeo de Active Directory.

- **Programar sondeo**

  El intervalo predeterminado es de 420 minutos. Los datos recibidos en el siguiente sondeo reemplazan completamente los datos antiguos.

  Las siguientes opciones de programación del sondeo están disponibles:

  - **Cada N días**

    El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

    De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.

  - **Cada N minutos**

    El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.

    De forma predeterminada, el sondeo se ejecuta cada cinco minutos, a partir de la hora actual del sistema.

  - **Por días de la semana**

    El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.

    De forma predeterminada, el sondeo se realiza todos los viernes a las 6:00:00 p.m.

  - **Cada mes, en días concretos de las semanas seleccionadas**

    El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.

    De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 6:00:00 p.m.

  - **Ejecutar tareas no realizadas**

    Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de que se encienda o esperar a la próxima vez que se programe el sondeo.

    Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de que se encienda.

    Si esta opción está desactivada, el Servidor de administración espera a la próxima vez que se programe el sondeo.

    Esta opción está activada de forma predeterminada.

Si desea realizar el sondeo de inmediato, haga clic en **Sondear ahora**. Este botón solo está disponible Si ha seleccionado **Activar sondeos de rangos IP**.

En el Servidor de administración virtual, puede ver y editar la configuración de sondeo de rangos IP en la ventana de propiedades del punto de distribución, en la sección **Detección de dispositivos**. Los dispositivos cliente detectados durante el sondeo de los rangos IP se muestran en la carpeta **Dominios** del Servidor de administración virtual.

Sondeo de Zeroconf

Este tipo de sondeo solo es compatible con los puntos de distribución basados en Linux.

Un punto de distribución puede sondear las redes que tienen dispositivos con direcciones IPv6. En este caso, no se especifican los rangos de IP y el punto de distribución sondea toda la red mediante el uso de una red de configuración cero (denominada *Zeroconf*). Para empezar a usar Zeroconf, debe instalar la utilidad avahi-browse en el punto de distribución.

Para activar el sondeo de Zeroconf:

1. En el árbol de consola, en la carpeta **Detección de dispositivos**, seleccione la subcarpeta **Rangos IP**.

   Puede proceder desde la carpeta **Dispositivos no asignados** a la carpeta **Detección de dispositivos** haciendo clic en **Sondear ahora**.

2. Haga clic en **Configurar sondeo**.

3. En la ventana de las propiedades de los rangos de IP que se abre, seleccione **Activar el sondeo con la tecnología Zeroconf**.

Después de esto, el punto de distribución empieza a sondear su red. En este caso, se ignoran los rangos de IP especificados.

Trabajo con dominios de Windows. Visualización y cambio de los parámetros del dominio

Para modificar los parámetros del dominio:

1. En el árbol de consola, en la carpeta **Detección de dispositivos**, seleccione la subcarpeta **Dominios**.

2. Seleccione un dominio y abra su ventana de propiedades por algunos de los siguientes medios:

   - Seleccione **Propiedades** en el menú contextual del dominio.

   - Al hacer clic en el enlace **Mostrar propiedades del grupo**.

   Se abrirá la ventana **Propiedades: <nombre de dominio>** en la cual puede configurar el dominio seleccionado.

Configuración de reglas de retención para dispositivos no asignados

Una vez finalizado el sondeo de la red de Windows, los dispositivos encontrados se colocan en subgrupos del grupo de administración de dispositivos no asignados. Puede encontrar este grupo de administración en **Avanzado → Detección de dispositivos → Dominios**. El grupo primario es **Dominios**. Contiene grupos secundarios nombrados después de los dominios correspondientes y grupos de trabajo que se han encontrado durante el sondeo de red. El grupo primario también puede contener el grupo de administración de dispositivos móviles. Puede configurar las reglas de retención de los dispositivos no asignados para el grupo primario y para cada uno de los grupos secundarios. Las reglas de retención no dependen de la configuración de sondeo de la red y funcionan incluso si el sondeo de la red está desactivado.

Para configurar reglas de retención para dispositivos no asignados:

1. En el árbol de la consola, en la carpeta de **Detección de dispositivos**, realice una de las siguientes acciones:

   - Para configurar los ajustes del grupo primario, haga clic con el botón derecho en la subcarpeta **Dominios** y seleccione **Propiedades**.

     Se abrirá la ventana de propiedades del grupo primario.

   - Para configurar los ajustes de un grupo secundario, haga clic con el botón derecho en su nombre y seleccione **Propiedades**.

     Se abrirá la ventana de propiedades del grupo secundario.

2. En la sección **Dispositivos**, configure los siguientes parámetros:

   - **Quitar el dispositivo del grupo si ha estado inactivo durante más de (días)**

     Si esta opción está activada, puede especificar el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo. De forma predeterminada, esta opción también se distribuye a los grupos secundarios. De forma predeterminada, el intervalo de tiempo es 7 día.

     Esta opción está activada de forma predeterminada.

   - **Heredar del grupo primario**

     Si esta opción está activada, el periodo de retención para los dispositivos en el grupo actual se hereda del grupo primario y no se puede cambiar.

     Esta opción solo está disponible para grupos secundarios.

     Esta opción está activada de forma predeterminada.

   - **Forzar herencia en grupos secundarios**

     Los valores de configuración se distribuirán a grupos secundarios, pero en las propiedades de los grupos secundarios estas configuraciones están bloqueadas.

     Esta opción está desactivada de forma predeterminada.

Sus cambios están guardados y aplicados.

Trabajo con rangos IP

Se pueden personalizar los rangos IP existentes y crear otros nuevos.

Creación de un rango IP

Para crear una rango IP:

1. En el árbol de consola, en la carpeta **Detección de dispositivos**, seleccione la subcarpeta **Rangos IP**.
2. En el menú contextual de la carpeta, seleccione **Nueva** → **Rango IP**.
3. En la ventana **Nuevo rango IP** que se abrirá, personalice el nuevo rango IP.

El nuevo rango IP aparece en la carpeta **Rangos IP**.

Visualización y cambio de los parámetros de rangos IP

Para modificar los parámetros de rango IP:

1. En el árbol de consola, en la carpeta **Detección de dispositivos**, seleccione la subcarpeta **Rangos IP**.
2. Seleccione un rango IP y abra su ventana de propiedades por algunos de los siguientes medios:
   - Seleccione **Propiedades** en el menú contextual del rango IP.
   - Al hacer clic en el enlace **Mostrar propiedades del grupo**.

Se abrirá la ventana **Propiedades: <nombre del rango IP>** en la cual puede configurar las propiedades del rango IP seleccionado.

Trabajo con los grupos de Active Directory. Visualización y modificación de los parámetros de grupo

Para modificar los parámetros del grupo del Active Directory:

1. En el árbol de consola, en la carpeta **Detección de dispositivos**, seleccione la subcarpeta **Active Directory**.
2. Seleccione un grupo de Active Directory y abra su ventana de propiedades por algunos de los siguientes medios:
   - Seleccione **Propiedades** en el menú contextual del rango IP.
   - Al hacer clic en el enlace **Mostrar propiedades del grupo**.

Se abrirá la ventana **Propiedades: <nombre de grupo de Active Directory>** en la cual puede configurar el grupo seleccionado de Active Directory.

Creación de reglas para trasladar dispositivos automáticamente a los grupos de administración

Los dispositivos se pueden configurar de tal manera que, una vez descubiertos durante un sondeo de red en la empresa, se los traslade automáticamente a grupos de administración.

Para configurar las reglas de traslado automático a grupos de administración:

1. En el árbol de consola, seleccione la carpeta **Dispositivos no asignados**.
2. En el espacio de trabajo de esta carpeta, haga clic en **Configurar reglas**.

   De este modo, se abre la ventana **Propiedades: Dispositivos no asignados**. En la sección **Mover dispositivos**, configure las reglas de traslado automático de dispositivos a grupos de administración.

La primera regla aplicable en la lista (de arriba a abajo de la lista) se aplicará al dispositivo.

Uso del modo dinámico para VDI en los dispositivos cliente

Se puede desplegar una infraestructura virtual en una red corporativa mediante máquinas virtuales temporales. Kaspersky Security Center detecta las máquinas virtuales temporales y agrega información sobre ellas a la base de datos del Servidor de administración. Cuando un usuario termina de usar una máquina virtual temporal, dicha máquina se quita de la infraestructura virtual. Pero es posible guardar registros sobre las máquinas virtuales quitadas en la base de datos del Servidor de administración. Asimismo, se pueden mostrar máquinas virtuales no existentes en la Consola de administración.

Para evitar que se guarde información sobre las máquinas virtuales no existentes, Kaspersky Security Center admite el modo dinámico de la Infraestructura de Escritorio Virtual (VDI). El administrador puede habilitar la compatibilidad con el modo dinámico para VDI en las propiedades del paquete de instalación del Agente de red que se instalará en la máquina virtual temporal (solo Windows).

Cuando se deshabilita una máquina virtual temporal, el Agente de red informa al Servidor de administración de que la máquina se ha deshabilitado. Cuando una máquina virtual se ha deshabilitado correctamente, se quita de la lista de dispositivos conectados al Servidor de administración. Si la máquina virtual se deshabilita con errores y el Agente de red no envía ninguna notificación acerca de la máquina virtual deshabilitada al Servidor de administración, se recurre a una copia de seguridad. En este caso, se quita la máquina virtual de la lista de dispositivos conectados al Servidor de administración tras tres intentos fallidos de sincronización con el Servidor de administración.

Activación del modo VDI dinámico en las propiedades de un paquete de instalación para el Agente de red

El uso del modo dinámico para la Infraestructura de Escritorio Virtual (VDI) solo está disponible para dispositivos que ejecutan Windows.

Siga estos pasos para activar el modo dinámico de VDI:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. En el menú contextual del paquete de instalación del Agente de red, seleccione **Propiedades**.
   Se abrirá la ventana **Propiedades: Agente de red de Kaspersky Security Center**.
3. En la ventana **Propiedades: Agente de red de Kaspersky Security Center**, seleccione la sección **Avanzado**.
4. En la sección **Avanzado**, seleccione la opción **Activar modo dinámico para VDI**.

El dispositivo cliente en el que se va a instalar el Agente de red formará parte de la (VDI).

Búsqueda de dispositivos integrantes de la VDI

Para buscar dispositivos integrantes de la VDI:

1. Seleccione **Buscar** en el menú contextual de la carpeta **Dispositivos no asignados**.
2. En la ventana **Buscar dispositivos**, en la ficha **Máquinas virtuales** en la lista del menú desplegable **Es una máquina virtual**, seleccione **Sí**.
3. Haga clic en el botón **Buscar ahora**.

La aplicación busca dispositivos que formen parte de la infraestructura de escritorio virtual.

Mover dispositivos de la VDI a un grupo de administración

Para mover los dispositivos que forman parte de la VDI a un grupo de administración, haga lo siguiente:

1. En el espacio de trabajo de la carpeta **Dispositivos no asignados**, haga clic en **Configurar reglas**.
   Se abre la ventana de propiedades de la carpeta **Dispositivos no asignados**.
2. En la ventana de propiedades de la carpeta **Dispositivos no asignados**, en la sección **Mover dispositivos**, haga clic en el botón **Agregar**.
   Se abre la ventana **Nueva regla**.
3. En la ventana **Nueva regla**, seleccione la sección **Máquinas virtuales**.
4. En la lista desplegable **Es una máquina virtual**, seleccione **Sí**.

Se creará una regla para la reubicación del dispositivo a un grupo de administración.

Inventario de equipos

La lista de hardware (**Repositorios** → **Hardware**) que utiliza para elaborar un inventario de equipos se rellena de dos maneras: automática o manual. Después de cada sondeo de red, todos los equipos detectados se añaden a la lista automáticamente. Sin embargo, también puede añadir equipos manualmente si no desea sondear la red. Puede añadir manualmente otros dispositivos a la lista, por ejemplo, enrutadores, impresoras o hardware de equipo.

En las propiedades de un dispositivo, puede verse y modificarse la información detallada sobre dicho dispositivo.

La lista de hardware puede incluir los siguientes tipos de dispositivos:

- Equipos
- Dispositivos móviles
- Dispositivos de red
- Dispositivos virtuales
- Componentes de OEM
- Periféricos del equipo
- Dispositivos conectados
- Teléfonos VoIP
- Repositorios de red

El administrador puede asignar el atributo *Equipo de empresa* a los dispositivos detectados. Este atributo se puede asignar manualmente en las propiedades de un dispositivo; asimismo, el administrador puede especificar criterios para que el atributo se asigne automáticamente. En este caso, el atributo *Equipo de empresa* se asigna según el tipo de dispositivo.

Kaspersky Security Center permite excluir dispositivos. Para ello, seleccione la opción **Dispositivo dado de baja** en las propiedades de un dispositivo. El dispositivo no aparece en la lista de dispositivos.

Un administrador puede administrar la lista de controladores lógicos programables (PLC) en la carpeta **Hardware**. En la *Guía del usuario de Kaspersky Industrial CyberSecurity para nodos* encontrará información detallada sobre la administración de la lista de PLC.

Adición de información sobre nuevos dispositivos

Siga estos pasos para agregar información sobre nuevos dispositivos en la red:

1. En la carpeta **Repositorios** del árbol de consola, seleccione la subcarpeta **Hardware**.
2. En el espacio de trabajo de la carpeta **Hardware**, haga clic en el botón **Agregar dispositivo** para abrir la ventana **Nuevo dispositivo**.

   Se abre la ventana **Nuevo dispositivo**.

3. En la ventana **Nuevo dispositivo**, en la lista desplegable **Tipo**, seleccione el tipo de dispositivo que desee agregar.

4. Haga clic en **Aceptar**.

   La ventana de propiedades del dispositivo se abre en la sección **General**.

5. En la sección **General**, complete los campos de entrada con datos del dispositivo. La sección **General** muestra la siguiente configuración:

   - **Dispositivo de empresa**. Elija esta casilla si desea asignar el atributo *Corporativo* al dispositivo. Mediante este atributo, puede buscar los dispositivos en la carpeta **Hardware**.

   - **Dispositivo dado de baja**. Seleccione esta casilla si no desea que el dispositivo aparezca en la lista de dispositivos de la carpeta **Hardware**.

6. Haga clic en **Aplicar**.

El nuevo dispositivo aparece en el espacio de trabajo de la carpeta **Hardware**.

Criterios de configuración empleados para definir los dispositivos de empresas

Siga estos pasos para configurar criterios de detección de dispositivos de empresas:

1. En la carpeta **Repositorios** del árbol de consola, seleccione la subcarpeta **Hardware**.

2. En el espacio de trabajo de la carpeta **Hardware**, haga clic en el botón **Acciones adicionales** y seleccione **Configurar regla para Dispositivos de empresa** en la lista desplegable.

   Se abre la ventana de propiedades del hardware.

3. En la ventana de propiedades del hardware, en la sección **Dispositivos de empresa**, elija un modo de asignación del atributo *Corporativo* al dispositivo:

   - **Configurar el atributo Dispositivo de empresa manualmente para el dispositivo**. El atributo *Hardware corporativo* se asigna manualmente al dispositivo en la ventana de propiedades del dispositivo, en la sección **General**.

   - **Configurar el atributo Dispositivo de empresa automáticamente para el dispositivo**. En el bloque de configuración **Por tipo de dispositivo**, especifique los tipos de dispositivo a los que la aplicación asignará automáticamente el atributo *Corporativo*.

     > Esta opción afecta solo a los dispositivos añadidos a través del sondeo de red. Para los dispositivos añadidos de forma manual, configure el atributo *Empresa* manualmente.

4. Haga clic en **Aceptar**.

Se configuran los criterios de detección para dispositivos empresariales.

Configuración de campos personalizados

Para configurar campos personalizados de dispositivos:

1. En la carpeta **Repositorios** del árbol de consola, seleccione la subcarpeta **Hardware**.
2. En el espacio de trabajo de la carpeta **Hardware**, haga clic en el botón **Acciones adicionales** y seleccione **Configurar campos de datos personalizados** en la lista desplegable.

   Se abre la ventana de propiedades del hardware.
3. En la ventana de propiedades del hardware, seleccione la sección **Campos personalizados** y haga clic en el botón **Agregar**.

   Se abre la ventana **Agregar campo**.
4. En la ventana **Agregar campo**, especifique el nombre del campo personalizado que se mostrará en las propiedades del hardware.

   Puede crear varios campos personalizados con nombres exclusivos.
5. Haga clic en **Aceptar**.

Los campos personalizados que se han agregado se muestran en la sección **Campos personalizados** de las propiedades del hardware. Puede usar campos personalizados para proporcionar información específica sobre los dispositivos. Por ejemplo, el número de referencia interna del pedido de compra del hardware.

Licencias

Esta sección proporciona información acerca de los conceptos generales relacionados con la licencia de Kaspersky Security Center 14.

Eventos de límite de licencias superado

Kaspersky Security Center permite obtener información sobre los eventos que ocurren cuando el Servidor de administración y otras aplicaciones Kaspersky instaladas en dispositivos cliente exceden determinados límites de licencias.

El nivel de importancia de eventos sobre superación de restricciones de licencia se define según las reglas siguientes:

- Si las unidades usadas en un momento dado y cubiertas por una única licencia constituye entre el 90 % y 100 % del número total de unidades cubiertas por dicha licencia, el evento se publica con el nivel de importancia **Información**.
- Si las unidades usadas en un momento dado y cubiertas por una única licencia constituye entre el 100% y 110% del número total de unidades cubiertas por dicha licencia, el evento se publica con el nivel de importancia **Advertencia**.

- Si el número de unidades usadas en un momento dado y cubiertas por una única licencia supera el 110% del número total de unidades cubiertas por la licencia, el evento se publica con el nivel de importancia **Evento crítico**.

Sobre licencias

Esta sección contiene información sobre licencias de aplicaciones de Kaspersky administradas a través de Kaspersky Security Center.

Información acerca de la licencia

Una *licencia* es un derecho de uso de la aplicación durante un tiempo limitado que se concede en las condiciones del Contrato de licencia de usuario final.

Una licencia le da derecho a los siguientes tipos de servicios:

- Uso de la aplicación de acuerdo con las condiciones del Contrato de licencia de usuario final.
- Obtención de soporte técnico.

La cobertura de los servicios y el periodo de validez dependen del tipo de licencia bajo la cual se activó la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *Evaluación*: licencia gratuita para evaluar la aplicación.

  La licencia de evaluación suele tener una duración limitada. Cuando caduque la licencia de prueba, se desactivarán todas las funciones de Kaspersky Security Center. Para continuar usando la aplicación, debe comprar la licencia comercial.

  Solo puede activar una vez la aplicación con una licencia de prueba.

- *Comercial*: licencia de pago concedida con la compra de la aplicación.

  Cuando la licencia comercial expira, la aplicación continúa ejecutándose con una funcionalidad limitada (por ejemplo, las actualizaciones de la base de datos de Kaspersky Security Center no están disponibles). Para continuar usando todas las funciones de Kaspersky Security Center, debe renovar su licencia comercial.

Le recomendamos que renueve la licencia antes de que caduque, a fin de garantizar la máxima protección frente a todas las amenazas de seguridad.

Acerca del Contrato de licencia de usuario final

El Contrato de licencia de usuario final (Contrato de licencia o EULA) es un acuerdo obligatorio entre AO Kaspersky Lab y usted que estipula las condiciones según las cuales puede utilizar la aplicación.

Lea detenidamente el Contrato de licencia antes de comenzar a utilizar la aplicación.

Kaspersky Security Center y sus componentes, por ejemplo, el Agente de red, tienen su propio EULA.

Puede ver las condiciones del Contrato de licencia de usuario final para Kaspersky Security Center utilizando los siguientes métodos:

- Durante la instalación de Kaspersky Security Center.
- Leyendo el documento license.txt incluido en el kit de distribución de Kaspersky Security Center.
- Leyendo el documento license.txt en la carpeta de instalación de Kaspersky Security Center.

Puede ver las condiciones del Contrato de licencia de usuario final para el Agente de red para Windows, el Agente de red para Mac y el Agente de red para Linux utilizando los siguientes métodos:

- Durante la descarga del paquete de distribución del Agente de red desde los servidores web de Kaspersky.
- Durante la instalación del Agente de red para Windows, el Agente de red para Mac y el Agente de red para Linux.
- Al leer el documento license.txt incluido en el paquete de distribución del Agente de red para Windows, el Agente de red para Mac y el Agente de red para Linux.
- Al leer el documento license.txt incluido en la carpeta de instalación del Agente de red para Windows, el Agente de red para Mac y el Agente de red para Linux.

Acepta las condiciones del Contrato de Licencia de Usuario Final si así lo confirma al instalar la aplicación. Si no acepta las condiciones del Contrato de licencia, cancele la instalación de la aplicación y no la utilice.

Sobre el certificado de licencia

El *certificado de licencia* es un documento que recibe junto con un archivo clave o un código de activación.

Un certificado de licencia contiene la siguiente información sobre la licencia proporcionada:

- Clave de licencia o número de pedido.
- Información sobre el usuario al que se le ha concedido la licencia.
- Información sobre la aplicación que se puede activar según la licencia proporcionada.
- Límite del número de unidades de licencia (por ejemplo, los dispositivos en los que se puede utilizar la aplicación según la licencia proporcionada).
- Fecha de inicio de la validez de la licencia.
- Periodo de vigencia o fecha de caducidad de la licencia.
- Tipo de licencia.

Sobre la clave de licencia

La *clave de licencia* es una secuencia de bits que puede usar para activar y utilizar la aplicación de acuerdo con las condiciones del Contrato de licencia de usuario final. Las claves de licencia las generan los especialistas de Kaspersky.

Puede añadir una clave de licencia a la aplicación con uno de los siguientes métodos: aplicando un *archivo clave* o introduciendo un *código de activación*. La clave de licencia se mostrará en la interfaz de la aplicación como una secuencia alfanumérica única cuando la añada a la aplicación.

Kaspersky puede bloquear una clave de licencia si se infringen las condiciones del Contrato de licencia. Si se bloquea una clave de licencia, deberá añadir otra para poder utilizar la aplicación.

Las claves de licencia pueden ser activas o adicionales (o de reserva).

Una *clave de licencia activa* es una clave que actualmente utiliza la aplicación. Se puede añadir una clave de licencia activa para una licencia de prueba o comercial. La aplicación no puede tener más de una clave de licencia activa.

Una *clave de licencia adicional (o de reserva)* es una clave de licencia que da derecho al usuario a usar la aplicación, pero actualmente no está en uso. La clave de licencia adicional se activa automáticamente cuando caduca la licencia asociada a la clave de licencia activa actual. Se puede añadir una clave de licencia adicional solo si se ha agregado ya una clave de licencia activa.

Se puede añadir una clave de licencia para una licencia de prueba como clave de licencia activa. No se puede añadir una clave de licencia para una licencia de prueba como clave de licencia adicional.

Acerca del archivo clave

Un *archivo clave* es un archivo con la extensión .key que Kaspersky le proporciona. Los archivos clave están diseñados para activar la aplicación agregando una clave de licencia.

Recibirá un archivo clave en la dirección de correo electrónico que proporcionó cuando compró Kaspersky Security Center o solicitó la versión de prueba de Kaspersky Security Center.

No es necesario que se conecte a los servidores de activación de Kaspersky para activar la aplicación con un archivo clave.

Puede restaurar un archivo clave si se ha eliminado accidentalmente. Es posible que necesite un archivo clave para registrar una cuenta de Kaspersky CompanyAccount, por ejemplo.

Para restaurar su archivo clave, realice una de las siguientes acciones:

- Contacte con el vendedor de la licencia.
- Obtener un archivo clave a través del sitio web de Kaspersky utilizando su código de activación disponible.

Acerca de la suscripción

Suscripción a Kaspersky Security Center es una solicitud para usar la aplicación con las opciones seleccionadas (fecha de vencimiento de la suscripción, cantidad de dispositivos protegidos). Puede registrar la suscripción a Kaspersky Security Center con su proveedor de servicios (por ejemplo, su proveedor de Internet). La suscripción se puede renovar de forma manual o automática; también se puede cancelar.

Una suscripción puede ser limitada (por ejemplo, de 1 año) o ilimitada (sin fecha de caducidad). Para seguir utilizando Kaspersky Security Center tras la caducidad de una suscripción limitada, debe renovarla. Una suscripción ilimitada se renueva automáticamente si se ha pagado previamente al proveedor de servicios en el plazo de vencimiento.

Cuando caduca una suscripción limitada, se le puede proporcionar un periodo de gracia para la renovación durante el cual la aplicación continúa funcionando. El proveedor de servicios determina la disponibilidad y la duración del periodo de gracia.

Para utilizar Kaspersky Security Center con suscripción, debe aplicar el código de activación facilitado por el proveedor de servicios.

Puede aplicar un código de activación diferente para Kaspersky Security Center solo cuando haya caducado la suscripción o la haya cancelado.

Las acciones posibles en la administración de suscripciones pueden variar en función del proveedor de servicios. Puede suceder que el proveedor de servicios no conceda ningún periodo de gracia para la renovación de la suscripción, con lo cual la aplicación deja de estar operativa.

Los códigos de activación adquiridos mediante suscripción no son válidos para activar versiones anteriores de Kaspersky Security Center.

Al utilizar la aplicación en la modalidad de suscripción, Kaspersky Security Center intenta automáticamente acceder al servidor de activación durante los intervalos de tiempo especificados hasta que caduca la suscripción. Puede renovar la suscripción en el sitio web del proveedor de servicios.

Acerca del código de activación

El *código de activación* es una secuencia única de 20 caracteres alfanuméricos. Introduzca un código de activación para añadir una clave de licencia que active Kaspersky Security Center. Recibirá el código de activación a través de la dirección de correo electrónico que ha especificado después de adquirir Kaspersky Security Center o tras solicitar la versión de prueba de Kaspersky Security Center.

Para activar la aplicación con un código de activación, necesita disponer de acceso a Internet a fin de establecer conexión con los servidores de activación de Kaspersky.

Si la aplicación se activó con un código de activación, en algunos casos envía solicitudes regulares a los servidores de activación de Kaspersky para comprobar el estado actual de la clave de licencia. Es necesario que la aplicación tenga acceso a Internet para que pueda enviar solicitudes.

Si ha perdido su código de activación después de instalar la aplicación, póngase en contacto con el socio de Kaspersky a quien le compró la licencia.

No puede usar archivos clave para activar aplicaciones administradas; solo se aceptan códigos de activación.

Revocación de consentimiento con el Contrato de licencia de usuario final

Si decide detener la protección de sus dispositivos cliente, puede desinstalar las aplicaciones administradas de Kaspersky y revocar su Contrato de licencia de usuario final (EULA) para estas aplicaciones.

Para revocar un EULA para aplicaciones Kaspersky administradas:

1. En el árbol de la consola, seleccione **Servidor de administración → Avanzado → EULA aceptados**.

   Se muestra una lista de EULA, aceptada tras la creación de paquetes de instalación, la instalación sin problemas de actualizaciones o el despliegue de Kaspersky Security for Mobile.

2. En la lista, seleccione el EULA que quiere revocar.

   Puede ver las siguientes propiedades del EULA:

   - Fecha en la que se aceptó el EULA.
   - Nombre del usuario que aceptó el EULA.
   - Enlace a las condiciones del EULA.
   - Lista de los objetos que están conectados al EULA: nombres de paquetes de instalación, nombres de actualizaciones integradas, nombres de aplicaciones móviles.

3. Haga clic en el botón **Revocar EULA**.

   En la ventana que se abre, se le informa que debe desinstalar la aplicación Kaspersky correspondiente al EULA.

4. Haga clic en el botón para confirmar la revocación.

   Kaspersky Security Center verifica que se hayan eliminado los paquetes de instalación (correspondientes a la aplicación administrada de Kaspersky cuyo EULA desea revocar).

   Puede revocar solo el EULA para una aplicación Kaspersky administrada, cuyos paquetes de instalación se eliminarán.

El EULA se ha revocado. No se muestra en la lista de EULA en la sección **Servidor de administración** → **Avanzado** → **EULA aceptados**. No puede proteger los dispositivos cliente utilizando una aplicación de Kaspersky cuyo EULA ha revocado.

Sobre la provisión de datos

Datos transferidos a terceros

Al usar la funcionalidad de administración de dispositivos móviles del Software, con el fin de hacer llegar oportunamente a través del mecanismo de notificación automática los comandos a los dispositivos que ejecutan el sistema operativo Android, se utiliza el servicio de mensajería de nube Google Firebase. Si el Usuario ha configurado el uso del servicio Google Firebase Cloud Messaging, acepta proporcionar la siguiente información al servicio Google Firebase Cloud Messaging en modo automático: Id. de instalación de las aplicaciones de Kaspersky Endpoint Security for Android a las que deben enviarse las notificaciones push.

Para bloquear el intercambio de información con el servicio Google Firebase Cloud Messaging, el usuario debe revertir la configuración de uso del servicio Google Firebase Cloud Messaging.

Al usar la funcionalidad de administración de dispositivos móviles del Software, con el fin de entregar a tiempo los comandos mediante el mecanismo de notificación push a los dispositivos que funcionen con el sistema operativo iOS, se utiliza el servicio Apple Push Notification Service (APN). Si el usuario instaló un certificado de APNs en un servidor de MDM para iOS, creó un perfil de MDM para iOS con una colección de ajustes para la conexión de dispositivos móviles iOS al Software e instaló este perfil de MDM para iOS en dispositivos móviles, el usuario acepta proporcionar la siguiente información a los APNs en modo automático:

- Token: token de inserción del dispositivo. El servidor usa este token cuando envía notificaciones push al dispositivo.
- PushMagic: cadena que debe incluirse en la notificación push. El valor de cadena es generado por el dispositivo.

Datos procesados localmente

Kaspersky Security Center está diseñado para la ejecución centralizada de las tareas básicas de administración y de mantenimiento en la red de una organización. Kaspersky Security Center proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización; Kaspersky Security Center le permite al administrador configurar todos los componentes de protección de las aplicaciones de Kaspersky. Kaspersky Security Center realiza las siguientes funciones principales;

- Detectar dispositivos y sus usuarios en la red de la organización.
- Crear una jerarquía de grupos de administración para la administración de dispositivos.
- Instalar aplicaciones de Kaspersky en dispositivos.
- Administrar la configuración y las tareas de las aplicaciones instaladas.
- Administrar las actualizaciones para Kaspersky y aplicaciones de terceros, y encontrar y corregir vulnerabilidades.
- Activar aplicaciones de Kaspersky en dispositivos.
- Administración de cuentas de usuario.
- Mostrar información sobre el funcionamiento de las aplicaciones de Kaspersky en dispositivos.
- Ver informes.

Para realizar sus principales funciones, Kaspersky Security Center puede recibir, almacenar y procesar la siguiente información:

- Información sobre los dispositivos en la red de la organización recibida como resultado de la detección de dispositivos en la red de Active Directory o en la red de Windows, o mediante el escaneo de intervalos de IP. El Servidor de administración recibe datos de forma independiente o recibe datos del Agente de red.
- Información sobre las unidades organizativas, dominios, usuarios y grupos de Active Directory recibida como resultado de la detección de dispositivos en la red de Active Directory. El Servidor de administración recibe datos de forma independiente o recibe datos del Agente de red.
- Detalles de los dispositivos administrados. Agente de red transfiere los datos que se enumeran a continuación desde el dispositivo hasta el Servidor de administración. El usuario ingresa el nombre para mostrar y la descripción del dispositivo en la interfaz de la Consola de administración o en la interfaz de Kaspersky Security Center 14 Web Console:
  - Especificaciones técnicas del dispositivo administrado y sus componentes necesarios para la identificación del dispositivo: nombre y descripción para mostrar del dispositivo, nombre y tipo de dominio de Windows, nombre del dispositivo en el entorno de Windows, dominio DNS y nombre DNS, dirección IPv4, dirección IPv6, ubicación de red, dirección MAC, tipo de sistema operativo, si el dispositivo es una máquina virtual junto con el tipo de hipervisor y si el dispositivo es una máquina virtual dinámica como parte de VDI.
  - Otras especificaciones de los dispositivos administrados y sus componentes necesarios para la auditoría de los dispositivos administrados y para tomar decisiones sobre la aplicación de parches y actualizaciones específicas: estado del Agente de Windows Update (WUA), arquitectura del sistema operativo, proveedor del sistema operativo, número de compilación del sistema operativo, id. de versión del sistema operativo, carpeta de ubicación del sistema operativo, si el dispositivo es una máquina virtual: el tipo de máquina virtual; el nombre del Servidor de administración virtual que administra el dispositivo; datos del dispositivo en la nube (región de la nube, VPC, zona de disponibilidad de la nube, subred de la nube, zona de disponibilidad de la nube).

- Detalles de acciones en dispositivos administrados: fecha y hora de la última actualización; hora a la que el dispositivo estuvo visible por última vez en la red; estado de espera de reinicio, hora a la que se encendió el dispositivo.

- Detalles de cuentas de usuario del dispositivo y sus sesiones.

- Estadísticas de operación del punto de distribución, si el dispositivo es un punto de distribución. Agente de red transfiere los datos del dispositivo al Servidor de administración.

- Configuración del punto de distribución ingresada por el usuario en la Consola de administración o en Kaspersky Security Center 14 Web Console.

- Datos necesarios para la conexión de los dispositivos móviles con el Servidor de administración: certificado, puerto de conexión móvil, dirección de conexión del Servidor de administración. El usuario ingresa los datos en la Consola de administración o en Kaspersky Security Center 14 Web Console.

- Información de los dispositivos móviles transferidos mediante el protocolo Exchange ActiveSync. Los datos enumerados a continuación se transfieren desde el dispositivo móvil al Servidor de administración:

  - Especificaciones técnicas del dispositivo móvil y sus componentes necesarios para la identificación del dispositivo: nombre del dispositivo, modelo, nombre del sistema operativo, IMEI y número de teléfono.

  - Especificaciones del dispositivo móvil y sus componentes: estado de administración del dispositivo, soporte de SMS, permiso para enviar mensajes SMS, soporte de FCM, soporte de comandos de usuario, carpeta de almacenamiento del sistema operativo y nombre del dispositivo.

  - Detalles de las actividades de los dispositivos móviles: ubicación del dispositivo (a través del comando Localizar), hora de la última sincronización, hora de la última conexión al Servidor de administración y detalles de soporte de sincronización.

- Información de los dispositivos móviles transferidos mediante el protocolo MDM de iOS. Los datos enumerados a continuación se transfieren desde el dispositivo móvil al Servidor de administración:

  - Especificaciones técnicas del dispositivo móvil y sus componentes necesarios para la identificación del dispositivo: nombre del dispositivo, modelo, nombre del sistema operativo y número de compilación, número de modelo del dispositivo, número IMEI, UDID, MEID, número de serie, cantidad de memoria, versión de firmware del módem, dirección MAC de Bluetooth, dirección MAC de Wi-Fi y detalles de la tarjeta SIM (ICCID como parte del Id. de la tarjeta SIM).

  - Información de la red móvil utilizada por el dispositivo administrado: tipo de red móvil, nombre de la red móvil utilizada actualmente, nombre de la red móvil doméstica, versión de la configuración del operador de la red móvil, estado de roaming de voz, estado de roaming de datos, código de país del red doméstica, código de país de residencia, código de país de la red utilizada actualmente y nivel de cifrado.

  - Configuración de seguridad del dispositivo móvil: uso de una contraseña y su conformidad con la configuración de directivas, lista de perfiles de configuración y perfiles de aprovisionamiento utilizados para la instalación de aplicaciones de terceros.

  - Fecha de la última sincronización con el Servidor de administración y el estado de administración del dispositivo.

- Detalles de las aplicaciones de Kaspersky instaladas en el dispositivo. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red:

  - Configuración de las aplicaciones de Kaspersky instaladas en el dispositivo administrado: nombre y versión de la aplicación de Kaspersky, estado, estado de protección en tiempo real, fecha y hora del último análisis del dispositivo, número de amenazas detectadas, número de objetos que no se desinfectaron, disponibilidad y estado del componentes de la aplicación, hora de la última actualización y versión de las bases de datos

antivirus, detalles de las configuraciones y tareas de la aplicación Kaspersky, información sobre las claves de licencia activas y de reserva, fecha de instalación de la aplicación e Id.

- Estadísticas de operación de la aplicación: eventos relacionados con cambios en el estado de los componentes de la aplicación Kaspersky del dispositivo administrado y el desempeño de las tareas iniciadas por los componentes de la aplicación.
- Estado del dispositivo definido por la aplicación Kaspersky.
- Etiquetas asignadas por la aplicación Kaspersky.
- Conjunto de actualizaciones instaladas y aplicables para la aplicación Kaspersky.

- Datos contenidos en los eventos de los componentes de Kaspersky Security Center y las aplicaciones de Kaspersky administradas. Agente de red transfiere los datos del dispositivo al Servidor de administración.
- Datos necesarios para la integración de Kaspersky Security Center con un sistema SIEM para la exportación de eventos. El usuario ingresa los datos en la Consola de administración o en Kaspersky Security Center 14 Web Console.
- Configuración de los componentes de Kaspersky Security Center y las aplicaciones administradas de Kaspersky presentes en las directivas y los perfiles de las directivas. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.
- Configuración de tarea de los componentes de Kaspersky Security Center y las aplicaciones administradas de Kaspersky. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.
- Datos tratados por la función Administración de vulnerabilidades y parches. Agente de red transfiere los datos que se enumeran a continuación desde el dispositivo hasta el Servidor de administración:
  - Detalles de las aplicaciones y los parches instalados en los dispositivos administrados (Registro de aplicaciones).
  - Información sobre el hardware detectado en dispositivos administrados (registro de hardware).
  - Detalles de vulnerabilidades en software de terceros detectados en dispositivos administrados.
  - Detalles de las actualizaciones disponibles para aplicaciones de terceros instaladas en dispositivos administrados.
  - Detalles de las actualizaciones de Microsoft encontradas por la función WSUS.
  - Lista de actualizaciones de Microsoft encontradas por la función WSUS que deben instalarse en el dispositivo.
- Datos necesarios para descargar actualizaciones en el Servidor de administración aislado para reparar vulnerabilidades de software de terceros en dispositivos administrados. El Usuario ingresa y transmite datos mediante la utilidad klscflag del Servidor de administración.
- Datos necesarios para el trabajo de Kaspersky Security Center con los entornos de nube (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). El usuario ingresa los datos en la Consola de administración o en Kaspersky Security Center 14 Web Console.
- Categorías de usuario de aplicaciones. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Detalles de los archivos ejecutables detectados en dispositivos administrados por la función Control de aplicaciones. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Detalles de los archivos colocados en la Copia de seguridad. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Detalles de los archivos colocados en cuarentena. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Detalles de los archivos solicitados por los especialistas de Kaspersky para un análisis detallado. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Detalles del estado y la activación de las reglas de control de anomalías adaptativo. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Detalles de dispositivos externos (unidades de memoria, herramientas de transferencia de información, herramientas de copia impresa de información y buses de conexión) instalados o conectados al dispositivo administrado y detectados por la función Control de dispositivos. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Información sobre dispositivos cifrados y el estado del cifrado. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red.

- Detalles de los errores de cifrado de datos en dispositivos realizados con la función de cifrado de datos de las aplicaciones de Kaspersky. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Lista de controladores lógicos programables administrados (PLC). La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Datos necesarios para la creación de una cadena de desarrollo de amenazas. La aplicación administrada transfiere datos desde el dispositivo al Servidor de administración a través de Agente de red. Se proporciona una lista completa de datos en los archivos de Ayuda de la aplicación correspondiente.

- Datos necesarios para la integración de Kaspersky Security Center con el servicio Kaspersky Managed Detection and Response (el complemento dedicado debe estar instalado para Kaspersky Security Center 14 Web Console): token de inicio de integración, token de integración y token de sesión de usuario. El Usuario ingresa el token de inicio de integración en la interfaz de Kaspersky Security Center 14 Web Console. El servicio Kaspersky MDR transfiere el token de integración y el token de sesión del usuario a través del complemento dedicado.

- Detalles de los códigos de activación ingresados o archivos de clave especificados. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Cuentas de usuario: nombre, descripción, nombre completo, dirección de correo electrónico, número de teléfono principal, contraseña, clave secreta generada por el Servidor de administración y contraseña de un solo uso para la verificación en dos pasos. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Datos que Identity and Access Manager necesita para la autenticación centralizada y para proporcionar un inicio de sesión único (Single Sign-on, SSO) entre las aplicaciones de Kaspersky integradas con Kaspersky Security Center: parámetros de instalación y configuración de Identity and Access Manager, sesión de usuario de Identity and Access Manager, tokens de Identity and Access Manager, estados de la aplicación cliente y estados del servidor de recursos. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Historial de revisión de objetos de administración. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Registro de objetos de administración eliminados. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Paquetes de instalación creados a partir del archivo, así como configuración de instalación. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Datos necesarios para mostrar los anuncios de Kaspersky en Kaspersky Security Center 14 Web Console. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Datos necesarios para el funcionamiento de los complementos de aplicaciones administradas en Kaspersky Security Center 14 Web Console y guardados por los complementos en la base de datos del Servidor de administración durante su operación de rutina. La descripción y las formas de proporcionar los datos se proporcionan en los archivos de Ayuda de la aplicación correspondiente.

- Configuración de usuario de Kaspersky Security Center 14 Web Console: idioma de localización y tema de la interfaz, configuración de visualización del panel de monitoreo, información sobre el estado de las notificaciones (Leídas/No leídas), estado de las columnas en las hojas de cálculo (Mostrar/Ocultar), progreso del modo Formación. El Usuario ingresa los datos en la interfaz de Kaspersky Security Center 14 Web Console.

- Componentes de Registro de eventos de Kaspersky for Kaspersky Security Center y aplicaciones administradas de Kaspersky. El Registro de eventos de Kaspersky se almacena en cada dispositivo y no se transfieren nunca al Servidor de administración.

- Certificados para la conexión segura con dispositivos administrados para los componentes de Kaspersky Security Center. El Usuario ingresa los datos en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

- Datos necesarios para el funcionamiento de Kaspersky Security Center en entornos de nube, como Amazon Web Services (AWS), Microsoft Azure, Google Cloud y Yandex.Cloud. El Servidor de administración recibe los datos de la máquina virtual en la que se ejecuta.

- Información sobre la aceptación por parte del Usuario de los términos y condiciones de los acuerdos legales con Kaspersky.

- Los datos del Servidor de Administración que el Usuario ingresa en los siguientes componentes:

  - Consola de administración

  - Kaspersky Security Center 14 Web Console

  - Terminal de línea de comandos cuando se usa la utilidad klscflag

  - Componentes que interactúan con el Servidor de administración a través de objetos de automatización klakaut y Kaspersky Security Center OpenAPI

- Cualquier dato que el Usuario ingrese en la interfaz de Consola de administración o Kaspersky Security Center 14 Web Console.

Los datos enumerados anteriormente pueden estar presentes en Kaspersky Security Center si se aplica uno de los siguientes métodos:

- El Usuario ingresa datos en la interfaz de los siguientes componentes:
  - Consola de administración
  - Kaspersky Security Center 14 Web Console
  - Terminal de línea de comandos cuando se usa la utilidad klscflag
  - Componentes que interactúan con el Servidor de administración a través de objetos de automatización klakaut y Kaspersky Security Center OpenAPI
- El Agente de red recibe los datos automáticamente desde el dispositivo y los transfiere al Servidor de administración.
- El Agente de red recibe los datos recuperados mediante la aplicación de Kaspersky administrada y los transfiere al Servidor de administración. Las listas de datos que procesan las aplicaciones de Kaspersky administradas se proporciona en los archivos de Ayuda de las aplicaciones correspondientes.
- El Servidor de administración y el Agente de red asignados a un punto de distribución recibe información sobre los dispositivos en red.
- Los datos se transfieren desde el dispositivo móvil al Servidor de administración utilizando el protocolo Exchange ActiveSync o MDM de iOS.

Los datos enumerados se almacenan en la base de datos del Servidor de administración. Los nombres de usuario y contraseñas se almacenan en forma cifrada.

Todos los datos arriba enumerados solo pueden transferirse a Kaspersky a través de archivos de volcado, archivos de seguimiento o archivos de registro de componentes de Kaspersky Security Center, entre ellos archivos de registro creados por instaladores y utilidades.

Los archivos de volcado, los archivos de seguimiento y los archivos de registro de los componentes de Kaspersky Security Center contienen datos aleatorios del Servidor de administración, Agente de red, Consola de administración, Servidor de MDM para iOS, Servidor de dispositivos móviles de Exchange y Kaspersky Security Center 14 Web Console. Estos archivos pueden contener datos personales y confidenciales. Los archivos de volcado, los archivos de seguimiento y los archivos de registro se almacenan en el dispositivo de forma no cifrada. Los archivos de volcado, los archivos de seguimiento y los archivos de registro no se transfieren automáticamente a Kaspersky; sin embargo, el administrador puede transferir datos a Kaspersky manualmente si así lo solicita el Servicio de soporte técnico para resolver problemas de funcionamiento de Kaspersky Security Center.

Al seguir los enlaces de la Consola de administración o de Kaspersky Security Center 14 Web Console, el usuario acepta la transferencia automática de los siguientes datos:

- Código de Kaspersky Security Center.
- Versión de Kaspersky Security Center.
- Localización de Kaspersky Security Center.
- Id. de licencia.
- Tipo de licencia.

- Si la licencia se compró a través de un socio.

La lista de datos proporcionada a través de cada enlace depende de la finalidad y la ubicación de este.

Kaspersky utiliza cualquier información recibida de forma anónima y solo como estadísticas generales. Las estadísticas resumidas se generan automáticamente a partir de la información recibida originalmente y no contienen ningún dato personal o confidencial. Tan pronto como se acumulan nuevos datos, los datos anteriores se borran (una vez al año). Los resúmenes de estadísticas se almacenan indefinidamente.

Kaspersky protege cualquier información recibida de acuerdo con la ley y las reglas aplicables de Kaspersky. Los datos se transmiten a través de un canal seguro.

Opciones de licencias de Kaspersky Security Center

En Kaspersky Security Center, la licencia se puede aplicar a diferentes grupos de funcionalidad.

Al añadir una clave de licencia en la ventana de propiedades del Servidor de administración, asegúrese de añadir una clave de licencia que le permita usar Kaspersky Security Center. Puede encontrar esta información en el sitio web de Kaspersky. La página web de cada solución contiene la lista de aplicaciones incluidas en la solución. El Servidor de administración puede aceptar claves de licencia no compatibles, por ejemplo, una clave de licencia para Kaspersky Endpoint Security Cloud, pero en tales casos será incompatible con la funcionalidad de Kaspersky Security Center.

Funcionalidad básica de la Consola de administración

Las siguientes funciones están disponibles:

- Creación de Servidores de administración virtuales para administrar una red de oficinas remotas u organizaciones cliente.
- Creación de una jerarquía de grupos de administración para administrar dispositivos específicos como un conjunto.
- Control del estado de la seguridad antivirus de una organización.
- Instalación remota de aplicaciones.
- Visualización de la lista de imágenes de sistema operativo disponibles para la instalación remota.
- Configuración centralizada de aplicaciones instaladas en dispositivos cliente.
- Visualización y modificación de grupos de aplicaciones con licencia existentes.
- Estadísticas e informes sobre el funcionamiento de la aplicación, así como notificaciones sobre eventos críticos.
- Administración de Protección y cifrado de datos.
- Visualización y edición manual de la lista de componentes de hardware que detectó el sondeo de la red.
- Operaciones centralizadas con archivos que se movieron a la cuarentena o copia de seguridad y archivos cuyo procesamiento se ha pospuesto.
- Administración de funciones de usuario.

Kaspersky Security Center con la funcionalidad básica de la Consola de administración se proporciona como parte de las aplicaciones de Kaspersky para la protección de redes corporativas. También se puede descargar desde el sitio web de Kaspersky.

Antes de que la aplicación se active o después de que caduque la licencia comercial, Kaspersky Security Center proporciona únicamente la funcionalidad básica de la Consola de administración.

Función Administración de vulnerabilidades y parches

Las siguientes funciones están disponibles:

- Instalación remota de sistemas operativos.
- Instalación remota de actualizaciones de software, análisis y reparación de vulnerabilidades.
- Inventario de hardware.
- Administración del grupo de aplicaciones con licencia.
- Permiso remoto de conexión a dispositivos cliente a través de un componente de Microsoft® Windows® llamado Conexión a escritorio remoto.
- Conexión remota con dispositivos cliente mediante la opción de Uso compartido del escritorio de Windows.

La unidad de administración de la Administración de vulnerabilidades y parches es un dispositivo cliente en el grupo Dispositivos administrados.

Como parte de las funcionalidades de Administración de vulnerabilidades y parches, durante el proceso de creación de inventarios está disponible información más detallada sobre el hardware de los dispositivos. Para garantizar el funcionamiento correcto de Administración de vulnerabilidades y parches, debe haber al menos 100 GB de espacio libre en disco disponible.

Función de Administración de dispositivos móviles

La función Administración de dispositivos móviles se usa para administrar Exchange ActiveSync (EAS) y Dispositivos móviles con MDM de iOS.

Las siguientes funciones están disponibles para dispositivos móviles de Exchange ActiveSync:

- Creación y edición de perfiles de administración de dispositivos móviles, asignación de perfiles a los buzones de correo de los usuarios.
- Configuración de dispositivos móviles (sincronización del correo electrónico, uso de las aplicaciones, contraseñas de usuarios, cifrado de datos y conexión de unidades extraíbles).
- Instalación de certificados en dispositivos móviles.

Las siguientes funciones están disponibles para los dispositivos iOS con MDM:

- Creación y edición de perfiles de configuración, e instalación de perfiles de configuración en dispositivos móviles.

- Instalación de aplicaciones en dispositivos móviles mediante App Store® o el uso de archivos de manifiesto (.plist).
- Bloqueo de dispositivos móviles, restablecimiento de la contraseña del dispositivo móvil y eliminación de todos los datos del dispositivo móvil.

Además, la administración de dispositivos móviles permite ejecutar comandos proporcionados por los protocolos correspondientes.

La unidad de administración de la Administración de dispositivos móviles es un dispositivo móvil. Un dispositivo móvil se considera administrado, después de conectarlo al Servidor de dispositivos móviles.

Control de acceso basado en funciones

Kaspersky Security Center proporciona recursos para el acceso basado en funciones a las funciones de Kaspersky Security Center o las aplicaciones administradas de Kaspersky.

Puede configurar los derechos de acceso de los usuarios de Kaspersky Security Center a las funciones de la aplicación de una de las siguientes formas:

- Mediante la configuración por separado de los derechos de cada usuario o grupo de usuarios.
- Mediante la creación de funciones de usuario estándar con un conjunto de derechos preestablecido y la asignación de esas funciones a los usuarios según su ámbito de responsabilidad.

Instalación de sistemas operativos y aplicaciones

Kaspersky Security Center permite crear imágenes de los sistemas operativos y desplegarlas en los dispositivos cliente de la red, como también permite realizar la instalación remota de las aplicaciones de Kaspersky y de otros proveedores. Puede capturar imágenes de sistemas operativos de los dispositivos y transferirlas al Servidor de administración. Estas imágenes de sistemas operativos se almacenan en el Servidor de administración en una carpeta exclusiva. La imagen del sistema operativo de un dispositivo de referencia se captura y luego se crea a través de una tarea de creación de paquete de instalación. Puede usar las imágenes recibidas para desplegarlas en los nuevos dispositivos de red en los que aún no se ha instalado ningún sistema operativo. En este caso, se usa una tecnología denominada Entorno de ejecución de prearranque (PXE).

Integración con entornos de nube

Kaspersky Security Center no solo funciona con dispositivos locales, sino que también proporciona características especiales para trabajar en un entorno de nube, como el Asistente de configuración del entorno de nube. Kaspersky Security Center funciona con las siguientes máquinas virtuales:

- Instancias de Amazon EC2
- Máquinas virtuales de Microsoft Azure
- Instancias de máquinas virtuales de Google Cloud

Exportación de eventos a sistemas SIEM: QRadar de IBM y ArcSight de Micro Focus

La exportación de eventos se puede utilizar en sistemas centralizados que tratan con problemas de seguridad a un nivel organizativo y técnico, proporcionan servicios de supervisión de la seguridad y unifican la información de soluciones diferentes. Estos son sistemas de SIEM, que proporcionan análisis en tiempo real de alertas de seguridad y eventos generados por el hardware de la red y las aplicaciones o Centros operativos de seguridad (SOCs).

Con una licencia especial, puede utilizar los protocolos CEF y LEEF para exportar eventos generales a los sistemas SIEM, como así también eventos que las aplicaciones de Kaspersky transfieren al Servidor de administración.

LEEF (Log Event Extended Format) es un formato de evento personalizado para IBM Security QRadar SIEM. QRadar puede integrar, identificar y procesar eventos LEEF. Los eventos LEEF deben usar la codificación de caracteres UTF-8. Puede encontrar información detallada sobre el protocolo LEEF en IBM Knowledge Center.

CEF (Common Event Format) es un estándar abierto de administración de registros que mejora el interoperabilidad de la información relacionada con la seguridad desde diferentes dispositivos y aplicaciones de seguridad y red. CEF le permite usar un formato de registros de eventos común de modo que los datos se puedan integrar y añadir fácilmente para que un sistema de administración de la empresa los analice. Los sistemas ArcSight y Splunk SIEM utilizan este protocolo.

Acerca de las restricciones de las funciones principales

Antes de que la aplicación se active o después de que caduque la licencia comercial, Kaspersky Security Center proporciona únicamente la funcionalidad básica de la Consola de administración. Las limitaciones de este funcionamiento básico de la aplicación se describen a continuación.

Administración de dispositivos móviles

No se puede crear un perfil nuevo y asignarlo a un dispositivo móvil (MDM de iOS) o a un buzón de correo (Exchange ActiveSync). Es posible modificar en cualquier momento los perfiles existentes y asignar perfiles a buzones de correo.

Administración de aplicaciones

No puede ejecutar la tarea de instalación de actualizaciones y la tarea de extracción de actualizaciones. Se completarán todas las tareas iniciadas antes de que caduque la licencia, pero no se instalarán las últimas actualizaciones. Por ejemplo, si la tarea de instalación de actualizaciones crítica se inició antes de caducar la licencia, solo se instalarán las actualizaciones críticas encontradas antes de que caducara la licencia.

Dispone en todo momento del inicio y la edición de la sincronización, el análisis de vulnerabilidades y las tareas de actualización de las bases de datos de vulnerabilidades. Además, no existen limitaciones de visualización, búsqueda ni clasificación de entradas en la lista de vulnerabilidades y actualizaciones.

Instalación remota de sistemas operativos y aplicaciones

No se pueden ejecutar tareas para capturar e instalar una imagen del sistema operativo. Se completarán las tareas iniciadas antes de caducar la licencia.

Inventario de hardware

No se puede recuperar información sobre nuevos dispositivos mediante el Servidor de dispositivos móviles. Se mantiene actualizada la información sobre dispositivos conectados.

No se envían notificaciones sobre cambios en la configuración de dispositivos.

La lista de equipos está disponible para su visualización y edición manual.

Administración del grupo de aplicaciones con licencia

No puede añadir una clave de licencia nueva.

No se envían notificaciones sobre infracciones de restricciones de uso de claves de licencia.

Conexión remota con dispositivos cliente

La conexión remota con dispositivos cliente no está disponible.

Seguridad Antivirus

El Antivirus usa bases de datos que se han instalado antes de que caduque la licencia.

Integración con entornos de nube

Al trabajar en un entorno de nube, no puede usar las herramientas de la API de AWS, Azure, o Google para el sondeo de segmentos de la nube y la instalación de aplicaciones en dispositivos. Tampoco hay disponibles elementos de interfaz que muestren funciones específicas para trabajar en un entorno de nube.

Funciones de obtención de licencias de Kaspersky Security Center y aplicaciones administradas

Tenga en cuenta las siguientes indicaciones relativas a las licencias del Servidor de administración y las aplicaciones administradas:

- Puede añadir una clave de licencia o un código de activación válido a un Servidor de administración para activar la administración de vulnerabilidades y parches, la administración de dispositivos móviles o la integración con los sistemas SIEM. Algunas funciones de Kaspersky Security Center solo son accesibles dependiendo de los archivos de claves activos o los códigos de activación válidos añadidos al Servidor de administración.

- Puede añadir varias archivos clave y códigos de activación para aplicaciones administradas al repositorio del Servidor de administración.

Acerca de la obtención de licencias de Kaspersky Security Center

Si ha activado una de las funciones de la licencia (por, ejemplo, la Administración de dispositivos móviles) con un archivo clave pero también desea usar función de la licencia (por ejemplo, la Administración de vulnerabilidades y parches), debe comprarle a su proveedor de servicios una archivo clave que active ambas funciones y debe activar el Servidor de administración con esta archivo clave.

Funciones de obtención de licencias de aplicaciones administradas

Para obtener las licencias de las aplicaciones administradas, puede instalar automáticamente (o de cualquier forma que le resulte cómoda) una archivo clave o un código de activación. Puede usar los siguientes métodos para desplegar un código de activación o archivo clave:

- Despliegue automático

  Si usa diferentes aplicaciones administradas y tiene que desplegar un archivo clave o un código de activación específicos en los dispositivos, opte por otras formas de desplegar ese código de activación o archivo clave.

  Kaspersky Security Center le permite desplegar automáticamente las claves de licencia disponibles en los dispositivos. Por ejemplo, en el repositorio del Servidor de administración se almacenan tres claves de licencia. Ha seleccionado la casilla de verificación **Distribuir automáticamente la clave de licencia a los dispositivos administrados** para las tres claves de licencia. En los dispositivos de la organización se ha instalado una aplicación de seguridad de Kaspersky, por ejemplo, Kaspersky Endpoint Security para Windows. Se detecta un nuevo dispositivo en el que se debe desplegar una clave de licencia. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden aplicar al dispositivo: la clave de licencia llamada *Clave_1* y la clave de licencia llamada *Clave_2*. Una de estas claves de licencia se despliega en el dispositivo. En este caso, no se puede predecir cuál de las dos claves de licencia se instalará en el dispositivo porque el despliegue automático de claves de licencia no prevé ninguna actividad de administrador.

  Cuando se despliega una clave de licencia, los dispositivos se vuelven a contar para esa clave de licencia. Debe asegurarse de que la cantidad de dispositivos en los que se desplegó la clave de licencia no exceda el límite de la licencia. Si la cantidad de dispositivos excede el límite de la licencia, se asignará a todos los dispositivos que no estaban cubiertos por la licencia el estado *Crítico*.

- Adición de un archivo clave o un código de activación al paquete de instalación de una aplicación administrada

  Si instala una aplicación administrada con un paquete de instalación, puede especificar un código de activación o un archivo clave en este paquete de instalación o en la directiva de la aplicación. La clave de licencia se desplegará en los dispositivos administrados en la próxima sincronización del dispositivo con el Servidor de administración.

- Despliegue al ejecutar la tarea de añadir clave de licencia a una aplicación administrada

  Si opta por usar la tarea Agregar clave de licencia a una aplicación administrada, puede seleccionar la clave de licencia que debe instalarse en los dispositivos y seleccionar los dispositivos con comodidad, por ejemplo, seleccionando un grupo de administración o una selección de dispositivos.

- Adición de un código de activación o un archivo clave manualmente a los dispositivos

Aplicaciones de Kaspersky. Despliegue centralizado

Esta sección describe los métodos para la instalación remota de las aplicaciones de Kaspersky y su eliminación desde dispositivos conectados a una red.

Antes de desplegar aplicaciones en dispositivos cliente, asegúrese de que el hardware y el software de los dispositivos cliente cumplen los requisitos aplicables.

El Agente de red es un componente que permite la conexión del Servidor de administración con dispositivos cliente. Por lo tanto, debe estar instalado en cada dispositivo cliente, que se debe conectar al sistema de control centralizado remoto. El dispositivo con el Servidor de administración instalado solo puede usar la versión de servidor del Agente de red. Esta versión se incluye en el Servidor de administración como componente que se instala y se elimina junto con el servidor. No es necesario instalar el Agente de red en ese dispositivo.

El Agente de red se puede instalar remota o localmente como cualquier aplicación. Durante el despliegue centralizado de las aplicaciones de seguridad a través de la Consola de administración, puede instalar el Agente de red junto con aplicaciones de seguridad.

Los Agentes de red pueden ser diferentes según las aplicaciones de Kaspersky con las que trabajan. En algunos casos, el Agente de red solo se puede instalar localmente (para obtener detalles, consulte la documentación de las aplicaciones correspondientes). Solo tiene que instalar el Agente de red en un dispositivo cliente una vez.

Las aplicaciones de Kaspersky se administran a través de la Consola de administración usando complementos de administración. Por lo tanto, para obtener acceso a la interfaz de administración de aplicaciones a través de Kaspersky Security Center, se debe instalar el complemento de administración correspondiente en la estación de trabajo del administrador.

Puede realizar la instalación remota de aplicaciones desde la estación de trabajo del administrador en la ventana principal de Kaspersky Security Center.

Para instalar software de forma remota, debe crear una tarea de instalación remota.

La tarea creada para la instalación remota se iniciará de acuerdo con su planificación. Puede interrumpir el procedimiento de instalación deteniendo la tarea manualmente.

Si la instalación remota de una aplicación devuelve un error, puede encontrar la causa de este error y solucionarlo usando la herramienta de preparación de instalación remota.

Puede supervisar el progreso de la instalación remota de las aplicaciones Kaspersky en una red con el informe de despliegue.

Para obtener detalles sobre la administración de las aplicaciones mencionadas en Kaspersky Security Center, consulte la documentación de las aplicaciones correspondientes.

Sustitución de aplicaciones de seguridad de terceros

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center puede requerir la eliminación del software de terceros incompatible con la aplicación instalada. Kaspersky Security Center proporciona varias formas de eliminar las aplicaciones de terceros.

Eliminar aplicaciones incompatibles utilizando el instalador

Esta opción está disponible solo en la Consola de administración basada en la Consola de administración de Microsoft.

El método del programa de instalación de eliminar aplicaciones incompatibles es compatible con varios tipos de instalación. Antes de instalar la aplicación de seguridad, todas las aplicaciones incompatibles se eliminan automáticamente si la ventana de propiedades del paquete de instalación de esta aplicación de seguridad (sección **Aplicaciones incompatibles**) tiene la opción **Desinstalar automáticamente las aplicaciones incompatibles** seleccionada.

Eliminar aplicaciones incompatibles al configurar la instalación remota de una aplicación

Puede habilitar la opción **Desinstalar automáticamente las aplicaciones incompatibles** al configurar la instalación remota de una aplicación de seguridad. En la Consola de administración basada en la Consola de administración de Microsoft (MMC), esta opción está disponible en el Asistente de instalación remota. En Kaspersky Security Center 14 Web Console, puede encontrar esta opción en el Asistente de despliegue de la protección. Cuando esta opción se activa, Kaspersky Security Center elimina la aplicación incompatible antes de instalar una aplicación de seguridad en un dispositivo administrado.

Instrucciones:

- Consola de administración: Instalación de aplicaciones con el Asistente de Instalación Remota
- Kaspersky Security Center 14 Web Console: Eliminación de aplicaciones incompatibles antes de la instalación

Eliminación de aplicaciones incompatibles mediante una tarea dedicada

Para eliminar las aplicaciones incompatibles, use la tarea **Desinstalar aplicación en remoto**. Esta tarea debería ejecutarse en dispositivos antes de la tarea de instalación de la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar el tipo de la programación **Al completar otra tarea**, donde la otra tarea es **Desinstalar aplicación en remoto**.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

Instrucciones de la Consola de administración: Crear una tarea.

Instalación de aplicaciones con una tarea de instalación remota

Kaspersky Security Center permite instalar aplicaciones en dispositivos remotamente con tareas de instalación remota. Esas tareas se crean y se asignan a dispositivos a través de un Asistente dedicado. Para asignar una tarea a dispositivos de modo más fácil y rápido, puede especificar dispositivos en la ventana del Asistente de una de estas formas:

- **Seleccionar dispositivos de red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración así como dispositivos no asignados.
- **Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista**. Puede especificar nombres NetBIOS, nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.
- **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizado que haya creado.

- **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a dispositivos incluidos en un grupo de administración creado anteriormente.

Para realizar la instalación remota en un dispositivo en el que no se ha instalado el Agente de red, se deben abrir los siguientes puertos: (a) TCP 139 y 445; (b) UDP 137 y 138. De forma predeterminada, se abren los puertos en todos los dispositivos incluidos en el dominio. Se abren automáticamente mediante la utilidad de preparación de instalación remota.

Instalar la aplicación en los dispositivos seleccionados

Para instalar una aplicación en dispositivos seleccionados:

1. Establezca una conexión con el Servidor de administración que controla los dispositivos correspondientes.
2. En el árbol de consola, seleccione la carpeta **Tareas**.
3. Ejecute la creación de tarea al hacer clic en el botón **Crear una tarea**.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

   En la ventana **Seleccionar el tipo de tarea** del Asistente para añadir tareas, en el nodo **Servidor de administración de Kaspersky Security Center 14**, seleccione **Instalar aplicación de forma remota** como tipo de tarea.

   El Asistente para añadir tareas crea una tarea de instalación remota de la aplicación seleccionada en dispositivos específicos. La tarea recién creada se muestra en el espacio de trabajo de la carpeta **Tareas**.
4. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la planificación especificada en los parámetros de la tarea.

Al finalizar la tarea de instalación remota, se instalará la aplicación seleccionada en los dispositivos seleccionados.

Instalación de una aplicación en dispositivos cliente de un grupo de administración

Para instalar una aplicación en dispositivos cliente de un grupo de administración:

1. Establezca una conexión con el Servidor de administración que controla el grupo de administración correspondiente.
2. Seleccione un grupo de administración en el árbol de consola.
3. En el espacio de trabajo del grupo, seleccione la ficha **Tareas**.
4. Ejecute la creación de tarea al hacer clic en el botón **Crear una tarea**.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

   En la ventana **Seleccionar el tipo de tarea** del Asistente para añadir tareas, en el nodo **Servidor de administración de Kaspersky Security Center 14**, seleccione **Instalar aplicación de forma remota** como tipo de tarea.

   El Asistente para añadir tareas crea una tarea de grupo de instalación remota de la aplicación seleccionada. La nueva tarea aparece en el espacio de trabajo del grupo de administración, en la ficha **Tareas**.

5. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la planificación especificada en los parámetros de la tarea.

Al finalizar la tarea de instalación remota, se instalará la aplicación seleccionada en los dispositivos cliente del grupo de administración.

Instalación de una aplicación mediante directivas de grupo de Active Directory

Kaspersky Security Center permite usar directivas de grupo de Active Directory para instalar aplicaciones Kaspersky en dispositivos administrados.

Puede instalar aplicaciones mediante directivas de grupo de Active Directory solo desde los paquetes de instalación que incluyan el Agente de red.

Para instalar una aplicación mediante directivas de grupo de Active Directory:

1. Comience a configurar la instalación de la aplicación mediante el Asistente de instalación remota.
2. En la ventana **Definir la configuración de la tarea de instalación remota** del Asistente de instalación remota, seleccione la opción **Asignar instalación del paquete en las directivas de grupo de Active Directory**.
3. En la ventana **Seleccionar cuentas para acceder a los dispositivos** del Asistente de instalación remota, seleccione la opción **Se necesita una cuenta (no se utiliza Agente de red)**.
4. Añada la cuenta con privilegios de administrador en el dispositivo donde se instala Kaspersky Security Center o la cuenta incluida en el grupo de dominio Propietarios del creador de directivas de grupo.
5. Otorgue los permisos a la cuenta seleccionada:
   a. Vaya a **Panel de control** → **Herramientas administrativas** y abra **Administración de directivas de grupo**.
   b. Haga clic en el nodo con el dominio requerido.
   c. Haga clic en la sección **Delegación**.
   d. En la lista desplegable **Permiso**, seleccione **Vincular Objetos de directivas de grupo**.
   e. Haga clic en **Añadir**.
   f. En la ventana **Seleccionar usuario, equipo o grupo** que se abre, seleccione la cuenta necesaria.
   g. Haga clic en **Aceptar** para cerrar la ventana **Seleccionar usuario, equipo o grupo**.
   h. En la lista **Grupos y usuarios**, seleccione la cuenta que acaba de añadir y después haga clic en **Avanzado** → **Avanzado**.
   i. En la lista de **Entradas de permisos**, haga doble clic en la cuenta que acaba de añadir.
   j. Otorgue los siguientes permisos:
      - **Crear objetos de grupo**

- **Eliminar objetos de grupo**
- **Crear objetos contenedores de directivas de grupo**
- **Borrar objetos contenedores de directivas de grupo**

k. Haga clic en **Aceptar** para guardar los cambios.

6. Defina otras configuraciones siguiendo las instrucciones del Asistente.
7. Ejecute manualmente la tarea de instalación remota creada o espere a que se produzca el inicio programado.

Se inicia la siguiente secuencia de instalación remota:

1. Durante la ejecución de la tarea, se crean los siguientes objetos en cada dominio que incluye los dispositivos cliente del conjunto especificado:
   - Objeto de directiva de grupo (Group policy object, GPO) con el nombre **Kaspersky_AK{GUID}**.
   - Un grupo de seguridad que equivale al GPO. Este grupo de seguridad incluye dispositivos cliente cubiertos por la tarea. El contenido del grupo de seguridad define la cobertura del GPO.
2. Kaspersky Security Center instala las aplicaciones seleccionadas en los dispositivos cliente directamente desde la carpeta de red compartida Compartir de la aplicación. En la carpeta de instalación de Kaspersky Security Center, se creará una carpeta auxiliar anidada, que contendrá el archivo .msi de la aplicación que se instalará.
3. Cuando se añaden nuevos dispositivos al alcance de la tarea, se los añade también al grupo de seguridad al iniciarse la siguiente tarea. Si la opción **Ejecutar tareas no realizadas** está seleccionada en la planificación de tareas, los dispositivos se añadirán al grupo de seguridad inmediatamente.
4. Cuando los dispositivos se eliminan del alcance de la tarea, se borran del grupo de seguridad durante el siguiente inicio de la tarea.
5. Cuando se elimina una tarea de Active Directory, se eliminan también el GPO, el enlace del GPO y el grupo de seguridad correspondiente.

Si quiere aplicar algún otro esquema de instalación mediante Active Directory, puede configurar manualmente los parámetros requeridos. Puede ser necesario en los siguientes casos:

- Cuando el administrador de la protección antivirus no tiene permisos para realizar cambios en Active Directory de ciertos dominios
- Cuando el paquete de instalación original debe almacenarse en un recurso de red independiente
- Cuando es necesario vincular un GPO a unidades de Active Directory específicas

Están disponibles las siguientes opciones para utilizar una planificación de instalación alternativa a través de Active Directory:

- Si la instalación debe realizarse directamente desde la carpeta compartida de Kaspersky Security Center, deberá especificar en las propiedades del GPO el archivo .msi ubicado en la subcarpeta exec de la carpeta del paquete de instalación para la aplicación requerida.
- Si el paquete de instalación debe localizarse en otro recurso de red, deberá copiar todo el contenido de la carpeta exec en este, ya que, además del archivo con la extensión .msi, la carpeta contiene archivos de

configuración generados cuando se creó el paquete. Para instalar la clave de licencia con la aplicación, copie también el archivo clave en esta carpeta.

Instalación de aplicaciones en Servidores de administración secundarios

Para instalar una aplicación en los Servidores de administración secundarios:

1. Establezca una conexión con el Servidor de administración que controla los Servidores de administración secundarios.

2. Asegúrese de que el paquete de instalación correspondiente a la aplicación que se está instalando esté disponible en cada uno de los Servidores de administración secundarios seleccionados. Si el paquete de instalación no se encuentra en ninguno de los Servidores secundarios, distribúyalo usando la tarea de distribución de paquetes de instalación.

3. Cree la tarea de instalación de aplicaciones en los Servidores de administración secundarios de una de las siguientes formas:

   - Si desea crear una tarea para los Servidores de administración secundarios en el grupo de administración seleccionado, cree una tarea de grupo de instalación remota para este grupo.

   - Si desea crear una tarea para Servidores de administración secundarios específicos, cree una tarea de instalación remota para dispositivos específicos.

   El Asistente para crear tareas de despliegue empieza a guiarle en el procedimiento de creación de la tarea de instalación remota. Siga las instrucciones del Asistente.

   En la ventana **Seleccionar el tipo de tarea** del Asistente para añadir tareas, en la sección **Servidor de administración de Kaspersky Security Center 14**, abra la carpeta **Avanzado** y seleccione el tipo de tarea **Instalar aplicación en Servidores de administración secundarios de forma remota**.

   El Asistente para añadir tareas creará la tarea de instalación remota de la aplicación seleccionada en Servidores de administración secundarios específicos.

4. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la planificación especificada en los parámetros de la tarea.

Al finalizar la tarea de instalación remota, se instalará la aplicación seleccionada en los Servidores de administración secundarios.

Instalación de aplicaciones con el Asistente de Instalación Remota

Puede usar el Asistente de Instalación remota para instalar aplicaciones Kaspersky. El Asistente de instalación remota permite la instalación remota de aplicaciones mediante paquetes de instalación creados previamente o directamente desde un paquete de distribución.

Para el funcionamiento correcto de la tarea de instalación remota en un dispositivo cliente en el que no se ha instalado un Agente de red, deben estar abiertos los siguientes puertos: TCP 139 y 445; UDP 137 y 138. De forma predeterminada, los puertos se abren para todos los dispositivos cliente incluidos en el dominio. La utilidad de preparación de instalación remota los abre automáticamente.

Para instalar la aplicación en los dispositivos seleccionados con el Asistente de instalación remota:

1. En el árbol de consola, encuentre la carpeta **Instalación remota** y seleccione la subcarpeta **Paquetes de instalación**.

2. En el espacio de trabajo de la carpeta, seleccione el paquete de instalación de la aplicación que tiene que instalar.

3. En el menú contextual del paquete de instalación, seleccione **Instalar aplicación**.

   Se inicia el Asistente de instalación remota.

4. En la ventana **Seleccionar dispositivos para la instalación**, se puede crear una lista de dispositivos en los que se instalará la aplicación:

   - Instalar en grupo de dispositivos administrados

     Si se selecciona esta opción, la tarea de instalación remota se creará para un grupo de dispositivos.

   - Seleccionar dispositivos para la instalación

     Si se selecciona esta opción, la tarea de instalación remota se creará para dispositivos específicos. Esos dispositivos específicos pueden ser tanto administrados como no asignados.

5. En la ventana **Definir la configuración de la tarea de instalación remota**, especifique la configuración para la instalación remota de la aplicación.

   En el grupo de ajustes **Forzar la descarga del paquete de instalación**, especifique cómo los archivos necesarios para la instalación de la aplicación se distribuirán a los dispositivos cliente:

   - Usando el Agente de red

     Si esta opción está habilitada, el Agente de red instalado en dispositivos cliente entrega los paquetes de instalación a dichos dispositivos cliente.

     Si esta opción está deshabilitada, los paquetes de instalación se entregan mediante las herramientas de Microsoft Windows.

     Recomendamos que habilite esta opción si la tarea se ha asignado a dispositivos que tienen instalados Agentes de red.

     Esta opción está activada de forma predeterminada.

   - Usando los recursos del sistema operativo mediante el Servidor de administración

     Si esta opción está habilitada, los archivos se transmitirán a dispositivos cliente mediante herramientas de Microsoft Windows a través del Servidor de administración. Puede activar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

     Esta opción está activada de forma predeterminada.

   - Usando recursos del sistema operativo mediante puntos de distribución

Si esta opción está habilitada, los paquetes de instalación se transmiten a los dispositivos cliente mediante herramientas del sistema operativo a través de los puntos de distribución. Se puede seleccionar esta opción si existe al menos un punto de distribución en la red.

Si la opción **Usando el Agente de red** está habilitada, los archivos se entregan mediante herramientas del sistema operativo solo si los recursos del Agente de red no están disponibles.

De forma predeterminada, esta opción está habilitada para tareas de instalación remotas creadas en un Servidor de administración virtual.

- **Número de intentos de instalación**

  Si, al ejecutar la tarea de instalación remota, Kaspersky Security Center no logra instalar una aplicación en un dispositivo administrado dentro del número de intentos de instalación especificado por el parámetro, Kaspersky Security Center deja de enviar el paquete de instalación a este dispositivo administrado y ya no inicia el instalador en el dispositivo.

  La opción `Número de intentos de instalación` le permite guardar los recursos del dispositivo administrado y reducir el tráfico (desinstalación, ejecución de archivos MSI y mensajes de error).

  Los intentos de inicio de tarea reiterados pueden indicar un problema en el dispositivo que impide la instalación. El administrador debería resolver el problema dentro del número de intentos de instalación especificado (por ejemplo, al asignar espacio de disco suficiente, al eliminar aplicaciones incompatibles o al modificar la configuración de otras aplicaciones que impiden la instalación) y reiniciar la tarea (manualmente o mediante una programación).

  Si finalmente no se logra realizar la instalación, el problema se considera irresoluble y cualquier otro inicio de tarea se percibe como costoso en cuanto a consumo innecesario de recursos y tráfico.

  Cuando se crea la tarea, el contador de intentos se fija en `0`. Cada intento del instalador que devuelve un error en el dispositivo aumenta la lectura del contador.

  Si se ha superado el número de intentos especificados en el parámetro y el dispositivo está listo para la instalación de la aplicación, puede aumentar el valor del parámetro `Number of attempts to install` e iniciar la tarea de instalación de la aplicación. O bien, puede crear una nueva tarea de instalación remota.

Defina qué desea hacer con los dispositivos cliente administrados por otro Servidor de administración:

- **Instalar en todos los dispositivos**

  La aplicación se instalará incluso en los dispositivos administrados por otros Servidores de administración.

  Esta opción está seleccionada de manera predeterminada; no tiene que cambiar esta configuración si solo tiene un Servidor de administración en su red.

- **Instalar solo en dispositivos administrados a través de este Servidor de administración**

  La aplicación se instalará solo en los dispositivos administrados por este Servidor de administración. Seleccione esta opción si tiene más de un Servidor de administración en su red y desea evitar conflictos entre ellos.

Defina la configuración adicional:

- **No reinstalar la aplicación si ya se encuentra instalada**

  Si esta opción está habilitada, la aplicación seleccionada no se volverá a instalar si ya está instalada en el dispositivo cliente.

  Si esta opción está deshabilitada, la aplicación se instalará igualmente.

  Esta opción está activada de forma predeterminada.

- **Asignar instalación del paquete en las directivas de grupo de Active Directory**

  Si esta opción está habilitada, se instalará un paquete de instalación mediante las directivas de grupo del Active Directory.

  Esta opción está disponible si se ha seleccionado el paquete de instalación del Agente de red.

  Esta opción está desactivada de forma predeterminada.

6. En la ventana **Selección de una clave de licencia**, seleccione una clave de licencia y un método para su distribución:

   - **No incluir la clave de licencia en el paquete de instalación (recomendado)**

     La clave se distribuye automáticamente a todos los dispositivos con los que es compatible:

     - Si se ha activado la distribución automática en las propiedades de la clave.
     - Si se ha creado la tarea **Agregar clave**.

   - **Incluir la clave de licencia en el paquete de instalación**

     La clave se distribuye a dispositivos junto con el paquete de instalación.

     No recomendamos que distribuya la clave con este método porque en el repositorio de paquetes está activado el acceso de lectura compartido.

   La ventana **Selección de una clave de licencia** se muestra si el paquete de instalación no incluye una clave de licencia.

   Si el paquete de instalación incluye una clave de licencia, se muestra la ventana **Propiedades de la clave de licencia** con los detalles de las claves de licencia.

7. En la ventana **Selección de una opción de reinicio del sistema operativo**, especifique si los dispositivos se han de reiniciar en caso de que el sistema operativo se deba reiniciar durante la instalación de las aplicaciones:

   - **No reiniciar el dispositivo**

     Si se selecciona esta opción, el dispositivo no se reiniciará después de la instalación de la aplicación de seguridad.

   - **Reiniciar el dispositivo**

Si se selecciona esta opción, el dispositivo se reiniciará después de la instalación de la aplicación de seguridad.

- **Solicitar al usuario una acción**

  Si se selecciona esta opción, después de instalar la aplicación de seguridad, se le mostrará al usuario una notificación sobre la necesidad de reiniciar el dispositivo. Con el enlace **Modificar** se puede modificar el texto del mensaje, el período durante el cual se muestra el mensaje y el tiempo que debe transcurrir para que se reinicie automáticamente.

  Esta opción está seleccionada de forma predeterminada.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  Si esta opción está activada, las aplicaciones de los dispositivos bloqueados se ven forzadas a cerrarse antes del reinicio.

  Esta opción está desactivada de forma predeterminada.

8. En la ventana **Seleccionar cuentas para acceder a los dispositivos**, puede añadir las cuentas que se utilizarán para iniciar la tarea de instalación remota:

   - **No es necesaria una cuenta (Agente de red instalado)**

     Si se selecciona esta opción, no tiene que especificar la cuenta bajo la que se ejecutará el instalador de aplicación. La tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

     Si el Agente de red no se ha instalado en dispositivos cliente, esta opción no está disponible.

   - **Se necesita una cuenta (no se utiliza Agente de red)**

     Si se selecciona esta opción, puede especificar la cuenta bajo la que se ejecutará el instalador de aplicación. Puede especificar la cuenta de usuario si el Agente de red no se ha instalado en los dispositivos para los cuales está asignada la tarea.

     Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que se asignó esta tarea. En este caso, todas las cuentas que se han agregado se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

     Si no se agrega ninguna cuenta, la tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

9. En la ventana **Iniciando la instalación**, haga clic en el botón **Siguiente** para crear e iniciar una tarea de instalación remota en los dispositivos seleccionados.

   Si la ventana **Iniciando la instalación** tiene seleccionada la opción **No ejecutar la tarea después de que el Asistente de instalación remota finalice**, la tarea de instalación remota no se iniciará. Más tarde podrá iniciar esta tarea manualmente. El nombre de la tarea equivale al nombre del paquete de instalación para la aplicación: **Instalación de <nombre del paquete de instalación>**.

Para instalar la aplicación en dispositivos de un grupo de administración con el Asistente de instalación remota:

1. Establezca una conexión con el Servidor de administración que controla el grupo de administración correspondiente.

2. Seleccione un grupo de administración en el árbol de consola.

3. En el espacio de trabajo del grupo, haga clic en el botón **Realizar acción** y seleccione **Instalar aplicación** en la lista desplegable.

   Se iniciará el Asistente de Instalación Remota. Siga las instrucciones del Asistente.

4. En el paso final del Asistente, haga clic en **Siguiente** para crear y ejecutar la tarea de instalación remota en los dispositivos seleccionados.

Cuando el Asistente de instalación remota se completa, Kaspersky Security Center realiza las siguientes acciones:

- Crea un paquete de instalación para la instalación de la aplicación (si no se creó antes). El paquete de instalación se encuentra en la carpeta **Instalación remota**, en la subcarpeta **Paquetes de instalación** y tiene un nombre que corresponde al nombre y versión de la aplicación. Puede usar este paquete de instalación para la instalación de la aplicación en el futuro.

- Crea y ejecuta una tarea de instalación remota para dispositivos específicos o para un grupo de administración. La tarea de instalación remota recién creada se almacena en la carpeta **Tareas** o se agrega a las tareas del grupo de administración para el cual se crearon. Más tarde podrá iniciar esta tarea manualmente. El nombre de la tarea equivale al nombre del paquete de instalación para la aplicación: **Instalación de <nombre del paquete de instalación>**.

Visualización de un informe del despliegue de la protección

Puede usar el informe del despliegue de la protección para supervisar el progreso del despliegue de la protección de red.

Para ver un informe del despliegue de la protección:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.

2. En el espacio de trabajo del nodo, abra la ficha **Informes**.

3. En el espacio de trabajo de la carpeta **Informes**, seleccione la plantilla de informe llamada **Informe del despliegue de la protección**.

El espacio de trabajo muestra un informe que contiene información sobre el despliegue de la protección en todos los dispositivos de la red.

Puede generar un nuevo informe del despliegue de la protección y especificar el tipo de datos que debe incluir:

- Para un grupo de administración.

- Para dispositivos específicos.

- Para una selección de dispositivos.

- Para todos los dispositivos.

Kaspersky Security Center supone que la protección se despliegue en un dispositivo si se instala una aplicación de seguridad y la protección en tiempo real se activa.

Eliminación remota de aplicaciones

Kaspersky Security Center permite desinstalar aplicaciones desde dispositivos remotamente a través de tareas de la desinstalación remotas. Esas tareas se crean y se asignan a dispositivos a través de un Asistente dedicado. Para asignar una tarea a dispositivos de modo más fácil y rápido, puede especificar dispositivos en la ventana del Asistente de una de estas formas:

- **Seleccionar dispositivos de red detectados por el Servidor de administración**. En este caso, la tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración así como dispositivos no asignados.
- **Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista**. Puede especificar nombres NetBIOS, nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.
- **Asignar tarea a una selección de dispositivos**. En este caso, la tarea se asigna a dispositivos incluidos en una selección creada anteriormente. Puede especificar la selección predeterminada o una personalizado que haya creado.
- **Asignar tarea a un grupo de administración**. En este caso, la tarea se asigna a dispositivos incluidos en un grupo de administración creado anteriormente.

Eliminación remota de una aplicación de los dispositivos cliente de un grupo de administración

Para eliminar una aplicación de forma remota de los dispositivos cliente de un grupo de administración:

1. Establezca una conexión con el Servidor de administración que controla el grupo de administración correspondiente.
2. Seleccione un grupo de administración en el árbol de consola.
3. En el espacio de trabajo del grupo, seleccione la ficha **Tareas**.
4. Ejecute la creación de tarea al hacer clic en el botón **Crear una tarea**.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

   En la ventana **Seleccionar el tipo de tarea** del Asistente para añadir tareas del nodo **Servidor de administración de Kaspersky Security Center 14**, en la carpeta **Avanzado**, seleccione **Desinstalar aplicación de forma remota** como tipo de tarea.

   El Asistente para añadir tareas crea una tarea de grupo de eliminación remota de la aplicación seleccionada. La nueva tarea aparece en el espacio de trabajo del grupo de administración, en la ficha **Tareas**.
5. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la planificación especificada en los parámetros de la tarea.

Al finalizar la tarea de eliminación remota, se eliminará la aplicación seleccionada de los dispositivos cliente del grupo de administración.

Eliminación remota de una aplicación de dispositivos seleccionados

Para eliminar una aplicación remotamente desde dispositivos seleccionados:

1. Establezca una conexión con el Servidor de administración que controla los dispositivos correspondientes.
2. En el árbol de consola, seleccione la carpeta **Tareas**.
3. Ejecute la creación de tareas haciendo clic en **Nueva tarea**.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

   En la ventana **Seleccionar el tipo de tarea** del Asistente para añadir tareas del nodo **Servidor de administración de Kaspersky Security Center 14**, en la carpeta **Avanzado**, seleccione **Desinstalar aplicación de forma remota** como tipo de tarea.

   El Asistente para añadir tareas crea una tarea de eliminación remota de la aplicación seleccionada de dispositivos específicos. La tarea recién creada se muestra en el espacio de trabajo de la carpeta **Tareas**.
4. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la planificación especificada en los parámetros de la tarea.

Al finalizar la tarea de eliminación remota, se eliminará la aplicación seleccionada de los dispositivos seleccionados.

Trabajo con paquetes de instalación

Al crear tareas de instalación remota el sistema usa paquetes de instalación que contienen los conjuntos de parámetros necesarios para la instalación del software.

> Los paquetes de instalación pueden contener un archivo clave. Recomendamos que evite compartir el acceso a paquetes de instalación que contienen un archivo clave.

Puede usar un paquete de instalación único varias veces.

Los paquetes de instalación creados por el Servidor de administración se mueven al árbol de la consola y se ubican en la carpeta de **Instalación remota**, en la subcarpeta **Paquetes de instalación**. Los paquetes de instalación se almacenan en el Servidor de administración, en una subcarpeta de servicio llamada Paquetes, dentro de la carpeta compartida especificada.

Creación de un paquete de instalación

Siga estos pasos para crear un paquete de instalación:

1. Conéctese al Servidor de administración necesario.
2. En el árbol de consola, en la carpeta **Instalación remota**, seleccione la subcarpeta **Paquetes de instalación**.
3. Inicie la creación de un paquete de instalación de una de estas formas:

   - Seleccionando **Nuevo** → **Paquete de Instalación** en el menú contextual de la carpeta **Paquetes de instalación**.
   - Seleccionando **Crear** → **Paquete de Instalación** en el menú contextual de la lista de paquetes de instalación.

- Haga clic en el enlace **Crear paquete de instalación**, en la sección de administración de la lista de paquetes de instalación.

Se iniciará el Asistente de nuevo paquete. Siga las instrucciones del Asistente.

Al crear un paquete de instalación para la aplicación Kaspersky, es posible que se le solicite que consulte el Contrato de licencia y la Política de privacidad para la aplicación. Lea detenidamente el siguiente Contrato de licencia y la Política de privacidad. Si está de acuerdo con todos los términos del Contrato de licencia y la Política de privacidad, seleccione las siguientes opciones en la sección **Confirmo que he leído y que comprendo y acepto en su totalidad los términos y las condiciones de lo siguiente**:

- **Los términos y condiciones de este EULA**
- **La Política de privacidad que describe la gestión de los datos**

La instalación de la aplicación en su dispositivo continuará después de que seleccione ambas opciones. Se retoma la creación del paquete de instalación. La ruta al archivo del Contrato de licencia y la Política de privacidad se especifica en el archivo KUD o KPD incluido en el kit de distribución de la aplicación para la que se va a crear el paquete de instalación.

Cuando crea un paquete de instalación para Kaspersky Endpoint Security para Mac, puede seleccionar el idioma del Contrato de licencia y la Política de privacidad.

Durante la creación de un paquete de instalación para una aplicación de la base de datos de aplicaciones de Kaspersky, puede activar la instalación automática de los componentes del sistema (requisitos previos) necesarios para la instalación de la aplicación. El Asistente de nuevo paquete muestra una lista de todos los componentes de sistema disponibles para la aplicación seleccionada. Si se ha creado un paquete de instalación de parches (paquete de distribución incompleto), la lista contiene todos los requisitos previos del sistema para el despliegue del parche, hasta todo el paquete de distribución. Dicha lista se puede buscar en cualquier momento en las propiedades del paquete de instalación.

Las actualizaciones de aplicaciones administradas pueden requerir la instalación de una versión mínima específica de Kaspersky Security Center. Si esta versión es posterior a su versión actual, estas actualizaciones se muestran pero no se pueden aprobar. Además, no se pueden crear paquetes de instalación a partir de dichas actualizaciones hasta que actualice Kaspersky Security Center. Se le solicitará que actualice su instancia de Kaspersky Security Center a la versión mínima requerida.

Una vez que finaliza el Asistente de nuevo paquete, aparece el nuevo paquete de instalación en el espacio de trabajo de la carpeta **Paquetes de instalación**, en el árbol de la consola.

No hay necesidad de crear manualmente un paquete de instalación para la instalación remota del Agente de red. Se crea automáticamente durante la instalación de Kaspersky Security Center y se almacena en la carpeta **Paquetes de instalación**. Si se ha eliminado el paquete para la instalación remota del Agente de red, puede volver a crearlo seleccionando el archivo nagent.kud en la carpeta NetAgent del paquete de distribución de Kaspersky Security Center.

No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación.

Al crear un paquete de instalación del Servidor de administración, seleccione el archivo sc.kud en la carpeta raíz del paquete de distribución de Kaspersky Security Center como el archivo de descripción.

Crear paquetes de instalación independientes.

Usted y los usuarios de dispositivos de su organización pueden utilizar paquetes de instalación independientes para instalar aplicaciones en dispositivos de forma manual.

Un paquete de instalación independiente es un archivo ejecutable (installer.exe) que puede almacenar en el servidor web, en una carpeta compartida, o transferir al dispositivo cliente de cualquier manera. También puede enviar un enlace al paquete de instalación independiente por correo electrónico. En el dispositivo cliente, el usuario puede ejecutar el archivo recibido localmente para instalar una aplicación sin utilizar Kaspersky Security Center.

Asegúrese de que el paquete de instalación independiente no esté disponible para personas no autorizadas.

Puede crear paquetes de instalación independientes de aplicaciones de Kaspersky y de aplicaciones de terceros para plataformas Windows, macOS y Linux. Para crear un paquete de instalación independiente para una aplicación de terceros, debe primero crear un paquete de instalación personalizada.

La fuente para crear paquetes de instalación independientes son los paquetes de instalación en la lista de creados en el Servidor de administración.

Para crear un paquete de instalación independiente:

1. En el árbol de la consola, seleccione el **Servidor de administración → Avanzado → Instalación remota → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. En la lista de paquetes de instalación, seleccione un paquete de instalación para el que desee crear un paquete independiente.

3. En el menú contextual, seleccione **Crear paquete de instalación independiente**.

   Se inicia el Asistente para crear paquete de instalación independiente. Avance por el Asistente utilizando el botón **Siguiente**.

4. En la primera página del Asistente, si seleccionó un paquete de instalación para la aplicación Kaspersky y desea instalar el Agente de red junto con la aplicación seleccionada, asegúrese de que la opción **Instalar Agente de red junto con esta aplicación** está habilitada.

   Esta opción está activada de forma predeterminada. Le recomendamos que active esta opción si no sabe si el Agente de red está instalado en el dispositivo. Si el Agente de red ya está instalado en el dispositivo, una vez que instale el paquete de instalación independiente con el Agente de red, este último se actualizará a la versión más reciente.

   Si desactiva esta opción, el Agente de red no se instalará en el dispositivo y este quedará no administrado.

   Si la aplicación seleccionada ya cuenta con un paquete de instalación independiente en el Servidor de administración, el Asistente se lo informa. En este caso, debe seleccionar una de las siguientes acciones:

   - **Crear un paquete de instalación independiente**. Seleccione esta opción si, por ejemplo, desea crear un paquete de instalación independiente para una nueva versión de la aplicación y también conservar un paquete de instalación independiente que haya creado para una versión de la aplicación anterior. El nuevo paquete de instalación independiente se ubicará en otra carpeta.

   - **Utilice el paquete de instalación independiente existente**. Seleccione esta opción si desea utilizar un paquete de instalación independiente existente. El proceso para crear paquetes no se iniciará.

- **Reconstruya el paquete de instalación independiente existente**. Seleccione esta opción si desea volver a crear un paquete de instalación independiente para la misma aplicación. El paquete de instalación independiente se ubicará en la misma carpeta.

5. En la siguiente página del Asistente, seleccione la opción **Mover dispositivos no asignados a este grupo** y especifique un grupo de administración al que desea mover el dispositivo cliente después de la instalación del Agente de red.

   De manera predeterminada, el dispositivo se mueve al grupo de **Dispositivos administrados**.

   Si no desea mover el dispositivo cliente a ningún grupo de administración después de la instalación del Agente de red, seleccione la opción **No mover dispositivos**.

6. En la página siguiente del Asistente, cuando finaliza el proceso de creación del paquete de instalación independiente, se muestra el resultado de la creación del paquete independiente y una ruta al paquete independiente.

   Puede hacer clic en los enlaces y hacer lo siguiente:

   - Abra la carpeta con el paquete de instalación independiente.
   - Envíe por correo electrónico el enlace al paquete de instalación independiente que se creó. Para realizar esta acción, debe tener una aplicación de correo electrónico iniciada.
   - Ejemplo de código HTML para la publicación de enlaces en un sitio web. Se crea y abre un archivo TXT en una aplicación que está asociada con un formato TXT. En el archivo, se muestra la etiqueta HTML <a> con atributos.

7. En la siguiente página del Asistente, si desea abrir la lista de paquetes de instalación independientes, active la opción **Abrir la lista de paquetes independientes**.

8. Haga clic en el botón **Finalizar**.

   Asistente para crear paquete de instalación independiente se cierra.

Se crea el paquete de instalación independiente y se lo ubica en la subcarpeta PkgInst de la carpeta compartida del Servidor de administración. Puede ver la lista de paquetes independientes si hace clic en el botón **Ver la lista de paquetes independientes** que se encuentra encima de la lista de paquetes de instalación.

Crear paquetes de instalación personalizada

Puede utilizar paquetes de instalación personalizada para hacer lo siguiente:

- Para instalar cualquier aplicación (como un editor de texto) en un dispositivo cliente, por ejemplo, mediante una tarea.
- Para crear un paquete de instalación independiente.

Un paquete de instalación personalizada es una carpeta con un conjunto de archivos. La fuente para crear un paquete de instalación personalizada es un *archivo de almacenamiento*. El archivo de almacenamiento contiene un archivo o archivos que deben incluirse en el paquete de instalación personalizada. Al crear un paquete de instalación personalizada, puede especificar parámetros de línea de comandos, por ejemplo, para instalar la aplicación en modo silencioso.

Para crear un paquete de instalación personalizada:

1. En el árbol de la consola, seleccione el **Servidor de administración → Avanzado → Instalación remota → Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Encima de la lista de los paquetes de instalación, haga clic en el botón **Crear paquete de instalación**.

   Se inicia el Asistente de nuevo paquete. Avance por el Asistente utilizando el botón **Siguiente**.

3. En la primera página del Asistente, seleccione la opción **Crear un paquete de instalación para el archivo ejecutable especificado**.

4. En la siguiente página del Asistente, especifique el nombre del paquete de instalación personalizada

5. En la siguiente página del Asistente, haga clic en el botón **Examinar** y, en una ventana estándar de Windows **Abrir**, elija un archivo de almacenamiento ubicado en los discos disponibles para crear un paquete de instalación personalizada.

   Puede cargar un archivo ZIP, CAB, TAR o TAR.GZ. No es posible crear un paquete de instalación desde un archivo SFX (archivo autoextraíble).

   Los archivos se descargan al Servidor de administración de Kaspersky Security Center.

6. En la siguiente página del Asistente, especifique los parámetros de la línea de comandos de un archivo ejecutable.

   Puede especificar parámetros de línea de comandos para instalar la aplicación desde el paquete de instalación en modo silencioso. La especificación de los parámetros de la línea de comandos es opcional.

   Si lo desea, configure las siguientes opciones:

   - **Copiar toda la carpeta en el paquete de instalación**

     Seleccione esta opción si el archivo ejecutable viene acompañado de archivos adicionales necesarios para la instalación de la aplicación. Antes de habilitar esta opción, asegúrese de que todos los archivos requeridos estén almacenados en la misma carpeta. Si esta opción está habilitada, la aplicación agrega el contenido completo de la carpeta, incluido el archivo ejecutable especificado, al paquete de instalación.

   - **Convertir la configuración a valores recomendados para aplicaciones reconocidas por Kaspersky Security Center 14**

     La aplicación se instalará con la configuración recomendada, si la información sobre la aplicación especificada se encuentra en la base de datos de Kaspersky.

     Si ha ingresado parámetros en el campo **Línea de comando de archivo ejecutable**, se los reemplaza por los ajustes recomendados.

     Esta opción está activada de forma predeterminada.

     La base de datos de Kaspersky la crean y mantienen los analistas de Kaspersky. Para cada aplicación que se agrega a la base de datos, los analistas de Kaspersky definen la configuración de instalación óptima. La configuración se define para garantizar la instalación remota correcta de una aplicación en un dispositivo cliente. La base de datos se actualiza automáticamente en el Servidor de administración cuando ejecuta la tarea Descargar actualizaciones en el repositorio del Servidor de administración.

   Se inicia el proceso para crear el paquete de instalación personalizada.

   El Asistente le informa cuando finaliza el proceso.

   Si no se crea el paquete de instalación personalizada, se muestra el mensaje adecuado.

7. Haga clic en el botón **Finalizar** para cerrar el Asistente.

El paquete de instalación que ha creado se descarga en la subcarpeta Paquetes de la carpeta compartida del Servidor de administración. Después de la descarga, el paquete de instalación personalizada aparece en la lista de paquetes de instalación.

En la lista de paquetes de instalación en el Servidor de administración, puede ver y editar las propiedades del paquete de instalación personalizada.

Ver y editar propiedades de paquetes de instalación personalizada

Después de crear un paquete de instalación personalizada, puede ver información general sobre el paquete de instalación y especificar la configuración de instalación en la ventana de propiedades.

Ver y editar propiedades de paquetes de instalación personalizada:

1. En el árbol de la consola, seleccione el **Servidor de administración** → **Avanzado** → **Instalación remota** → **Paquetes de instalación**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Abra el menú contextual del paquete de instalación y seleccione **Propiedades**.

   Se abrirá la ventana de propiedades del paquete de instalación seleccionado.

3. Ver la siguiente información:

   - Nombre del paquete de instalación
   - Nombre de la aplicación empaquetada en el paquete de instalación personalizado
   - Versión de la aplicación
   - Fecha de creación del paquete de instalación
   - Ruta al paquete de instalación personalizada en el Servidor de administración
   - Línea de comando de archivo ejecutable

4. Especifique los siguientes parámetros:

   - Nombre del paquete de instalación
   - **Instalar componentes generales del sistema requeridos**

     Si esta opción está activada, antes de instalar una actualización, la aplicación instala automáticamente todos los componentes generales del sistema (requisitos previos) que se requieren para instalar la actualización. Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo

     Si esta opción está desactivada, es posible que tenga que instalar los requisitos previos de manera manual.

     Esta opción está desactivada de forma predeterminada.

     Esta opción solo está disponible cuando Kaspersky Security Center reconoce la aplicación añadida al paquete de instalación.

- Línea de comando de archivo ejecutable

  Si la aplicación requiere parámetros adicionales para una instalación silenciosa, especifíquelos en este campo. Consulte la documentación del proveedor para más detalles.

  También puede introducir otros parámetros.

  Esta opción solo está disponible para los paquetes que no se crean sobre la base de las aplicaciones de Kaspersky.

5. Haga clic en el botón **Aceptar** o **Aplicar** para guardar los cambios, si los hubiera.

Se guardan las nuevas configuraciones.

Obtención del paquete de instalación del Agente de red del kit de distribución de Kaspersky Security Center

Puede obtener el paquete de instalación del Agente de red del kit de distribución de Kaspersky Security Center, sin necesidad de instalar Kaspersky Security Center. Después, puede usar el paquete de instalación para instalar el Agente de red en los dispositivos cliente.

Para obtener el paquete de instalación del Agente de red del kit de distribución de Kaspersky Security Center, haga lo siguiente:

1. Ejecute el archivo ejecutable ksc_<version number>.<build number>_full_<localization language>.exe desde el kit de distribución de Kaspersky Security Center.
2. En la ventana que se abre, haga clic en el enlace **Extraer paquetes de instalación**.
3. En la lista de paquetes de instalación, seleccione la casilla junto al paquete de instalación del Agente de red y luego haga clic en el botón **Siguiente**.
4. Si es necesario, haga clic en el botón **Examinar** para cambiar la carpeta que se muestra para extraer el paquete de instalación.
5. Haga clic en el botón **Extraer**.

   La aplicación extrae el paquete de instalación del Agente de red.
6. Cuando el proceso se haya completado, haga clic en el botón **Cerrar**.

El paquete de instalación del Agente de red se extrae en la carpeta seleccionada.

Puede usar el paquete de instalación para instalar el Agente de red mediante uno de los siguientes métodos:

- Localmente, ejecutando el archivo setup.exe desde la carpeta extraída
- Mediante instalación silenciosa
- Utilizando directivas de grupo de Microsoft Windows

Distribución de paquetes de instalación a Servidores de administración secundarios

Para distribuir paquetes de instalación a Servidores de administración secundarios:

1. Establezca una conexión con el Servidor de administración que controla los Servidores de administración secundarios.

2. Cree una tarea de distribución de paquetes de instalación en Servidores de administración secundarios de una de las siguientes formas:

   - Si desea crear una tarea para los Servidores de administración secundarios en el grupo de administración seleccionado, inicie la creación de una tarea de grupo para este grupo.

   - Si desea crear una tarea para Servidores de administración secundarios, cree una tarea para dispositivos específicos.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

   En la ventana **Seleccionar el tipo de tarea** del Asistente para crear nueva tarea, en el nodo **Servidor de administración de Kaspersky Security Center 14**, en la carpeta **Avanzado**, seleccione el tipo de tarea **Distribuir paquete de instalación**.

   El Asistente para añadir tareas creará la tarea de distribución de los paquetes de instalación seleccionados en los Servidores de administración secundarios específicos.

3. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la programación que especificó en la configuración de la tarea.

Los paquetes de instalación seleccionados se copiarán en los Servidores de administración secundarios específicos.

La distribución de paquetes de instalación a través de puntos de distribución

Puede usar los puntos de distribución para distribuir paquetes de instalación dentro de un grupo de administración.

Después de haber recibido los paquetes de instalación del Servidor de administración, los puntos de distribución los distribuyen automáticamente a los dispositivos cliente mediante una distribución a varias direcciones IP. La multidifusión IP de nuevos paquetes de instalación en un grupo de administración ocurre una vez. Si un dispositivo cliente se desconectó de la red corporativa durante la sesión de distribución, el Agente de red (en el dispositivo cliente) descarga automáticamente el paquete de instalación requerido de un punto de distribución cuando se inicia la tarea de instalación.

Transferencia de resultados de instalación de aplicaciones en Kaspersky Security Center

Después de haber creado el paquete de instalación de la aplicación, puede configurarlo para que toda la información de diagnóstico sobre los resultados de la instalación de la aplicación se transfieran a Kaspersky Security Center. Para los paquetes de instalación de aplicaciones de Kaspersky, se configura de forma predeterminada la transferencia de la información de diagnóstico sobre los resultados de la instalación de la aplicación, y no se requiere ninguna configuración adicional.

Para configurar la transferencia de información de diagnóstico sobre los resultados de la instalación de la aplicación a Kaspersky Security Center:

1. Navegue hasta la carpeta del paquete de instalación creado mediante Kaspersky Security Center para la aplicación seleccionada. La carpeta se puede encontrar en la carpeta compartida especificada durante la instalación de Kaspersky Security Center.

2. Abra el archivo con la extensión .kpd o .kud para editar (por ejemplo, en el editor Bloc de notas de Microsoft Windows).

   El archivo tiene el formato de un archivo .ini de configuración normal.

3. Agregue las siguientes líneas al archivo:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Este comando configura Kaspersky Security Center para que espere la finalización de la configuración de la aplicación, para la cual se creó el paquete de instalación y para analizar el código de retorno. Si tiene que desactivar la transferencia de datos de diagnóstico, establezca el valor de la clave de espera en 0.

4. Agregue la descripción de los códigos de retorno para una instalación exitosa. Para ello, agregue las siguientes líneas al archivo:

   ```
   [SetupProcessResult_SuccessCodes]
   <código de retorno>=[<descripción>]
   <código de retorno 1>=[<descripción>]
   ...
   ```

   Los corchetes contienen claves opcionales.

   Sintaxis de las líneas:

   - `<código de retorno>`. Cualquier número que corresponda al código de retorno del instalador. La cantidad de códigos de retorno puede ser arbitraria.
   - `<descripción>`. Descripción del texto del resultado de la instalación Se puede omitir la descripción.

5. Agregue la descripción de los códigos de retorno para una instalación fallida. Para ello, agregue las siguientes líneas al archivo:

   ```
   [SetupProcessResult_ErrorCodes]
   <código de retorno>=[<descripción>]
   <código de retorno 1>=[<descripción>]
   ...
   ```

   La sintaxis de estas líneas es idéntica a la sintaxis de las líneas que contienen códigos de retorno de instalación exitosa.

6. Cierre el archivo .kpd o .kud guardando todos los cambios.

Por último, los resultados de la instalación de la aplicación definida por el usuario se incluirá en los registros de Kaspersky Security Center y aparecerán en la lista de eventos, en los informes y en los registros de ejecución de tareas.

Definición de la dirección del servidor proxy de KSN para los paquetes de instalación

En caso de que cambie la dirección o el dominio del Servidor de administración, puede definir la dirección del Servidor Proxy KSN para el paquete de instalación.

Para definir la dirección del servidor proxy de KSN para el paquete de instalación:

1. En el árbol de la consola, en la carpeta **Instalación remota**, haga doble clic en la subcarpeta **Paquetes de instalación**.
2. En el menú que se abre, seleccione **Propiedades**.
3. En la ventana de propiedades que se abre, seleccione la subsección **General**.
4. En la subsección **General** de la ventana de propiedades, ingrese la dirección del servidor proxy de KSN.

Los paquetes de instalación utilizarán esta dirección como predeterminada.

Recepción de versiones actualizadas de las aplicaciones

Kaspersky Security Center permite recibir versiones actualizadas de aplicaciones corporativas almacenadas en los servidores de Kaspersky.

Para recibir versiones actualizadas de las aplicaciones corporativas de Kaspersky:

1. Realice una de las siguientes acciones:

   - En el árbol de la consola, seleccione el nodo con el nombre del Servidor de administración requerido, asegúrese de que **Supervisión** se selecciona la ficha y en el **Despliegue** haga clic en la sección **Hay nuevas versiones disponibles de las aplicaciones de Kaspersky** enlace.

     El enlace **Hay nuevas versiones disponibles de las aplicaciones de Kaspersky** pasa a ser visible cuando el Servidor de administración encuentra una versión nueva de la aplicación corporativa en un servidor de Kaspersky.

   - En el árbol de la consola, seleccione **Avanzado** → **Instalación remota** → **Paquetes de instalación** y en el espacio de trabajo, haga clic en **Acciones adicionales** y de la lista desplegable, seleccione Ver versión actual de la aplicación Kaspersky.

   Se muestra la lista de la versión actual de las aplicaciones de Kaspersky.

2. Seleccione la aplicación requerida de la lista.
3. Descargue el paquete de distribución de la aplicación al hacer clic en el enlace **Dirección web del paquete de distribución**.

Las actualizaciones de aplicaciones administradas pueden requerir la instalación de una versión mínima específica de Kaspersky Security Center. Si esta versión es posterior a su versión actual, estas actualizaciones se muestran pero no se pueden aprobar. Además, no se pueden crear paquetes de instalación a partir de dichas actualizaciones hasta que actualice Kaspersky Security Center. Se le solicitará que actualice su instancia de Kaspersky Security Center a la versión mínima requerida.

Si se muestra el botón **Descargar aplicaciones y crear paquetes de instalación** para la aplicación seleccionada, puede hacer clic en él para descargar el paquete de distribución de la aplicación y crear un paquete de instalación automáticamente. Kaspersky Security Center descarga el paquete de distribución de la aplicación en el Servidor de administración, en la carpeta compartida especificada durante la instalación de Kaspersky Security Center. El paquete de instalación creado de forma automática se **Instalación remota** del árbol de consola, en la subcarpeta **Paquetes de instalación**.

Después de cerrarse la ventana **Versiones actuales de la aplicación** el enlace **Hay nuevas versiones disponibles de las aplicaciones de Kaspersky** desaparece de la sección **Despliegue**.

Puede crear paquetes de instalación para versiones nuevas de las aplicaciones y administrar paquetes de instalación de reciente creación en la carpeta **Instalación remota** del árbol de consola, en la subcarpeta **Paquetes de instalación**.

También puede abrir la ventana **Versiones actuales de la aplicación** si hace clic en el enlace **Ver versiones actuales de aplicaciones Kaspersky** en el espacio de trabajo de la carpeta **Paquetes de instalación**.

Preparación de un dispositivo para instalación remota. Herramienta de utilidad riprep.exe

La instalación remota de una aplicación en un dispositivo cliente puede devolver un error por los siguientes motivos:

- La tarea ya se ejecutó correctamente en este dispositivo. En este caso, la tarea no debe volver a ejecutarse.
- Cuando se inició la tarea, el dispositivo se apagó. En este caso, encienda el dispositivo y reinicie la tarea.
- No hay conexión entre el Servidor de administración y el Agente de red instalado en el dispositivo cliente. Para establecer la causa del problema, use la utilidad diseñada para el diagnóstico remoto de los dispositivos cliente (klactgui).
- Si el Agente de red no está instalado en el dispositivo, se pueden producir los siguientes problemas durante la instalación remota:
  - El dispositivo cliente tiene **Desactivar el uso compartido simple de archivos** activado.
  - El servicio del servidor no se está ejecutando en el dispositivo cliente.
  - Los puertos necesarios están cerrados en el dispositivo cliente.
  - La cuenta que se utiliza para ejecutar la tarea no tiene privilegios suficientes.

  Para solucionar los problemas que se produjeron al instalar la aplicación en un dispositivo cliente sin el Agente de red instalado, puede usar esta utilidad designada para preparar los dispositivos para la instalación remota (riprep).

Esta sección describe la utilidad, lo que le permite preparar un dispositivo para la instalación remota (riprep). La utilidad se encuentra en la carpeta de instalación de Kaspersky Security Center en el dispositivo en el que está instalado el Servidor de administración.

La utilidad que se usa para preparar un dispositivo para la instalación remota no se ejecuta en Microsoft Windows XP Home Edition.

Preparación de un dispositivo para la instalación remota en modo interactivo

Para preparar un dispositivo para la instalación remota en el modo interactivo:

1. Ejecute el archivo riprep.exe en el dispositivo cliente.
2. En la ventana principal de la utilidad de preparación de instalación remota, seleccione las siguientes opciones:
   - **Desactivar el uso compartido simple de archivos**
   - **Iniciar el servicio del Servidor de administración**
   - **Puertos abiertos**
   - **Agregar una cuenta**
   - **Deshabilitar el control de cuentas de usuario (UAC)** solo está disponible para dispositivos que ejecutan con Microsoft Windows Vista, Microsoft Windows 7 o Microsoft Windows Server 2008.
3. Haga clic en el botón **Iniciar**.

   Las etapas de preparación de dispositivos de instalación remota se muestran en la parte inferior de la ventana principal de la utilidad.

Si seleccionó la opción **Agregar una cuenta**, cuando se cree una cuenta, se le solicitará introducir el nombre de la cuenta y la contraseña. Se creará una cuenta local, que pertenece al grupo de administradores locales.

Si selecciona la opción **Deshabilitar el Control de Cuenta de Usuario (UAC)**, se intentará desactivar el Control de cuenta de usuario incluso si UAC se desactivó antes de que se iniciara la utilidad. Después de que UAC se desactive, se le solicitará reiniciar el dispositivo.

Preparación de un dispositivo para la instalación remota en modo no interactivo

Preparación de un dispositivo para la instalación remota en modo no interactivo:

Ejecute el archivo riprep.exe en el dispositivo cliente desde la línea de comandos con el conjunto de claves necesario.

Sintaxis de línea de comandos de la utilidad:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Descripciones de las claves:

- `-silent:` Inicia la utilidad en el modo no interactivo.
- `-cfg CONFIG_FILE`: Define la configuración de la utilidad donde `CONFIG_FILE` es la ruta al archivo de configuración (un archivo con extensión .ini).
- `-tl traceLevel`: Define el nivel de seguimiento, donde `traceLevel` – Un número de 0 a 5. Si no se especifica la clave, se usa el valor 0.

Puede ejecutar las siguientes tareas iniciando la utilidad en modo silencioso:

- Deshabilitar el uso compartido simple de archivos.
- Iniciar el servicio del servidor en el dispositivo cliente.
- Abrir los puertos.
- Crear una cuenta local.
- Deshabilitar el Control de Cuenta de Usuario (UAC).

Puede indicar los parámetros de preparación del dispositivo para la instalación remota en el archivo de configuración especificado en la clave `-cfg`. Para definir estos parámetros, agregue la siguiente información al archivo de configuración:

- En la sección `Common`, especifique las tareas a realizar:
  - `DisableSFS`: Desactivar el uso compartido simple de archivos (0: la tarea se desactiva; 1: la tarea se activa).
  - `StartServer`: Iniciar el servicio del servidor (0: la tarea se desactiva; 1: la tarea se activa).
  - `OpenFirewallPorts`: Abrir los puertos necesarios (0: la tarea se desactiva; 1: la tarea se activa).
  - `DisableUAC`: Desactivar control de cuenta de usuario (UAC) (0: la tarea se desactiva; 1: la tarea se activa).
  - `RebootType`: Definir el comportamiento si se requiere reiniciar el dispositivo cuando UAC está desactivado. Puede usar los siguientes valores:
    - 0: Nunca reiniciar el dispositivo.
    - 1: Reiniciar el dispositivo, si UAC se activó antes de iniciar la herramienta.
    - 2: Forzar reinicio, si UAC se activó antes de iniciar la utilidad.
    - 4: Siempre reiniciar el dispositivo.
    - 5: Siempre forzar reinicio del dispositivo.
- En la sección `UserAccount`, especifique el nombre de la cuenta (`user`) y la contraseña (`Pwd`).

Contexto de ejemplo del archivo de configuración:

```
[Common]
DisableSFS=0
StartServer=1
```

```
OpenFirewallPorts=1
[UserAccount]
user=Admin
Pwd=Pass123
```

Una vez que finaliza la utilidad, se crearán los siguientes archivos en la carpeta de inicio de la utilidad:

- riprep.txt: Informe de la operación, en el cual se mencionan las etapas de operación de la utilidad con motivos para estas operaciones.
- riprep.log: El archivo de seguimiento (se crea si se establece un nivel de seguimiento superior a 0).

Preparación de un dispositivo Linux para instalación remota del Agente de red

Para preparar un dispositivo con Linux para la instalación remota del Agente de red:

1. Asegúrese de que sudo está instalado en el dispositivo Linux de destino.
2. Pruebe la configuración del dispositivo:
   a. Compruebe si puede conectarse al dispositivo a mediante un cliente SSH (por ejemplo PuTTY).

      Si no puede conectarse al dispositivo, abra el archivo /etc/ssh/sshd_config y asegúrese de que los siguientes ajustes tengan los respectivos valores indicados a continuación:

      `PasswordAuthentication no`

      `ChallengeResponseAuthentication yes`

      Guarde el archivo (si es necesario) y reinicie el servicio SSH usando el comando `sudo service ssh restart`.

   b. Desactive la contraseña de sudo para la cuenta de usuario bajo la cual se debe conectar el dispositivo.

   c. Use el comando `visudo` en sudo para abrir el archivo de configuración sudoers.

      En el archivo que ha abierto, busque la línea que comienza con `%sudo` (o con `%wheel` is usa el sistema operativo CentOS). En dicha línea, especifique lo siguiente: <`nombre de usuario` > `ALL = (ALL) NOPASSWD: ALL`. En este caso, el < `nombre de usuario` > es la cuenta de usuario que se utilizará para conectar el dispositivo mediante SSH.

   d. Guarde el archivo sudoers y después ciérrelo.

   e. Conéctese al dispositivo de nuevo a través de SSH y asegúrese de que el servicio de Sudo no le solicite introducir una contraseña, porque puede usar el comando `sudo whoami` para hacerlo.
3. Abra el fichero /etc/systemd/logind.conf file, y ejecute una de las siguientes acciones:
   - Especifique “no” como valor para el ajuste KillUserProcesses: `KillUserProcesses=no`
   - Para la configuración de KillExcludeUsers, escriba el nombre de usuario de la cuenta con la que se va a realizar la instalación remota, por ejemplo, `KillExcludeUsers=root`.

   Para aplicar el ajuste modificado, reinicie el dispositivo Linux o ejecute el siguiente comando:

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

4. Si desea instalar Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, instale el paquete insserv-compat primero para configurar el Agente de red.

5. Descargar y crear un paquete de instalación:

   a. Antes de instalar el paquete en el dispositivo, asegúrese de que ya tiene instaladas todas las dependencias (programas y bibliotecas) para este paquete.

      Puede ver las dependencias de cada paquete por su propia cuenta, mediante las utilidades específicas de la distribución Linux en la que instalará el paquete. Para obtener más información sobre las utilidades, consulte la documentación del sistema operativo.

   b. Descargue el paquete de instalación del Agente de red.

   c. Para crear un paquete de instalación remota, use los siguientes archivos:

      - klnagent.kpd
      - akinstall.sh
      - Paquete .deb o .rpm de Agente de red

6. Cree una tarea de instalación remota con la siguiente configuración:

   - En la página **Configuración** del Asistente para añadir tareas, marque la casilla **Usando los recursos del sistema operativo mediante el Servidor de administración**. Desmarcar todas las demás selecciones.
   - En la página **Seleccionar una cuenta para ejecutar la tarea**, para ejecutar la tarea, especifique la configuración de la cuenta de usuario que se utiliza para conectar el dispositivo mediante SSH.

7. Ejecute la tarea de instalación remota.

Es posible que se devuelva un error si instala el Agente de red mediante SSH en dispositivos que ejecutan versiones de Fedora anteriores a la versión 20. En este caso, para una instalación correcta de Agente de red, comente la opción Defaults requiretty (inclúyala en la sintaxis de comentarios para eliminarla del código analizado) en el archivo /etc/sudoers. Para obtener una descripción detallada de la condición de la opción Defaults requiretty, que puede causar problemas durante la conexión SSH, consulte el sitio web Bugzilla bugtracker.

Preparación de un dispositivo que ejecuta SUSE Linux Enterprise Server 15 para la instalación del Agente de red

Para instalar el Agente de red en un dispositivo con el sistema operativo SUSE Linux Enterprise Server 15,

Antes de la instalación del Agente de red, ejecute el siguiente comando:

```
$ sudo zypper install insserv-compat
```

Esto le permite instalar el paquete insserv-compat y configurar el Agente de red correctamente.

Ejecute el comando `rpm -q insserv-compat` para verificar si el paquete ya está instalado.

Si su red incluye muchos dispositivos que ejecutan SUSE Linux Enterprise Server 15, puede usar el software especial para configurar y administrar la infraestructura de la empresa. Al usar este software, puede instalar automáticamente el paquete insserv-compat en todos los dispositivos necesarios a la vez. Por ejemplo, puede usar Puppet, Ansible, Chef o puede crear su propio script; use cualquier método que le resulte conveniente.

Además de la instalación del paquete insserv-compat, asegúrese de haber preparado completamente sus dispositivos Linux. Después, despliegue e instale el Agente de red.

Preparación de un dispositivo macOS para instalación remota del Agente de red

Para preparar un dispositivo con macOS para la instalación remota del Agente de red:

1. Asegúrese de que sudo está instalado en el dispositivo macOS de destino.
2. Pruebe la configuración del dispositivo:
   a. Asegúrese de que el puerto 22 esté abierto en el dispositivo cliente: en las **Preferencias del sistema**, abra el panel **Compartir** y asegúrese de que la casilla de verificación **Inicio de sesión remoto** esté seleccionada. Puede usar el comando `ssh <device_name>` para iniciar sesión en el dispositivo macOS de forma remota.

      En el panel **Compartir**, puede usar la opción **Permitir acceso a** para establecer el alcance de los usuarios a los que se les permite acceder al dispositivo macOS.

   b. Desactive la contraseña de sudo para la cuenta de usuario bajo la cual se debe conectar el dispositivo.

      Use el comando `sudo visudo` para abrir el archivo de configuración sudoers. En el archivo que ha abierto, en la entrada `User privilege specification`, especifique lo siguiente: `username ALL = (ALL) NOPASSWD: ALL`. Aquí, `username` es la cuenta de usuario que se utilizará para conectar el dispositivo Secure Shell (SSH).

   c. Guarde el archivo sudoers y después ciérrelo.

   d. Conéctese al dispositivo de nuevo a través de SSH y asegúrese de que el servicio de Sudo no le solicite introducir una contraseña, porque puede usar el comando `sudo whoami` para hacerlo.
3. Descargar y crear un paquete de instalación:
   a. Descargue el paquete de instalación del Agente de red utilizando uno de los siguientes métodos:

      - En el árbol de la consola, abra el menú contextual en **Instalación remota** → **Paquetes de instalación** y seleccione **Mostrar las versiones actuales de la aplicación** para elegir de entre los paquetes disponibles
      - Descargue versión pertinente del Agente de red del sitio web del Servicio de soporte técnico en https://support.kaspersky.com/
      - Solicite el paquete de instalación a especialistas del Servicio de soporte Técnico

   b. Para crear un paquete de instalación remota, use los siguientes archivos:

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. Cree una tarea de instalación remota con la siguiente configuración:

    - En la página **Configuración** del Asistente para añadir tareas, seleccione la casilla **Usando los recursos del sistema operativo mediante el Servidor de administración**. Desmarcar todas las demás selecciones.

    - En la página **Seleccionar una cuenta para ejecutar la tarea**, para ejecutar la tarea, especifique la configuración de la cuenta de usuario que se utiliza para conectar el dispositivo mediante SSH.

El dispositivo cliente está listo para la instalación remota del Agente de red a través de la tarea correspondiente que ha creado.

Aplicaciones de Kaspersky: licencia y activación

Esta sección describe las funciones de Kaspersky Security Center relacionadas con el manejo de claves de licencia de las aplicaciones administradas de Kaspersky.

Kaspersky Security Center le permite realizar una distribución centralizada de las claves de licencia para las aplicaciones Kaspersky en dispositivos cliente, supervisar su uso y renovar las licencias.

Al agregar una clave de licencia mediante Kaspersky Security Center, los parámetros de la clave de licencia se almacenan en el Servidor de administración. En función de esta información, la aplicación genera un informe de uso de claves de licencia y envía notificaciones al administrador cuando caducan las licencias y cuando se infringen las restricciones de las licencias especificadas en las propiedades de las claves de licencia. Puede configurar notificaciones del uso de claves de licencia en los parámetros del Servidor de administración.

Obtención de licencias de aplicaciones administradas

Las aplicaciones de Kaspersky instaladas en los dispositivos administrados se deben licenciar aplicando un archivo clave o código de activación a cada una de las aplicaciones. Los archivos clave o códigos de activación se pueden desplegar de las siguientes formas:

- Despliegue automático
- El paquete de instalación de una aplicación administrada
- La tarea *Agregar clave de licencia* para una aplicación administrada
- Activación manual de una aplicación administrada

Puede añadir una nueva clave de licencia activa o de reserva mediante cualquiera de los métodos enumerados anteriormente. Una aplicación de Kaspersky utiliza una clave activa en el momento actual y almacena una clave de reserva para aplicar después de que caduque la clave activa. La aplicación para la que añade una clave de licencia define si la clave está activa o si es de reserva. La definición de la clave no depende del método que utilice para añadir una nueva clave de licencia.

Despliegue automático

Si usa diferentes aplicaciones administradas y tiene que desplegar un archivo clave o un código de activación específicos en los dispositivos, opte por otras formas de desplegar ese código de activación o archivo clave.

Kaspersky Security Center le permite desplegar automáticamente las claves de licencia disponibles en los dispositivos. Por ejemplo, en el repositorio del Servidor de administración se almacenan tres claves de licencia. Ha seleccionado la casilla de verificación **Distribuir automáticamente la clave de licencia a los dispositivos administrados** para las tres claves de licencia. En los dispositivos de la organización se ha instalado una aplicación de seguridad de Kaspersky, por ejemplo, Kaspersky Endpoint Security para Windows. Se detecta un nuevo dispositivo en el que se debe desplegar una clave de licencia. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden instalar en el dispositivo: una clave de licencia llamada *Clave_1* y una clave de licencia llamada *Clave_2*. Una de estas claves de licencia se despliega en el dispositivo. En este caso, no se puede predecir cuál de las dos claves de licencia se instalará en el dispositivo porque el despliegue automático de claves de licencia no prevé ninguna actividad de administrador.

Cuando se despliega una clave de licencia, los dispositivos se vuelven a contar para esa clave de licencia. Debe asegurarse de que la cantidad de dispositivos en los que se desplegó la clave de licencia no exceda el límite de la licencia. Si la cantidad de dispositivos excede el límite de la licencia, se asignará a todos los dispositivos que no estaban cubiertos por la licencia el estado *Crítico*.

Antes del despliegue, se deben añadir el archivo clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Consola de administración:
  - Adición de una clave de licencia al repositorio del Servidor de administración
  - Distribución automática de una clave de licencia

  o bien
- Kaspersky Security Center 14 Web Console:
  - Adición de una clave de licencia al repositorio del Servidor de administración
  - Distribución automática de una clave de licencia

Adición de un archivo clave o un código de activación al paquete de instalación de una aplicación administrada

Por motivos de seguridad, esta opción no se recomienda. El archivo clave o el código de activación añadidos a un paquete de instalación pueden verse comprometidos.

Si instala una aplicación administrada con un paquete de instalación, puede especificar un código de activación o un archivo clave en este paquete de instalación o en la directiva de la aplicación. La clave de licencia se desplegará en los dispositivos administrados en la próxima sincronización del dispositivo con el Servidor de administración.

Instrucciones:

- Consola de administración:
  - Creación de un paquete de instalación
  - Instalación de aplicaciones en dispositivos cliente

  o bien

- Kaspersky Security Center 14 Web Console: Agregar una clave a un paquete de instalación

Despliegue al ejecutar la tarea de añadir clave de licencia a una aplicación administrada

Si opta por usar la tarea *Agregar clave de licencia* a una aplicación administrada, puede elegir la clave de licencia que debe instalarse en los dispositivos y elegir los dispositivos con comodidad, por ejemplo, seleccionando un grupo de administración o una selección de dispositivos.

Antes del despliegue, se deben añadir el archivo clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Consola de administración:
  - Adición de una clave de licencia al repositorio del Servidor de administración
  - Despliegue de una clave de licencia en dispositivos cliente

  o bien
- Kaspersky Security Center 14 Web Console:
  - Adición de una clave de licencia al repositorio del Servidor de administración
  - Despliegue de una clave de licencia en dispositivos cliente

Adición de un código de activación o un archivo clave manualmente a los dispositivos

Puede activar la aplicación Kaspersky instalada localmente, usando las herramientas provistas en la interfaz de la aplicación. Por favor, consulte la documentación de la aplicación instalada.

Visualización de información sobre claves de licencias en uso

Para ver información sobre las claves de licencia en uso, realice lo siguiente,

En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.

El espacio de trabajo de la carpeta muestra una lista de las claves de licencia utilizadas en los dispositivos cliente.

Junto a cada una de las claves de licencia, se muestra un icono que corresponde al tipo de uso:

-  —se recibe información sobre la clave de licencia usada en ese momento desde un dispositivo cliente conectado al Servidor de administración. El archivo de esta clave de licencia se almacena fuera del Servidor de administración.
-  —La clave de licencia se almacena en el repositorio del Servidor de administración. La distribución automática se encuentra deshabilitada para esta clave de licencia.

-  —La clave de licencia se almacena en el repositorio del Servidor de administración. La distribución automática se encuentra habilitada para esta clave de licencia.

Puede ver información sobre qué claves de licencia se usan para la activación de la aplicación de un dispositivo cliente, si abre la sección **Aplicaciones** de la ventana de propiedades del dispositivo cliente.

Para definir la configuración actualizada de las claves de licencia del Servidor de administración virtual, este envía una solicitud a los servidores de activación de Kaspersky como mínimo una vez al día.

Adición de una clave de licencia al repositorio del Servidor de administración

Para añadir una clave de licencia al repositorio del Servidor de administración, realice lo siguiente:

1. En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.
2. Inicie la tarea de incorporación de claves de licencia mediante uno de los siguientes métodos:
   - Seleccione **Agregar código de activación o archivo clave** en el menú contextual de la lista claves de licencia.
   - Haga clic en el enlace **Agregar código de activación o archivo clave** en el espacio de trabajo de la lista de claves de licencia.
   - Haga clic en el botón **Agregar código de activación o archivo clave**.

   Se inicia Asistente para agregar claves de licencia.
3. Seleccione cómo desea activar el Servidor de administración: usando un código de activación o usando un archivo de clave.
4. Especifique su código de activación o un archivo de clave.
5. Selecciona la opción **Distribuir automáticamente la clave de licencia a los dispositivos administrados** si desea distribuir una clave de licencia relevante en su red inmediatamente. Si no selecciona esta opción, puede distribuir manualmente una clave de licencia más tarde.

   Como resultado, el archivo de clave se descarga y finaliza Asistente para agregar claves de licencia. Ahora, puede ver la clave de licencia añadida en la lista de licencias de Kaspersky.

Eliminación de una clave de licencia del Servidor de administración

Para eliminar una clave de licencia del Servidor de administración:

1. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
2. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Claves de licencia**.
3. Elimine la clave de licencia al hacer clic en el botón **Eliminar**.

De este modo se eliminará la clave de licencia.

Si se ha añadido una clave de licencia de reserva, la clave de licencia de reserva se convierte automáticamente en la clave de licencia activa después de eliminar la clave de licencia activa anterior.

Una vez eliminada la clave de licencia activa del Servidor de administración, Administración de vulnerabilidades y parches y Administración de dispositivos móviles dejan de estar disponibles. Puede volver a añadir una clave de licencia eliminada o bien otra nueva.

Despliegue de una clave de licencia en dispositivos cliente

Kaspersky Security Center permite distribuir una clave de licencia en los dispositivos cliente mediante la tarea de distribución de claves de licencia.

Para distribuir una clave de licencia en los dispositivos cliente, realice lo siguiente:

1. En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.
2. En el espacio de trabajo de la lista de claves de licencia, haga clic en el botón **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.

   Inicia el Asistente para crear tareas de activación de aplicaciones. Siga las instrucciones del Asistente.

Las tareas creadas mediante el Asistente para crear tareas de activación de aplicaciones son tareas para dispositivos específicos que se almacenan en la carpeta **Tareas** del árbol de consola.

Mediante el Asistente para la creación de tareas, también puede crear una tarea de distribución de claves de licencia local o de grupo para un grupo de administración o para un dispositivo cliente.

Distribución automática de una clave de licencia

Kaspersky Security Center permite la distribución automática de claves de licencias en dispositivos administrados si estas se encuentran en el repositorio de claves del Servidor de administración.

Para distribuir una clave de licencia automáticamente en dispositivos administrados:

1. En el árbol de consola, seleccione la carpeta **Licencias de Kaspersky**.
2. En el espacio de trabajo de la carpeta, seleccione la clave de licencia que desee para distribuir automáticamente a dispositivos.
3. Abra la ventana de propiedades de la clave de licencia seleccionada mediante una de las siguientes formas:
   - Seleccionando **Propiedades** en el menú contextual de la clave de licencia.
   - Haga clic en el enlace **Ver propiedades de la clave de licencia** en el cuadro de información de la clave de licencia seleccionada.
4. En la ventana de propiedades de la clave de licencia que se abre, seleccione la casilla **Distribuir automáticamente la clave de licencia a los dispositivos administrados**. Cierre la ventana de propiedades de

la clave de licencia.

La clave de licencia se distribuirá automáticamente a todos los dispositivos compatibles.

La distribución de claves de licencia se realiza por medio del Agente de red. No se crean tareas de distribución de clave de licencia para la aplicación.

Durante la distribución automática de una clave de licencia, se tiene en cuenta el límite del número de licencias que se pueden asignar a los dispositivos. (El límite de licencias está configurado en las propiedades de la clave de licencia). Si se alcanza el límite de licencias, esta clave de licencia se deja de distribuir automáticamente en dispositivos.

Si elige la casilla de verificación **Distribuir automáticamente la clave de licencia a los dispositivos administrados**, en la ventana de propiedades de la clave de licencia, se distribuye una clave de licencia en su red inmediatamente. Si no selecciona esta opción, puede distribuir manualmente una clave de licencia más tarde.

Creación y visualización de un informe de uso de claves de licencias

Para crear un informe de uso de claves de licencia en los dispositivos cliente, realice lo siguiente:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. Seleccione la plantilla del informe llamada **Informe de uso de claves de licencia** o cree una nueva plantilla de informe del mismo tipo.

El espacio de trabajo del informe de uso de claves de licencia muestra información acerca de las claves de licencia activas y claves de licencia de reserva utilizadas en los dispositivos cliente. El informe también contiene información sobre los dispositivos en los que se utilizan las claves de licencia y sobre las restricciones especificadas en las propiedades de estas claves de licencia.

Visualización de la información sobre las claves de licencia de la aplicación

Para saber las claves de licencia que están en uso para una aplicación de Kaspersky, haga lo siguiente:

1. En el árbol de consola de Kaspersky Security Center, seleccione el nodo **Dispositivos administrados** y vaya a la ficha **Dispositivos**.
2. Haga clic con el botón derecho del ratón para abrir el menú contextual del dispositivo relevante y seleccione **Propiedades**.
3. En la ventana de propiedades del dispositivo que se abre, seleccione la sección **Aplicaciones**.
4. En la lista de aplicaciones que aparece, seleccione la aplicación cuyas claves de licencia desea ver, y haga clic en el botón **Propiedades**.
5. En la ventana de propiedades de la aplicación que se abre, seleccione la sección **Claves de licencia**.

   La información se muestra en el espacio de trabajo de esta sección.

Configuración de protección de la red

En esta sección, encontrará información sobre la configuración manual de las directivas y las tareas, sobre las funciones del usuario y sobre la creación de una estructura de grupos de administración y jerarquía de tareas.

Escenario: Configuración de protección de la red

El Asistente de inicio rápido crea directivas y tareas con la configuración predeterminada. Estas configuraciones pueden resultar subóptimas o, incluso, inadmisibles para la organización. Por lo tanto, le recomendamos que ajuste estas directivas y tareas, y cree otras en caso de ser necesarias para su red.

Requisitos previos

Antes de comenzar, asegúrese de haber hecho lo siguiente:

- Instalado el Servidor de administración de Kaspersky Security Center 14
- Instalado Kaspersky Security Center 14 Web Console (opcional)
- Completado el escenario de instalación principal de Kaspersky Security Center
- Completado el Asistente de inicio rápido o creado manualmente las siguientes directivas y tareas en el grupo de administración de **Dispositivos administrados**:
  - Directiva de Kaspersky Endpoint Security
  - Tarea de grupo para actualizar Kaspersky Endpoint Security
  - Directiva del Agente de red
  - Tarea *Encontrar vulnerabilidades y actualizaciones requeridas*

La configuración de la protección de red se realiza en etapas:

1. **Configuración y propagación de directivas de aplicación Kaspersky y perfiles de directiva**

   Para configurar y propagar la configuración de las aplicaciones Kaspersky instaladas en los dispositivos administrados, puede utilizar dos enfoques de la gestión de la seguridad diferentes: centrada en el dispositivo o centrada en el usuario. Estos dos enfoques también se pueden combinar. Para implementar la Administración de seguridad centrada en el dispositivo, puede usar las herramientas proporcionadas en la Consola de administración basada en la Consola de administración de Microsoft o en Kaspersky Security Center 14 Web Console. La administración de la seguridad centrada en el usuario solamente se puede implementar a través de Kaspersky Security Center 14 Web Console.

2. **Configuración de tareas para la administración remota de aplicaciones Kaspersky**

   Verifique las tareas creadas con el Asistente de inicio rápido y afínelas, si es necesario.

   Instrucciones:

   - Consola de administración:

- Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
- Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas

- Kaspersky Security Center 14 Web Console:
  - Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
  - Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

Si es necesario, cree tareas adicionales para administrar las aplicaciones Kaspersky instaladas en los dispositivos cliente.

3. **La evaluación y la limitación del evento se cargan en la base de datos**

   Se transfiere la información sobre eventos durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se registra en la base de datos del Servidor de administración. Para reducir la carga en el Servidor de administración, evalúe y limite el número máximo de eventos que se pueden almacenar en la base de datos.

   Instrucciones:

   - Consola de administración: Establecer el número máximo de eventos
   - Kaspersky Security Center 14 Web Console: Configuración del número máximo de eventos

Resultados

Cuando complete este escenario, su red estará protegida gracias a la configuración de las aplicaciones de Kaspersky, tareas y eventos recibidos por el Servidor de administración:

- Las aplicaciones de Kaspersky se configuran de acuerdo con las directivas y los perfiles de directiva
- Las aplicaciones se administran a través de un conjunto de tareas
- Se establece el número máximo de eventos que se pueden almacenar en la base de datos

Cuando se completa la configuración de protección de la red, puede proceder a configurar actualizaciones periódicas de las bases de datos y aplicaciones de Kaspersky.

Para obtener detalles sobre cómo configurar las respuestas automáticas a las amenazas detectadas por Kaspersky Sandbox, consulte la Ayuda en línea de Kaspersky Sandbox 2.0.

Configuración y propagación de directivas: enfoque centrado en el dispositivo

Cuando complete este escenario, las aplicaciones se configurarán en todos los dispositivos administrados de acuerdo con las directivas de aplicación y los perfiles de directiva que defina.

Requisitos previos

Antes de comenzar, asegúrese de haber instalado con éxito el Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console (opcional) Si instaló Kaspersky Security Center 14 Web Console, es posible que también desee considerar la administración de seguridad centrada en el usuario como una opción alternativa o adicional al enfoque centrado en el dispositivo.

Etapas

El escenario de administración centrada en el dispositivo de las aplicaciones de Kaspersky consiste en los siguientes pasos:

1. **Configuración de directivas de aplicación**

   Configure los ajustes para las aplicaciones de Kaspersky instaladas en los dispositivos administrados mediante la creación de una directiva para cada aplicación. El conjunto de directivas se propagará a los dispositivos cliente.

   Cuando configura la protección de su red en el Asistente de inicio rápido, Kaspersky Security Center crea la directiva predeterminada para Kaspersky Endpoint Security para Windows. Si completó el proceso de configuración utilizando este Asistente, no tiene que crear una nueva directiva para esta aplicación. Vaya a la Configuración manual de la directiva de Kaspersky Endpoint Security.

   Si tiene una estructura jerárquica de varios Servidores de administración y/o grupos de administración, los Servidores de administración secundarios y los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios y los Servidores de administración secundarios para prohibir cualquier modificación de los parámetros configurados en la directiva ascendente. Si desea que solo una parte de la configuración se herede a la fuerza, puede bloquearla en la directiva ascendente. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas creada le permitirá administrar efectivamente los dispositivos en los grupos de administración.

   Instrucciones:

   - Consola de administración: Creación de una directiva
   - Kaspersky Security Center 14 Web Console: Crear una directiva

2. **Creación de perfiles de directivas (opcional)**

   Si desea que los dispositivos dentro de un solo grupo de administración se ejecuten bajo diferentes configuraciones de directivas, cree perfiles de directivas para esos dispositivos. Un perfil de directiva es un subconjunto de parámetros de la directiva denominado. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa en una condición específica denominada la *Condición de activación de perfil*. Los perfiles solo contienen parámetros que se diferencian de la directiva "básica", que está activa en el dispositivo administrado.

   Al utilizar las condiciones de activación del perfil, puede aplicar diferentes perfiles de directivas, por ejemplo, a los dispositivos ubicados en una unidad específica o grupo de seguridad de Active Directory, con configuración de hardware específica o marcados con etiquetas específicas. Utilice etiquetas para filtrar dispositivos que cumplan criterios específicos. Por ejemplo, puede crear una etiqueta llamada *Windows*, marcar todos los dispositivos que ejecutan el sistema operativo Windows con esta etiqueta y luego especificar esta etiqueta como condición de activación para un perfil de directiva. Como resultado, las aplicaciones de Kaspersky instaladas en todos los dispositivos que ejecutan Windows serán administradas por su propio perfil de directiva.

   Instrucciones:

   - Consola de administración:
     - Crear perfil de directiva
     - Creación de una regla de activación de perfil de directiva
   - Kaspersky Security Center 14 Web Console:

- Crear perfil de directiva
- Creación de una regla de activación de perfil de directiva

3. **Propagación de directivas y perfiles de directiva a los dispositivos administrados**

   De forma predeterminada, el Servidor de administración se sincroniza automáticamente con los dispositivos administrados cada 15 minutos. Durante la sincronización, las directivas nuevas o modificadas y los perfiles de directivas se propagan a los dispositivos administrados. Puede evitar la sincronización automática y ejecutar la sincronización manualmente utilizando el comando Forzar sincronización. Una vez que se complete la sincronización, las directivas y los perfiles de las directivas se entregan y aplican a las aplicaciones instaladas de Kaspersky.

   Si usa Kaspersky Security Center 14 Web Console, puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center especifica la fecha y la hora de entrega en las propiedades del dispositivo.

   Instrucciones:

   - Consola de administración: sincronización forzada
   - Kaspersky Security Center 14 Web Console: Forzar sincronización

Resultados

Cuando se completa el escenario centrado en el dispositivo, las aplicaciones de Kaspersky se configuran de acuerdo con la configuración especificada y propagada a través de la jerarquía de directivas.

Las directivas de aplicación configuradas y los perfiles de directivas se aplicarán automáticamente a los nuevos dispositivos añadidos a los grupos de administración.

Acerca de los enfoques de administración de seguridad centrados en el dispositivo y centrados en el usuario

Puede administrar la configuración de seguridad desde el punto de vista de las funciones del dispositivo y desde el punto de vista de los roles de usuario. El primer enfoque se denomina *administración de seguridad centrada en el dispositivo* y el segundo se denomina *administración de seguridad centrada en el usuario*. Para aplicar diferentes configuraciones de aplicaciones a diferentes dispositivos, puede usar uno o ambos tipos de administración en combinación. Para implementar la Administración de seguridad centrada en el dispositivo, puede usar las herramientas proporcionadas en la Consola de administración basada en la Consola de administración de Microsoft o en Kaspersky Security Center 14 Web Console. La administración de la seguridad centrada en el usuario solamente se puede implementar a través de Kaspersky Security Center 14 Web Console.

La administración de seguridad centrada en el dispositivo le permite aplicar distintas configuraciones de la aplicación de seguridad a los dispositivos administrados según las funciones específicas del dispositivo. Por ejemplo, puede aplicar distintas configuraciones a los dispositivos asignados en diferentes grupos de administración. También puede diferenciar los dispositivos según su uso en Active Directory o según sus especificaciones de hardware.

La administración de seguridad centrada en el usuario le permite aplicar distintas configuraciones de la aplicación de seguridad a diferentes funciones de usuario. Puede crear varias funciones de usuario, asignar una función de usuario adecuada para cada usuario y definir diferentes configuraciones de la aplicación para los dispositivos de usuarios con diferentes funciones. Por ejemplo, es posible que desee aplicar diferentes configuraciones de aplicaciones a los dispositivos de contadores y especialistas del departamento de recursos humanos (HR). Como resultado, cuando se implementa la administración de seguridad centrada en el usuario, cada departamento (el departamento de contabilidad y el departamento de recursos humanos) tiene su propia configuración de opciones para las aplicaciones de Kaspersky. Una configuración define qué opciones de la aplicación pueden cambiar los usuarios y cuáles impone y bloquea el administrador.

Al utilizar la administración de seguridad centrada en el usuario, puede aplicar configuraciones de aplicaciones específicas incluso para usuarios individuales. Esto puede ser necesario cuando un empleado tiene un rol único en la empresa o cuando desea monitorear incidentes de seguridad relacionados con dispositivos de una persona específica. Dependiendo de la función de este empleado en la empresa, puede ampliar o limitar los derechos de esta persona para cambiar la configuración de la aplicación. Por ejemplo, es posible que desee ampliar los derechos de un administrador del sistema que administra los dispositivos cliente en una oficina local.

También puede combinar los enfoques de administración de seguridad centrados en el dispositivo y centrados en el usuario. Por ejemplo, puede configurar una directiva de aplicación específica para cada grupo de administración y luego crear perfiles de directivas para una o varias funciones de usuario de su empresa. En este caso, las directivas y los perfiles de directiva se aplican en el siguiente orden:

1. Se aplican las directivas creadas para la administración de seguridad centrada en el dispositivo.
2. Son modificados por los perfiles de directiva de acuerdo con las prioridades del perfil de directiva.
3. Las directivas son modificadas por los perfiles de directiva asociados con roles de usuario.

Configuración manual de la directiva de Kaspersky Endpoint Security

Esta sección proporciona recomendaciones sobre cómo configurar la directiva de Kaspersky Endpoint Security, que es creada por el Asistente de inicio rápido. Puede realizar la configuración en la ventana de propiedades de la directiva.

Al modificar un ajuste de configuración, tenga en cuenta que debe hacer clic en el icono de bloqueo sobre el ajuste relevante a fin de permitir que se use su valor en una estación de trabajo.

Configuración de la directiva en la sección Protección avanzada contra amenazas

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Protección avanzada contra amenazas**, puede configurar el uso de Kaspersky Security Network para Kaspersky Endpoint Security para Windows. También puede configurar los módulos de Kaspersky Endpoint Security para Windows, como detección de comportamiento, prevención de exploits, prevención de intrusiones en el host y motor de reparación.

En la subsección **Kaspersky Security Network**, le recomendamos que active la opción **Usar proxy KSN**. Utilice esta opción para redistribuir y optimizar el tráfico en la red. También puede habilitar el uso de servidores KSN si el servicio Proxy KSN no está disponible. Los servidores de KSN pueden estar localizados en el lado de Kaspersky (cuando se usa KSN global) o en el lado de terceros (cuando se usa KSN privada).

Configuración de la directiva en la sección Protección frente a amenazas básicas

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

A continuación, se describen las acciones de configuración adicionales que recomendamos que realice en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Protección frente a amenazas básicas**.

Sección Protección frente a amenazas básicas, subsección Firewall

Compruebe la lista de redes en las propiedades de la directiva. La lista puede no contener todas las redes.

Para comprobar la lista de redes, siga estos pasos:

1. En las propiedades de la directiva, en la sección **Protección frente a amenazas básicas**, seleccione la subsección **Firewall**.
2. En la sección **Redes disponibles**, haga clic en el botón **Configuración**.

   De este modo, se abre la ventana **Firewall**. Esta ventana muestra la lista de redes en la ficha **Redes**.

Sección Protección frente a amenazas básicas, subdivisión Protección frente a amenazas en archivos

La activación del análisis de las unidades de red puede aplicar una carga significativa a las unidades de red. Resulta más cómodo realizar un análisis indirecto en los servidores de archivo.

Para desactivar el análisis de unidades de red:

1. En las propiedades de la directiva, en la sección **Protección frente a amenazas básicas**, seleccione la subsección **Protección frente a amenazas en archivos**.
2. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.
3. En la ventana **Protección frente a amenazas en archivos** que se abre, en la ficha **General**, desactive la casilla **Todas las unidades de red**.

Configuración de la directiva en la sección Configuración general

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

A continuación, se describen las acciones de configuración avanzadas que recomendamos realizar en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Configuración general**.

Sección Configuración general, subsección Informes y Almacenamiento

En la sección **Transferencia de datos al Servidor de administración**, tenga en cuenta la configuración siguiente:

Casilla **Acerca de las aplicaciones iniciadas**: si esta casilla está seleccionada, la base de datos del Servidor de administración guarda la información acerca de todas las versiones de todos los módulos de software en los dispositivos en red. Esta información puede requerir una cantidad significativa de espacio en el disco en la base de datos de Kaspersky Security Center (docenas de gigabytes). Por lo tanto, si la casilla **Acerca de las aplicaciones iniciadas** aún está seleccionada en la directiva de alto nivel, se debe borrar.

Sección Configuración general, subsección Interfaz

Si la protección antivirus en la red de la organización debe administrarse en el modo centralizado a través de la Consola de administración, debe desactivar la visualización de la interfaz de usuario de Kaspersky Endpoint Security para Windows en las estaciones de trabajo (al desactivar la casilla **Mostrar interfaz de la aplicación** en la sección **Interacción con el usuario**) y activar la protección con contraseña (al seleccionar la casilla **Activar protección con contraseña** en la sección **Protección de contraseñas**).

Configuración de la directiva en la sección Configuración de eventos

En la sección **Configuración de eventos**, debe desactivar el guardado de todos los eventos en el Servidor de administración, excepto los siguientes:

- En la ficha **Evento crítico**:
  - La ejecución automática de la aplicación está desactivada
  - Acceso denegado
  - Inicio de aplicación prohibido
  - La desinfección no es posible
  - Contrato de licencia violado
  - No se pudo cargar el módulo de cifrado
  - No se pueden iniciar dos tareas al mismo tiempo
  - Se detectó una amenaza activa. Iniciar Desinfección avanzada
  - Se detectó un ataque de red

- No todos los componentes fueron actualizados
- Error de activación
- Error al activar el modo portátil
- Error en la interacción con Kaspersky Security Center
- Error al desactivar el modo portátil
- Error al cambiar los componentes de la aplicación
- Error al aplicar las reglas de cifrado/descifrado del archivo
- La directiva no se puede aplicar
- El proceso finalizó
- Actividad de red bloqueada

- En la pestaña **Fallo operativo**: Configuración incorrecta de la tarea. Configuración no aplicada
- En la ficha **Advertencia**:
  - La autoprotección está desactivada
  - Clave de reserva incorrecta
  - El usuario ha decidido excluirse de la directiva de cifrado
- En la pestaña **Información**: Inicio de la aplicación prohibido en el modo de prueba

Configuración manual de la tarea de actualización de grupo para Kaspersky Endpoint Security

La opción de programación óptima y recomendada para Kaspersky Endpoint Security versiones 10 y posteriores es **Cuando se descargan nuevas actualizaciones en el repositorio** cuando la casilla de verificación **Usar un retraso aleatorio automático para el inicio de las tareas** está seleccionada.

Configuración manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security

El Asistente de inicio rápido crea una tarea de grupo para analizar un dispositivo. De forma predeterminada, se asigna a la tarea la programación **Ejecutar el viernes a las 7:00 p. m.** con asignación aleatoria automática y la casilla **Ejecutar tareas no realizadas** está desmarcada.

Esto significa que si los dispositivos de una organización se apagan, por ejemplo, los viernes a las 6:30 p.m., la tarea de análisis de los dispositivos nunca se ejecutará. Debe configurar la programación más cómoda para esta tarea según las reglas del lugar de trabajo adoptadas en la organización.

Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas

El Asistente de inicio rápido crea la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para el Agente de red. De forma predeterminada, se asigna a la tarea la programación **Ejecutar los martes a las 7:00 p. m.** con asignación aleatoria automática y la casilla **Ejecutar tareas no realizadas** está marcada.

Si las reglas del lugar de trabajo de la organización garantizan que todos los dispositivos se apagan en este momento, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará después de que los dispositivos se enciendan nuevamente, es decir, el miércoles por la mañana. Tal actividad puede ser indeseable porque un análisis de vulnerabilidades puede aumentar la carga en los subsistemas del disco y las CPU. Debe configurar la programación más cómoda para la tarea según las reglas del lugar de trabajo adoptadas en la organización.

Configuración manual de la tarea de grupo para la instalación de actualizaciones y la reparación de la vulnerabilidad

El Asistente de inicio rápido crea una tarea de grupo para la instalación de actualizaciones y la reparación de la vulnerabilidad para el Agente de red. De forma predeterminada, la tarea está configurada para ejecutarse todos los días a la 01:00 A.M., con asignación aleatoria automática y la opción **Ejecutar tareas pendientes** está desactivada.

Si las reglas del lugar de trabajo de la organización garantizan el apagado de dispositivos durante la noche, la instalación de las actualizaciones nunca se ejecutará. Debe configurar la programación más cómoda para la tarea de análisis de vulnerabilidades según las reglas del lugar de trabajo adoptadas en la organización. También es importante tener en cuenta que la instalación de actualizaciones puede requerir reiniciar el dispositivo.

Configuración del número máximo de eventos en el repositorio de eventos

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede editar la configuración del almacenamiento de eventos en la base de datos del Servidor de administración limitando el número de registros de eventos o el tiempo de almacenamiento de los registros. Cuando especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede usar este cálculo aproximado para evaluar si tiene suficiente espacio libre en el disco para evitar el desbordamiento de la base de datos. La capacidad predeterminada de la base de datos del Servidor de administración es de 400.000 eventos. La capacidad máxima recomendada de la base de datos es 45 millones de eventos.

Si el número de eventos en la base de datos llega al valor máximo especificado por el administrador, la aplicación elimina los eventos más antiguos sobrescribiéndolos con los nuevos. Cuando el Servidor de administración elimina eventos antiguos, no puede guardar eventos nuevos en la base de datos. Durante este período de tiempo, la información sobre los eventos que fueron rechazados se escribe en el Registro de eventos de Kaspersky. Los nuevos eventos se ponen en cola y luego se guardan en la base de datos una vez que se completa la operación de eliminación.

Para limitar la cantidad de eventos que se pueden almacenar en el repositorio de eventos en el Servidor de administración:

1. Haga clic con el botón derecho en el Servidor de administración y luego seleccione **Propiedades**.

Se abre la ventana Propiedades del Servidor de administración.

2. En el espacio de trabajo de la sección del **Repositorio de eventos**, especifique el número máximo de eventos almacenados en la base de datos.

3. Haga clic en **Aceptar**.

El número de eventos que se pueden almacenar en la base de datos está limitado al valor especificado.

Configuración del periodo máximo de almacenamiento de la información sobre las vulnerabilidades reparadas

Para establecer el periodo máximo de almacenamiento en la base de datos de la información sobre las vulnerabilidades que ya han sido corregidas en los dispositivos administrados:

1. Haga clic con el botón derecho en el Servidor de administración y luego seleccione **Propiedades**.

   Se abre la ventana Propiedades del Servidor de administración.

2. En el espacio de trabajo de la sección **Repositorio de eventos**, especifique el período máximo de almacenamiento de la información sobre las vulnerabilidades fijadas en la base de datos.

   De forma predeterminada, el periodo de almacenamiento es de 90 días.

3. Haga clic en **Aceptar**.

El periodo máximo de almacenamiento de la información sobre las vulnerabilidades reparadas se limita al número de días especificado. Después, la tarea de mantenimiento del Servidor de administración eliminará la información obsoleta de la base de datos.

Administración de tareas

Kaspersky Security Center administra las aplicaciones instaladas en los dispositivos mediante la creación y ejecución de varias tareas. Las tareas son necesarias para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software, y realizar otras acciones en las aplicaciones.

Las tareas se subdividen en los siguientes tipos:

- *Tareas de grupo*. Las tareas se realizan en los dispositivos del grupo de administración seleccionado.
- *Tareas del Servidor de administración*. Tareas que se realizan en el Servidor de administración.
- *Tareas para dispositivos específicos*. Tareas que se realizan en dispositivos seleccionados, sin tener en cuenta si se encuentran incluidos en algunos grupos de administración.
- *Tareas locales*. Tareas que se realizan en un dispositivo específico.

Una tarea de la aplicación solo puede crearse si el complemento de administración para dicha aplicación está instalado en la estación de trabajo del administrador.

Puede recopilar una lista de dispositivos para los que se debe crear una tarea mediante uno de los siguientes métodos:

- Seleccionando dispositivos de red detectados por el Servidor de administración.
- Especificando manualmente una lista de dispositivos. Puede utilizar una dirección IP (o un rango IP), un nombre NetBIOS o un nombre DNS como la dirección del dispositivo.
- Importe una lista de dispositivos desde un archivo .txt que contenga las direcciones de los dispositivos que deben añadirse (cada dirección debe ponerse en una línea individual).

  Si importa una lista de dispositivos desde un archivo o crea una manualmente y los dispositivos se identifican por sus nombres, la lista solo podrá contener aquellos dispositivos para los que la información ya se haya introducido en la base de datos del Servidor de administración a la hora de conectar los dispositivos o en el transcurso de una detección de dispositivos.

Para cada aplicación, se puede crear cualquier número de tareas de grupo, tareas para dispositivos específicos o tareas locales.

El intercambio de información sobre tareas entre una aplicación instalada en un dispositivo cliente y la base de datos de Kaspersky Security Center se lleva a cabo cuando el Agente de red se conecta al Servidor de administración.

Puede realizar cambios en la configuración de tareas, ver el progreso de las tareas y copiar, exportar, importar y eliminar tareas.

Las tareas se inician en un dispositivo solo si está en ejecución la aplicación para la que se creó la tarea. Cuando la aplicación no se está ejecutando, todas las tareas en ejecución se anulan.

Los resultados de tareas completadas se guardan en los registros de eventos de Microsoft Windows y Kaspersky Security Center, tanto de forma centralizada en el Servidor de administración, como de forma local en cada dispositivo.

No incluya datos confidenciales en la configuración de la tarea. Por ejemplo, no especifique la contraseña del administrador de dominio.

Datos de la administración de tareas para aplicaciones con soporte de arrendamiento múltiple

Una tarea de grupo para una aplicación con soporte de arrendamiento múltiple se aplica a la aplicación en función de la jerarquía de los Servidores de administración y de los dispositivos cliente. El Servidor de administración virtual desde el que se crea la tarea debe estar en el mismo grupo de administración o en un nivel inferior al del dispositivo cliente en el que está instalada la aplicación.

En los eventos que corresponden a los resultados de la ejecución de la tarea, se muestra al administrador del proveedor de servicios la información sobre el dispositivo en el que se ejecutó la tarea. Por el contrario, a la administración de un inquilino se le muestra el **Nodo multiinquilino**.

Creación de una tarea

En la Consola de administración, puede crear tareas directamente en la carpeta del grupo de administración para el que se va a crear una tarea de grupo o bien en el espacio de trabajo de la carpeta **Tareas**.

Para crear una tarea de grupo en la carpeta de un grupo de administración:

1. En el árbol de consola, seleccione el grupo de administración para el que desee crear una tarea.
2. En el espacio de trabajo del grupo, seleccione la ficha **Tareas**.
3. Ejecute la creación de tarea al hacer clic en el botón **Crear una tarea**.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

*Para crear una tarea en el espacio de trabajo de la carpeta **Tareas**:*

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. Ejecute la creación de la tarea haciendo clic en el botón **Finalizar**.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

No incluya datos confidenciales en la configuración de la tarea. Por ejemplo, no especifique la contraseña del administrador de dominio.

Creación de la tarea del Servidor de administración

El Servidor de administración lleva a cabo las siguientes tareas:

- Distribución automática de informes
- Descarga de actualizaciones al repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de bases de datos
- Sincronización de Windows Update
- Creación de un paquete de instalación basado en la imagen del SO de un dispositivo de referencia

En un Servidor de administración virtual solo están disponibles la tarea de envío automático del informe y la de creación del paquete de instalación de la imagen del SO del dispositivo de referencia. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas en el Servidor de administración principal. La copia de seguridad de los datos del Servidor de administración virtual se realiza junto con la copia de seguridad de los datos del Servidor de administración principal.

Para crear la tarea del Servidor de administración:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. Inicie la creación de la tarea por alguno de los siguientes medios:

   - Seleccione **Nuevo** → **Tarea** en el menú contextual de la carpeta **Tareas** en el árbol de la consola.

- Haga clic en el botón **Crear una tarea** en el espacio de trabajo de la carpeta **Tareas**.

Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

Las tareas Descargar actualizaciones en el repositorio del Servidor de administración, Sincronizar Windows Update, Mantenimiento de bases de datos y *Copia de seguridad de los datos del Servidor de administración* solo se pueden crear una vez. Si las tareas *Descargar actualizaciones en el repositorio del Servidor de administración*, *Mantenimiento de bases de datos*, *Copia de seguridad de los datos del Servidor de administración* y *Sincronizar Windows Update* ya se han creado para el Servidor de administración, estas no aparecen en la ventana de la selección del tipo de tarea del Asistente para añadir tareas.

Creación de una tarea para dispositivos específicos

En Kaspersky Security Center se pueden crear tareas para dispositivos específicos. Los dispositivos ubicados en un conjunto se pueden incluir en varios grupos de administración o estar fuera de cualquier grupo de administración. Kaspersky Security Center puede realizar las siguientes tareas principales para dispositivos específicos:

- Instalar una aplicación en remoto
- Enviar mensaje al usuario
- Cambiar Servidor de administración
- Administrar dispositivos
- Verificar actualizaciones
- Distribuir paquetes de instalación
- Instalar una aplicación de forma remota en Servidores de administración secundarios
- Desinstalar aplicación en remoto

Para crear una tarea para dispositivos específicos:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. Inicie la creación de la tarea por alguno de los siguientes medios:
   - Seleccione **Nuevo** → **Tarea** en el menú contextual de la carpeta **Tareas** en el árbol de la consola.
   - Haga clic en el botón **Crear una tarea** en el espacio de trabajo de la carpeta **Tareas**.

Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

Creación de una tarea local

Para crear una tarea local para un dispositivo:

1. Seleccione la ficha **Dispositivos** en el espacio de trabajo del grupo que incluye el dispositivo cliente.
2. En la lista de dispositivos de la ficha **Dispositivos**, seleccione el dispositivo para el que hay que crear una tarea local.
3. Cree la tarea para el dispositivo seleccionado con uno de los siguientes métodos:
   - Haga clic en el botón **Realizar acción** y seleccione **Crear una tarea** en la lista desplegable.
   - Haga clic en el enlace **Crear una tarea** en el espacio de trabajo del dispositivo.
   - Use las propiedades del dispositivo de la forma siguiente:
     a. En el menú contextual del dispositivo, seleccione **Propiedades**.
     b. En la ventana de propiedades del dispositivo que se abra, seleccione la sección **Tareas** y haga clic en **Agregar**.

Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

En las Guías de las respectivas aplicaciones Kaspersky se proporcionan instrucciones detalladas sobre la creación y configuración de tareas locales.

Visualización de tareas de grupo heredadas en el espacio de trabajo de un grupo anidado

Para habilitar las tareas heredadas de un grupo anidado en el espacio de trabajo:

1. Seleccione la ficha **Tareas** en el espacio de trabajo del grupo anidado.
2. En el espacio de trabajo de la ficha **Tareas**, haga clic en el botón **Mostrar tareas heredadas**.

Las tareas heredadas se mostrarán en la lista de tareas con uno de los siguientes iconos:

-  — Si se han heredado de un grupo creado en el Servidor de administración principal.
-  — Si se han heredado de un grupo de nivel superior.

Si se habilita el modo herencia, las tareas heredadas solo se pueden editar en el grupo en el que se crearon. Las tareas heredadas no se pueden editar en el grupo que hereda las tareas.

Encendido automático de dispositivos antes de iniciar una tarea

Kaspersky Security Center no ejecuta tareas en dispositivos que están apagados. Mediante la función Wake-on-LAN, puede configurar Kaspersky Security Center para que encienda estos dispositivos automáticamente antes de iniciar una tarea.

Para configurar el encendido automático de dispositivos antes de iniciar una tarea:

1. En la ventana propiedades de la tarea, seleccione la sección **Programación**.
2. Para configurar las acciones en dispositivos, haga clic en el enlace **Avanzado**.
3. En la ventana **Avanzado** que se abre, marque la casilla **Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea (min)** y a continuación, especifique el intervalo de tiempo en minutos.

Como resultado, durante la cantidad de minutos especificada antes de iniciar la tarea, Kaspersky Security Center enciende los dispositivos y carga el sistema operativo en ellos mediante la función Wake-on-LAN. Una vez completada la tarea, los dispositivos se apagan automáticamente si los usuarios del dispositivo no inician sesión en el sistema. Tenga en cuenta que Kaspersky Security Center apaga automáticamente solo los dispositivos que se encienden mediante la función Wake-on-LAN.

Kaspersky Security Center puede iniciar los sistemas operativos automáticamente solo en los dispositivos compatibles con el estándar Wake-on-LAN (WoL).

Apagado automático de un dispositivo después de completar una tarea

Kaspersky Security Center le permite configurar una tarea para que los dispositivos en los cuales se ha distribuido se apaguen automáticamente una vez finalizada la tarea.

Apagado automático de un dispositivo después de completar una tarea:

1. En la ventana propiedades de la tarea, seleccione la sección **Programación**.
2. Haga clic en el enlace **Avanzado** para abrir la ventana diseñada para configurar acciones en dispositivos.
3. En la ventana que se abre **Avanzado**, seleccione la casilla de verificación **Apagar los dispositivos después de completar la tarea**.

Limitación del tiempo de ejecución de la tarea

Para limitar el tiempo de ejecución de una tarea en dispositivos:

1. En la ventana propiedades de la tarea, seleccione la sección **Programación**.
2. Haga clic en el enlace **Avanzado** para abrir la ventana diseñada para configurar las acciones en los dispositivos cliente.
3. En la ventana **Avanzado** que se abre, seleccione la casilla de verificación **Detener la tarea si tarda más de (min)** y especifique el intervalo de tiempo en minutos.

Si la tarea aún no se ha completado en el dispositivo cliente cuando termine el intervalo de tiempo, Kaspersky Security Center detendrá automáticamente la ejecución de la tarea.

Exportación de una tarea

Se pueden exportar a un archivo tareas de grupo y tareas para dispositivos específicos. Las tareas del Servidor de administración y las tareas locales no se pueden exportar.

Para exportar una tarea:

1. En el menú contextual de la tarea, seleccione **Todas las tareas → Exportar**.
2. En la ventana **Guardar como** que se abre, especifique la ruta del nombre de archivo.
3. Haga clic en el botón **Guardar**.

Los derechos de los usuarios locales no se exportan.

Importación de una tarea

Se pueden importar tareas de grupo y tareas para dispositivos específicos. Las tareas del Servidor de administración y las tareas locales no se pueden importar.

Para importar una tarea:

1. Seleccione la lista a la que se debe importar la tarea:
   - Si quiere importar la tarea a la lista de tareas de grupo, seleccione la ficha **Tareas** en el espacio de trabajo del grupo de administración requerido.
   - Si quiere importar una tarea a la lista de tareas para dispositivos específicos, seleccione la carpeta **Tareas** en el árbol de consola.
2. Seleccione una de las opciones siguientes para importar la tarea:
   - En el menú contextual de la lista de tareas, seleccione **Todas las tareas → Importar**.
   - Haga clic en el enlace **Importar tarea desde archivo** en el bloque de administración de la lista de tareas.
3. En la ventana que se abre, especifique la ruta del archivo del que quiere importar la tarea.
4. Haga clic en el botón **Abrir**.

   La tarea se muestra en la lista de tareas.

Si una tarea con un nombre idéntico al de la tarea recién importada ya existe en la lista seleccionada, el índice **(<siguiente número secuencial>)** se añade al nombre de la tarea importada, por ejemplo: **(1)**, **(2)**.

Conversión de tareas

Se puede utilizar Kaspersky Security Center para convertir tareas de versiones anteriores de las aplicaciones Kaspersky en otras de versiones más actualizadas de esas aplicaciones.

La conversión está disponible para las tareas de las siguientes aplicaciones:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 para Windows
- Kaspersky Endpoint Security 10 para Windows

Para convertir tareas:

1. Del árbol de consola seleccione el Servidor de administración para el que quiera convertir las tareas.
2. En el menú contextual del Servidor de administración, seleccione **Todas las tareas → Asistente de conversión por lotes de directivas y tareas**.

Se inicia el Asistente de conversión por lotes de directivas y tareas. Siga las instrucciones del Asistente.

Cuando el Asistente complete su operación, se habrán creado tareas nuevas, que utilizarán los parámetros de las tareas de versiones anteriores de las aplicaciones.

Inicio y detención manual de una tarea

Puede iniciar y detener tareas manualmente de las siguientes maneras: desde el menú contextual de la tarea o en la ventana de propiedades del dispositivo cliente al cual se le ha asignado esta tarea.

Solo se permite iniciar tareas de grupo desde el menú contextual del dispositivo cliente a los usuarios que se encuentren incluidos en el grupo **KLAdmins**.

Siga estos pasos para iniciar o detener una tarea en el menú contextual de la ventana de propiedades de la propia tarea:

1. Elija una tarea de la lista de tareas.
2. Inicie o detenga la tarea por alguno de los medios siguientes:
   - Seleccione **Iniciar** o **Detener** en el menú contextual de la tarea.
   - Haciendo clic en **Iniciar** o **Detener** en la sección **General** de la ventana de propiedades de la tarea.

Par iniciar o detener una tarea en el menú contextual de la ventana de propiedades del dispositivo cliente:

1. Elija un dispositivo de la lista de dispositivos.
2. Inicie o detenga la tarea por alguno de los medios siguientes:
   - Seleccionando **Todas las tareas → Ejecutar una tarea** en el menú contextual del dispositivo. Seleccione la tarea pertinente de la lista de tareas.

     La lista de dispositivos a los que se ha asignado la tarea se sustituirá por el dispositivo que haya seleccionado. Se iniciará la tarea.
   - Haciendo clic en el botón  o  en la sección **Tareas** de la ventana de propiedades del dispositivo.

Suspensión y reanudación manual de una tarea

Para pausar o reanudar la ejecución de una tarea manualmente:

1. Elija una tarea de la lista de tareas.
2. Suspenda o reanude la tarea mediante uno de los siguientes métodos:
   - Seleccione **Pausar** o **Reanudar** en el menú contextual de la tarea.
   - En la ventana propiedades de la tarea, seleccione la sección **General** y haga clic en **Pausar** o **Reanudar**.

Supervisión de la ejecución de tareas

Para supervisar la ejecución de la tarea,

en la ventana propiedades de la tarea, seleccione la sección **General**.

en la parte central de la sección **General** se muestra el estado actual de la tarea.

Visualización de los resultados de ejecución de la tarea almacenados en el Servidor de administración

Kaspersky Security Center le permite visualizar los resultados de la ejecución de las tareas de grupo, tareas para dispositivos específicos y tareas del Servidor de administración. No se pueden visualizar los resultados de ejecución de las tareas locales.

Para visualizar los resultados de tarea:

1. En la ventana propiedades de la tarea, seleccione la sección **General**.
2. Haga clic en el enlace **Resultados** para abrir la ventana **Resultados de tarea**.

Configuración del filtrado de información sobre los resultados de ejecución de una tarea

Kaspersky Security Center le permite filtrar la información sobre los resultados de ejecución de tareas de grupo, tareas para dispositivos específicos y tareas del Servidor de administración. No está disponible el filtrado para las tareas locales.

Para configurar el filtrado de información sobre los resultados de ejecución de una tarea:

1. En la ventana propiedades de la tarea, seleccione la sección **General**.

2. Haga clic en el enlace **Resultados** para abrir la ventana **Resultados de tarea**.

   La tabla de la parte superior contiene una lista de todos los dispositivos a los que se ha asignado la tarea. La tabla de la parte inferior muestra los resultados de la tarea realizada en el dispositivo seleccionado.

3. Haga clic con el botón secundario del ratón en la tabla pertinente para abrir el menú contextual y seleccionar **Filtro**.

4. En la ventana **Establecer filtro** que se abre, defina la configuración del filtro en las secciones **Eventos**, **Dispositivos** y **Hora**. Haga clic en **Aceptar**.

La ventana **Resultados de tarea** mostrará la información que cumpla los parámetros especificados en el filtro.

Modificar una tarea Revertir cambios

Para modificar una tarea:

1. En el árbol de consola, seleccione la carpeta **Tareas**.

2. En el espacio de trabajo de la carpeta **Tareas**, seleccione una tarea y vaya a la ventana de propiedades de la tarea usando el menú contextual.

3. Haga los cambios relevantes.

   > En la sección **Exclusiones de la cobertura de la tarea** puede configurar la lista de subgrupos a los que no se aplicará la tarea.

4. Haga clic en **Aplicar**.

Los cambios de la tarea se guardarán en la ventana de propiedades de la tarea, en la sección **Historial de revisiones**.

Puede revertir los cambios hecho a una tarea, si es necesario.

Para revertir los cambios hechos a una tarea:

1. En el árbol de consola, seleccione la carpeta **Tareas**.

2. Seleccione la tarea cuyos cambios hay que revertir y vaya a la ventana de propiedades de la tarea usando el menú contextual.

3. En la ventana propiedades de la tarea, seleccione la sección **Historial de revisiones**.

4. En la lista de revisiones de tareas, seleccione el número de la revisión a la que quiere revertir los cambios.

5. Haga clic en el botón **Avanzado** y seleccione el valor **Revertir** en la lista desplegable.

Comparación de tareas

Puede comparar tareas del mismo tipo: por ejemplo, puede comparar dos tareas de análisis antivirus, pero no puede comparar una tarea de análisis antivirus y una tarea de instalación de actualización. Después de la comparación, tiene un informe que muestra qué configuración de las tareas coincide y qué configuración difiere. Puede imprimir el informe de la comparación de la tarea o guardarlo como un archivo. Puede necesitar la comparación de tareas cuando se asignan varias tareas del mismo tipo a departamentos diferentes de una empresa. Por ejemplo, los empleados del departamento de contabilidad tienen una tarea de análisis antivirus solo en los discos locales de sus dispositivos, mientras que los empleados del departamento de ventas se comunican con clientes y, por tanto, tienen una tarea de análisis tanto de discos locales como de correo electrónico. No tiene que ver toda la configuración de la tarea para observar rápidamente tal diferencia; puede simplemente comparar las tareas.

Solo se pueden comparar tareas del mismo tipo.

Las tareas solo se pueden comparar en pares.

Puede comparar tareas de una de estas formas: seleccionando una tarea y comparándola con la otra, o comparando cualquiera de las dos tareas desde la lista de tareas.

Para seleccionar una tarea y compararla con la otra:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. En el espacio de trabajo de la carpeta **Tareas**, seleccione la tarea que desea comparar con la otra.
3. En el menú contextual de la tarea, seleccione **Todas las tareas** → **Comparar con otra tarea**.
4. En la ventana **Elija una tarea**, seleccione la tarea para la comparación.
5. Haga clic en **Aceptar**.

   Se muestra un informe en formato HTML que compara las dos tareas.

Para comparar dos tareas desde la lista de tareas:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. En la carpeta **Tareas**, en la lista de tareas, pulse la tecla **Mayús** o **Ctrl** para seleccionar dos tareas del mismo tipo.
3. En el menú contextual, seleccione **Comparar**.

   Se muestra un informe en formato HTML que compara las tareas seleccionadas.

Cuando se comparan las tareas, si las contraseñas difieren, se muestran asteriscos (******) en el informe de comparación de la tarea.

Si se modificó la contraseña en las propiedades de la tarea, se muestran asteriscos (******) en el informe de comparación de la revisión (******).

Cuentas para iniciar tareas

Puede especificar una cuenta en la que se ejecutará la tarea.

Por ejemplo, para realizar una tarea de análisis a petición, es necesario que disponga de privilegios de acceso sobre los objetos que se están analizando, y para llevar a cabo una tarea de actualización, necesita privilegios de usuario autorizado para el servidor proxy. La capacidad de especificar una cuenta para la ejecución de la tarea le permite evitar problemas con las tareas de análisis a petición y de actualización en caso de que el usuario que ejecuta la tarea no tenga los derechos de acceso necesarios.

Durante la ejecución de las tareas de instalación o desinstalación remotas, la cuenta especificada se utiliza para descargar a los dispositivos cliente los archivos requeridos para instalar o desinstalar una aplicación en caso de que no se haya instalado o no esté disponible el Agente de red. Si el Agente de red está instalado y disponible, la cuenta se utiliza si, de conformidad con la configuración de las tareas, la entrega de archivos se realiza mediante utilidades de Microsoft Windows exclusivamente desde una carpeta compartida. En este caso, la cuenta debe tener los siguientes permisos en el dispositivo:

- El permiso para ejecutar aplicaciones de forma remota.
- El permiso para usar el recurso Admin$.
- El permiso para *Iniciar sesión como Servicio*.

Si los archivos se envían a los dispositivos cliente mediante el Agente de red, no se usará la cuenta. Todas las operaciones de copia e instalación de archivos las realiza el **Agente de red** (**Cuenta LocalSystem**).

Asistente para cambiar contraseñas de tareas

Para una tarea no local, puede especificar una cuenta en la que se debe ejecutar la tarea. Puede especificar la cuenta durante la creación de la tarea o en las propiedades de una tarea existente. Si la cuenta especificada se usa de acuerdo con las instrucciones de seguridad de la organización, estas instrucciones pueden requerir cambiar la contraseña de la cuenta de vez en cuando. Cuando la contraseña de la cuenta caduca y establece una nueva, las tareas no se iniciarán hasta que especifique la nueva contraseña válida en las propiedades de la tarea.

El Asistente para cambiar contraseñas de tareas le permite reemplazar automáticamente la contraseña anterior por la nueva en todas las tareas en las que se especifica la cuenta. Alternativamente, puede hacerlo manualmente en las propiedades de cada tarea.

Para iniciar el Asistente para cambiar contraseñas de tareas:

1. En el árbol de consola, seleccione el nodo **Tareas**.
2. En el menú contextual del nodo, seleccione **Asistente para cambiar contraseñas de tareas**.

   Siga las instrucciones del Asistente.

Paso 1. Especificar credenciales

En los campos **Cuenta** y **Contraseña**, especifique nuevas credenciales que sean válidas actualmente en su sistema (por ejemplo, en Active Directory). Cuando cambia al siguiente paso del Asistente, Kaspersky Security Center verifica si el nombre de cuenta especificado coincide con el nombre de cuenta en las propiedades de cada tarea no local. Si los nombres de las cuentas coinciden, la contraseña en las propiedades de la tarea se reemplazará automáticamente por la nueva.

Si completa el campo **Contraseña anterior (opcional)**, Kaspersky Security Center reemplaza la contraseña solo para aquellas tareas en las que se encuentran tanto el nombre de la cuenta como la contraseña anterior. El reemplazo se realiza automáticamente. En todos los demás casos, debe elegir una acción para realizar el siguiente paso del Asistente.

Paso 2. Seleccionar una acción para realizar

Si no ha especificado la contraseña anterior en el primer paso del Asistente o si la contraseña anterior especificada no coincide con las contraseñas en las tareas, debe elegir una acción para las tareas encontradas.

Para cada tarea que tiene el estado *Debe aprobarse*, decida si desea eliminar la contraseña en las propiedades de la tarea o reemplazarla por la nueva. Si elige eliminar la contraseña, la tarea cambia para ejecutarse con la cuenta predeterminada.

Paso 3. Ver los resultados

En el último paso del Asistente, vea los resultados de cada una de las tareas encontradas. Para completar el Asistente, haga clic en el botón **Finalizar**.

Creación de una jerarquía de grupos de administración subordinados al Servidor de administración virtual

Una vez creado el Servidor de administración virtual, este contiene de forma predeterminada un grupo de administración llamado **Dispositivos administrados**.

El procedimiento de creación de una jerarquía de grupos de administración subordinados al Servidor de administración virtual es el mismo que para la creación de una jerarquía de grupos de administración subordinados al Servidor de administración físico.

No puede añadir Servidores de administración secundarios y virtuales a los grupos de administración subordinados a un Servidor de administración virtual. Esto se debe a limitaciones de los Servidores de administración virtuales.

Directivas y perfiles de directivas

En Kaspersky Security Center 14 Web Console, puede crear directivas para las aplicaciones de Kaspersky. Esta sección describe las directivas y los perfiles de directivas, y proporciona instrucciones para crearlos y modificarlos.

Jerarquía de directivas, uso de perfiles de directiva

Esta sección proporciona información sobre cómo aplicar directivas a dispositivos en grupos de administración. Esta sección también proporciona información sobre los perfiles de la directiva admitidos en Kaspersky Security Center, que comienza en la versión 10 Service Pack 1.

Jerarquía de directivas

En Kaspersky Security Center, se usan directivas para definir un conjunto único de opciones en varios dispositivos. Por ejemplo, la cobertura de la directiva de la aplicación P definida para el grupo de administración G incluye dispositivos administrados con la aplicación P instalada que se hayan desplegado en el grupo G y todos sus subgrupos, excepto los subgrupos en los que la casilla **Heredar del grupo primario** esté desactivada en las propiedades.

Una directiva se diferencia de cualquier parámetro local por iconos de bloqueo (🔒) al lado de su parámetro. Si un parámetro (o un grupo de parámetros) está bloqueado en las propiedades de la directiva, debe usar, en primer lugar, este parámetro (o el grupo de parámetros) al crear la configuración efectiva y, en segundo lugar, debe escribir el parámetro o el grupo de parámetros en la directiva hacia abajo.

La creación de parámetros efectivos en un dispositivo se puede describir de la forma siguiente: los valores de todos los parámetros que no se han bloqueado se toman de la directiva, luego, se sobrescriben con los valores de los parámetros locales y, luego, la recopilación se sobrescribe con los valores de los parámetros bloqueados tomados de la directiva.

Las directivas de la misma aplicación se afectan mutuamente mediante la jerarquía de los grupos de administración: los parámetros Bloqueados de la directiva ascendente sobrescriben los mismos parámetros de la directiva descendente.

Existe una directiva especial para los usuarios fuera de la oficina. Esta directiva entra en vigor en un dispositivo cuando el dispositivo cambia a modo fuera de la oficina. Las directivas fuera de la oficina no afectan otras directivas mediante la jerarquía de grupos de administración.

La directiva fuera de la oficina no se admitirá en versiones posteriores de Kaspersky Security Center. Los perfiles de directiva se utilizarán en vez de directivas fuera de la oficina.

Perfiles de directiva

Aplicar directivas a dispositivos solo a través de la jerarquía de los grupos de administración puede ser incómodo en muchas circunstancias. Puede que sea necesario crear varias instancias de una sola directiva que se diferencie en uno o dos parámetros para diferentes grupos de administración y sincronizar el contenido de esas directivas en el futuro.

Para ayudarle a evitar tales problemas, Kaspersky Security Center, a partir de la versión 10 Service Pack 1, admite *perfiles de directiva*. Un perfil de directiva es un subconjunto de parámetros de la directiva denominado. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa en una condición específica denominada la *Condición de activación de perfil*. Los perfiles solo contienen parámetros que se diferencian de la directiva "básica", que está activa en el dispositivo cliente (equipo o dispositivo móvil). Al activarse un perfil se modifica la configuración de directiva que se encontraba activa en el dispositivo antes de que se activara el perfil. Esa configuración toma los valores especificados en el perfil.

Actualmente se imponen las siguientes restricciones en perfiles de directiva:

- Una directiva puede incluir un máximo de 100 perfiles.
- Un perfil de directiva no puede contener otros perfiles.
- Un perfil de directiva no puede contener configuraciones de notificación.

Contenido de un perfil

Un perfil de directiva contiene las siguientes partes constituyentes:

- Los perfiles de nombre con nombres idénticos se afectan mutuamente mediante la jerarquía de los grupos de administración con reglas comunes.
- Subconjunto de configuración de la directiva. A diferencia de la directiva, que contiene todos los parámetros, un perfil solo contiene los parámetros que realmente se requieren (parámetros bloqueados).
- La condición de activación es una expresión lógica con las propiedades del dispositivo. Un perfil está activo (complementa la directiva) solo cuando la condición de activación de perfil es verdadera. En todos los demás casos, el perfil es inactivo y se ignora. Las siguientes propiedades del dispositivo se pueden incluir en esa expresión lógica:
  - Estado de modo fuera de la oficina.
  - Propiedades de entorno de la red — Nombre de la regla activa para la conexión de Agente de red.
  - Presencia o ausencia de etiquetas específicas en el dispositivo.
  - Ubicación del dispositivo en una unidad de Active Directory: explícita (el dispositivo está en la UO especificada) o implícita (el dispositivo está en una UO, que está dentro de la UO especificada en cualquier nivel de anidamiento).
  - Pertenencia del dispositivo al grupo de seguridad de Active Directory (explícita o implícita).
  - Pertenencia del propietario del dispositivo al grupo de seguridad de Active Directory (explícita o implícita).
- Casilla de desactivación del perfil. Los perfiles desactivados siempre se ignoran y sus respectivas condiciones de activación no se verifican.
- Prioridad del perfil. Las condiciones de activación de diferentes perfiles son independientes, por lo tanto, es posible activar varios perfiles simultáneamente. Si los perfiles activos contienen recopilaciones no superpuestas de parámetros, no surgirán problemas. Sin embargo, si dos perfiles activos contienen valores diferentes del mismo parámetro, se producirá una ambigüedad. Esta ambigüedad se debe evitar a través de prioridades del perfil: el valor de la variable ambigua se tomará del perfil que tiene la prioridad más alta (el que tenga el valor más alto en la lista de perfiles).

Comportamiento de los perfiles cuando las directivas se afectan mutuamente mediante la jerarquía

Los perfiles con el mismo nombre se fusionan según las reglas de fusión de directivas. Los perfiles de una directiva hacia arriba tienen una prioridad más alta que los perfiles de una directiva hacia abajo. Si se prohíbe la modificación de parámetros en la directiva hacia arriba (están bloqueados), la directiva hacia abajo usa las condiciones de activación de perfil de la directiva hacia arriba. Si se permite la modificación de parámetros en la directiva hacia arriba, se utilizan las condiciones de activación de perfil de la directiva hacia abajo.

Ya que un perfil de directiva puede contener la propiedad **El dispositivo está desconectado** en su condición de activación, los perfiles reemplazan completamente la función de directivas para los usuarios fuera de la oficina, que ya no se admitirán.

Una directiva para los usuarios fuera de la oficina puede contener perfiles, pero sus perfiles solo se pueden activar después de que el dispositivo cambia al modo fuera de la oficina.

Herencia de los ajustes de directivas

Una directiva se especifica para un grupo de administración. La configuración de la directiva se puede *heredar*, es decir, la pueden recibir los subgrupos (grupos secundarios) del grupo de administración para el que se estableció la configuración originalmente. En adelante, también se hará referencia a una directiva para un grupo primario como *directiva primaria*.

Puede activar o desactivar dos opciones de herencia: **Heredar configuración de la directiva primaria** y **Forzar la herencia de la configuración en las directivas secundarias**:

- Si activa **Heredar configuración de la directiva primaria** para una directiva secundaria y bloquea parámetros de la directiva primaria, no podrá cambiar esos parámetros para el grupo secundario. Pero sí podrá cambiar los parámetros que no estén bloqueados en la directiva primaria.

- Si desactiva **Heredar configuración de la directiva primaria** para una directiva secundaria, podrá cambiar toda la configuración del grupo secundario, incluso si hay parámetros bloqueados en la directiva primaria.

- Si activa **Forzar la herencia de la configuración en las directivas secundarias** en el grupo primario, se activará **Heredar configuración de la directiva primaria** para cada directiva secundaria. En este caso, no puede desactivar esta opción para ninguna directiva secundaria. Todos los parámetros de configuración bloqueados en la directiva primaria se heredan obligatoriamente en los grupos secundarios y no puede cambiarlos en esos grupos.

- En directivas para el grupo **Dispositivos administrados**, la opción **Heredar configuración de la directiva primaria** no afecta a ningún parámetro, porque el grupo **Dispositivos administrados** no tiene grupos en dirección ascendente y por lo tanto no hereda ninguna directiva.

De forma predeterminada, la opción **Heredar configuración de la directiva primaria** está activada para directivas nuevas.

Si una directiva tiene perfiles, todas las directivas secundarias heredan estos perfiles.

Administrar directivas

Las aplicaciones instaladas en los dispositivos cliente se configuran de manera centralizada mediante la definición de directivas.

Las directivas creadas en un grupo de administración, para aplicaciones, se muestran en la ficha **Directivas** del espacio de trabajo. Delante del nombre de cada directiva se muestra un icono con su estado.

Después de eliminar o revocar una directiva, la aplicación seguirá trabajando con los parámetros especificados en la directiva. Estos parámetros pueden modificarse manualmente más tarde.

Una directiva se aplica del siguiente modo: si un dispositivo cliente está ejecutando tareas residentes (tareas de protección en tiempo real), estas tareas seguirán funcionando con los nuevos valores de configuración. Cualquier tarea periódica iniciada (análisis a petición, actualización de las bases de datos de la aplicación) se mantendrá en ejecución con los mismos valores. La próxima vez, se ejecutará con los nuevos valores de configuración.

Las directivas para aplicaciones con soporte de arrendamiento múltiple se heredan a grupos de administración de nivel inferior así como a grupos de administración de nivel superior: la directiva se propaga a todos los dispositivos cliente en los que está instalada la aplicación.

Si los Servidores de administración están organizados en una estructura jerárquica, los Servidores de administración secundarios reciben las directivas del Servidor de administración principal y las distribuyen a los dispositivos cliente. Cuando se permite la herencia, la configuración de la directiva puede modificarse en el Servidor de administración principal. Después, cualquier cambio realizado en los parámetros de la directiva se propaga a las directivas heredadas en los Servidores de administración secundarios.

Si finaliza la conexión entre los Servidores de administración principal y secundario, la directiva en el Servidor secundario continúa con los parámetros aplicados. Los parámetros de la directiva modificados en el Servidor de administración principal se distribuyen a un Servidor de administración secundario una vez que se restablezca la conexión.

Si se deshabilita la herencia, la configuración de la directiva puede modificarse en un Servidor de administración secundario, independientemente del Servidor de administración principal.

Si se interrumpe la conexión entre un Servidor de administración y un dispositivo cliente, el dispositivo cliente empezará a trabajar con la directiva fuera de la oficina (si está definida) o la directiva seguirá usando los parámetros aplicados hasta que se restablezca la conexión.

Los resultados de la distribución de la directiva en el Servidor de administración secundario se muestran en la ventana de propiedades de la directiva de la consola del Servidor de administración principal.

Los resultados de la distribución de directivas a los dispositivos cliente se muestran en la ventana de propiedades de la directiva del Servidor de administración al que están conectados.

No use datos confidenciales en la configuración de la directiva. Por ejemplo, no especifique la contraseña del administrador de dominio.

Creación de una directiva

En la Consola de administración, puede crear directivas directamente en la carpeta del grupo de administración para el que se crea la directiva o bien en el espacio de trabajo de la carpeta **Directivas**.

Para crear una directiva en la carpeta de un grupo de administración:

1. En el árbol de consola, seleccione el grupo de administración para el que quiera crear una directiva.
2. En el espacio de trabajo del grupo, seleccione la tabla **Directivas**.
3. Ejecute el Asistente de nueva directiva; para ello, haga clic en el botón **Nueva directiva**.

   Se inicia el Asistente de nueva directiva. Siga las instrucciones del Asistente.

*Para crear una directiva en el espacio de trabajo de la carpeta **Directivas**:*

1. En el árbol de consola, seleccione la carpeta **Directivas**.
2. Ejecute el Asistente de nueva directiva; para ello, haga clic en el botón **Nueva directiva**.

   Se inicia el Asistente de nueva directiva. Siga las instrucciones del Asistente.

Se pueden crear varias directivas para una aplicación del grupo, pero solo puede activarse una directiva a la vez. Cuando se crea una nueva directiva activa, la anterior se desactiva.

Al crear una directiva, puede especificar un conjunto mínimo de parámetros requeridos para que la aplicación funcione correctamente. El resto de valores se establecen de manera predeterminada y corresponden a los valores aplicados en la instalación local de la aplicación. La directiva se puede cambiar después de su creación.

No use datos confidenciales en la configuración de la directiva. Por ejemplo, no especifique la contraseña del administrador de dominio.

Los parámetros de las aplicaciones de Kaspersky, modificados después de haber aplicado las directivas, se describen en detalle en sus Guías respectivas.

Una vez creada la directiva, los parámetros cuya modificación esté bloqueada (indicados por el icono de cerradura) entrarán en vigor en los dispositivos cliente, sin tener en cuenta qué ajustes se hayan especificado anteriormente para la aplicación.

Visualización de la directiva heredada en un subgrupo

Para habilitar la visualización de directivas heredadas en un grupo de administración anidado:

1. En el árbol de consola seleccione el grupo de administración del que se mostrarán las directivas heredadas.
2. En el espacio de trabajo del grupo seleccionado, seleccione la ficha **Directivas**.
3. En el menú contextual de la lista de directivas, seleccione **Ver** → **Directivas heredadas**.

Las directivas heredadas se mostrarán en la lista de directivas con el siguiente icono:

- — Si se han heredado de un grupo creado en el Servidor de administración principal.
- — Si se han heredado de un grupo de nivel superior.

Al habilitar el modo herencia de configuración, las directivas heredadas solo se pueden modificar en el grupo en el que se crearon. La modificación de las directivas heredadas no está disponible en el grupo que las heredó.

Activación de una directiva

Para activar una directiva para un grupo seleccionado:

1. En el espacio de trabajo del grupo, en la ficha **Directivas**, seleccione la directiva que necesite activar.
2. Para activas la directiva, realice una de las siguientes acciones:
   - En el menú contextual de la directiva, seleccione **Directiva activa**.
   - En la ventana de propiedades de la directiva, abra la sección **General** y seleccione **Directiva activa** del grupo de parámetros **Estado de la directiva**.

Se activa la directiva para el grupo de administración seleccionado.

Cuando una directiva se aplica a un gran número de dispositivos cliente, tanto la carga del Servidor de administración como el tráfico de red se incrementan de forma significativa durante por algún tiempo.

Activación automática de una directiva en el evento Brote de virus

Para que una directiva realice la activación automática en el evento Brote de virus:

1. En la ventana propiedades del Servidor de administración, abra la sección **Brote de virus**.
2. Abra la ventana **Activación de directiva** haciendo clic en el enlace **Configurar directivas para activar cuando se produce un evento de brote de virus** y añada la directiva a la lista seleccionada de directivas que se activan cuando se detecta un brote de virus.

Si se activa una directiva en el evento *Brote de virus*, la única forma de volver a la directiva anterior es mediante el modo manual.

Aplicación de una directiva fuera de la oficina

La directiva fuera de la oficina entra en vigor en un dispositivo cuando se desconecta de la red empresarial.

Para aplicar una directiva fuera de la oficina, haga lo siguiente:

En la ventana de propiedades de la directiva, abra la sección **General** y en el grupo de la configuración **Estado de la directiva**, seleccione **Directiva fuera de la oficina**.

La directiva fuera de la oficina se aplica a los dispositivos si están desconectados de la red corporativa.

Modificación de una directiva. Revertir cambios

Para modificar una directiva, siga estos pasos:

1. En el árbol de consola, seleccione la carpeta **Directivas**.
2. En el espacio de trabajo de la carpeta **Directivas**, seleccione una directiva y vaya a la ventana de propiedades de la directiva usando el menú contextual.
3. Haga los cambios relevantes.
4. Haga clic en **Aplicar**.

Los cambios hechos a la directiva se guardarán en las propiedades de la directiva, en la sección **Historial de revisiones**.

Puede revertir los cambios hechos a la directiva, si es necesario.

Para revertir los cambios hechos a la directiva:

1. En el árbol de consola, seleccione la carpeta **Directivas**.
2. Seleccione la directiva cuyos cambios hay que revertir y vaya a la ventana de propiedades de la directiva usando el menú contextual.
3. En la ventana de propiedades de la directiva, seleccione la ficha **Historial de revisiones**.
4. En la lista de revisiones de la directiva, seleccione el número de la revisión a la que quiere revertir los cambios.
5. Haga clic en el botón **Avanzado** y seleccione el valor **Revertir** en la lista desplegable.

Comparación de directivas

Puede comparar dos directivas para una sola aplicación administrada. Después de la comparación, tiene un informe que muestra qué configuración de la directiva coincide y qué configuración difiere. Por ejemplo, puede tener que comparar directivas si diferentes administradores en sus oficinas respectivas han creado varias directivas para una sola aplicación administrada, o si una sola directiva de alto nivel ha sido heredada por todas las oficinas locales y se ha modificado para cada oficina. Puede comparar directivas de una de estas formas: al seleccionar una directiva y al compararla con la otra, o al comparar cualquiera de las dos directivas desde la lista de directivas.

Comparar una directiva con otra:

1. En el árbol de consola, seleccione la carpeta **Directivas**.
2. En el espacio de trabajo de la carpeta **Directivas**, seleccione la directiva que necesita comparar con la otra.
3. En el menú contextual de la directiva, seleccione **Comparar la directiva con otra directiva**.
4. En la ventana **Seleccionar directiva**, seleccione la directiva con la cual su directiva se debe comparar.
5. Haga clic en **Aceptar**.

Un informe en formato HTML se muestra para la comparación de las dos directivas para la misma aplicación.

Para comparar dos directivas desde la lista de directivas:

1. En la carpeta **Directivas**, en la lista de directivas, use la tecla **`Mayús`** o **`Ctrl`** para seleccionar dos directivas para una sola aplicación administrada.
2. En el menú contextual, seleccione **Comparar**.

Un informe en formato HTML se muestra para la comparación de las dos directivas para la misma aplicación.

El informe sobre la comparación de la configuración de directivas para Kaspersky Endpoint Security para Windows también proporciona detalles de la comparación de perfiles de directivas. Puede minimizar los resultados de la comparación de perfiles de directivas. Para minimizar la sección, haga clic en el icono al lado del nombre de la sección.

Eliminación de una directiva

Para eliminar una directiva:

1. En el espacio de trabajo de un grupo de administración, en la ficha **Directivas** seleccione la directiva que necesite eliminar.
2. Elimine la directiva mediante alguno de los siguientes métodos:
   - Seleccionando **Eliminar** en el menú contextual de la directiva.
   - Haga clic en el enlace **Eliminar directiva** en el cuadro de información para la directiva seleccionada.

Copia de una directiva

Para copiar una directiva:

1. Seleccione una directiva en el espacio de trabajo del grupo requerido en la ficha **Directivas**.
2. En el menú contextual de la directiva, seleccione **Copiar**.
3. En el árbol de consola, seleccione el grupo al que quiera agregar la directiva.

   Puede agregar una directiva al grupo del cual se copió.
4. En el menú contextual de la lista de directivas del grupo seleccionado, en la ficha **Directivas**, seleccione **Pegar**.

La directiva se copiará con todos los parámetros y se aplicará a los dispositivos del grupo en los que se las ha copiado. Si pega la directiva en el mismo grupo desde el cual se copió, el índice **(<siguiente número secuencial>)** se agrega automáticamente al nombre de la directiva; por ejemplo, **(1)**, **(2)**.

Una directiva activa se desactiva mientras se está copiando. Si fuera necesario, se puede activar.

Exportación de una directiva

Para exportar una directiva:

1. Exporte una directiva por alguno de los siguientes medios:
   - Seleccionando **Todas las tareas** → **Exportar** en el menú contextual de la directiva.
   - Haga clic en el enlace **Exportar directiva al archivo** en el cuadro de información para la directiva seleccionada.
2. En la ventana **Guardar como** que se abre, especifique la ruta y el nombre del archivo de la directiva. Haga clic en el botón **Guardar**.

Importación de una directiva

Para importar una directiva:

1. En el espacio de trabajo del grupo relevante, en la ficha **Directivas**, seleccione uno de los siguientes métodos de importación de directivas:

   - Mediante la selección de **Todas las tareas** → **Importar** en el menú contextual de la lista de directivas.
   - Haga clic en el botón **Importar directiva desde archivo** en el bloque administrativo para la lista de directiva.

2. En la ventana que se abre, especifique la ruta del archivo del que quiere importar la directiva. Haga clic en el botón **Abrir**.

A continuación, la directiva se muestra en la lista de directivas.

Si en la lista de directivas existe una con un nombre idéntico al de la directiva recién importada, el nombre de la directiva importada se ampliará con el índice **(<siguiente número secuencial>)**; por ejemplo: **(1)**, **(2)**.

Conversión de directivas

Kaspersky Security Center puede convertir directivas de versiones anteriores de las aplicaciones Kaspersky en otras más actualizadas para esas mismas aplicaciones.

La conversión está disponible para las directivas de las siguientes aplicaciones:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4.
- Kaspersky Endpoint Security 8 para Windows.
- Kaspersky Endpoint Security 10 para Windows.

Para convertir directivas:

1. En el árbol de consola, seleccione el Servidor de administración para el que quiera convertir las directivas.
2. En el menú contextual del Servidor de administración, seleccione **Todas las tareas** → **Asistente de conversión por lotes de directivas y tareas**.

Se inicia el Asistente de conversión por lotes de directivas y tareas. Siga las instrucciones del Asistente.

Cuando el Asistente finalice, se habrán creado directivas nuevas, que utilizarán los parámetros de las directivas de versiones anteriores de las aplicaciones Kaspersky.

Administración de perfiles de directivas

Esta sección describe la gestión de perfiles de directivas y proporciona información sobre cómo ver los perfiles de una directiva, cambiar la prioridad de un perfil de directiva, crear un perfil de directiva, modificar un perfil de directiva, copiar un perfil de directiva, crear una regla de activación de perfil de directiva y eliminar un perfil de directiva.

Acerca del perfil de directiva

Un perfil de directiva es un conjunto determinado de parámetros de configuración de una directiva que se activa en un dispositivo cliente (dispositivo o dispositivo móvil) cuando el dispositivo cumple reglas de activación especificadas. Al activarse un perfil se modifica la configuración de directiva que se encontraba activa en el dispositivo antes de que se activara el perfil. Esa configuración toma los valores especificados en el perfil.

Los perfiles de directiva tienen la finalidad de que los dispositivos de un único grupo de administración se ejecuten bajo distintas configuraciones de directiva. Por ejemplo, podría ser preciso modificar una configuración de directiva para algunos dispositivos de un grupo de administración. En este caso, puede configurar perfiles para dicha directiva que permitan modificar la configuración de la directiva para dispositivos concretos en el grupo de administración. Por ejemplo, la directiva prohíbe la ejecución de cualquier software de navegación GPS en todos los dispositivos del grupo de administración de usuarios. El software de navegación GPS solo hace falta en un dispositivo del grupo de administración de usuarios: el perteneciente al usuario que realiza las tareas de mensajería. Puede etiquetar ese dispositivo como “Mensajería” y vuelva a configurar el perfil de directiva de modo que permita la ejecución del software de navegación GPS únicamente en el dispositivo etiquetado como “Mensajería” a la vez que se mantienen los demás parámetros de la directiva. En este caso, si hay un dispositivo etiquetado como “Mensajería” en el grupo de administración de Usuarios, se le permitirá ejecutar el software de navegación GPS. Pero la ejecución del software de navegación GPS seguirá estando prohibida en otros dispositivos del grupo de administración de usuarios a menos que también se etiqueten como “Mensajería”.

Solo las siguientes directivas admiten perfiles:

- Directivas de Kaspersky Endpoint Security 10 Service Pack 1 para Windows o posterior.
- Directivas de Kaspersky Endpoint Security 10 Service Pack 1 for Mac.
- Directivas del complemento de Kaspersky Mobile Device Management desde la versión 10 Service Pack 1 hasta la versión 10 Service Pack 3 Maintenance Release 1.
- Directivas del complemento de Kaspersky Device Management for iOS.
- Directivas de Kaspersky Security for Virtualization 5.1 Light Agent para Windows.
- Directivas de Kaspersky Security for Virtualization 5.1 Light Agent para Linux.

Los perfiles de directiva simplifican la administración de dispositivos cliente a los que se aplican las directivas:

- La configuración del perfil de directiva puede ser distinta de la configuración de la directiva.
- No tiene que mantener ni aplicar manualmente varias instancias de una única directiva que difiera solo en algunos ajustes.
- No tiene que asignar una directiva aparte para los usuarios que estén fuera de la oficina.
- Puede exportar e importar perfiles de directiva, así como crear nuevos perfiles de directiva basados en perfiles existentes.
- Una misma directiva puede tener varios perfiles de directiva activos. Solo se aplicarán a ese dispositivo los perfiles que cumplan las reglas de activación vigentes en el dispositivo.
- Los perfiles están sujetos a la jerarquía de directiva. Una directiva heredada incluye todos los perfiles de la directiva del nivel más alto.

Prioridades de perfiles

Los perfiles que se han creado para una directiva se clasifican en orden descendente de prioridad. Por ejemplo, si el perfil X está en una posición de la lista de perfiles superior a la posición del perfil Y, el perfil X tiene una prioridad más alta que el Y. Se pueden aplicar simultáneamente varios perfiles a un mismo dispositivo. Si los valores de un parámetro varían en perfiles diferentes, se aplicará al dispositivo el valor del perfil con prioridad más alta.

Reglas de activación de perfil

Un perfil de directiva se activa en un dispositivo cliente cuando se aplica una regla de activación. Las *Reglas de activación* son un conjunto de condiciones que, al cumplirse, inician el perfil de directiva en un dispositivo. Una regla de activación puede incluir estas condiciones:

- Agente de red de un dispositivo cliente se conecta con el Servidor de administración con un conjunto dado de parámetros de conexión, como la dirección del Servidor de administración, el número de puerto, etc.
- El dispositivo cliente está desconectado.
- Se ha asignado etiquetas específicas al dispositivo cliente.
- El dispositivo cliente se encuentra ubicado explícitamente (el dispositivo se ubica inmediatamente en la unidad especificada) o implícitamente (el dispositivo se ubica en una unidad que está en la unidad especificada en cualquier nivel de anidamiento) en una unidad concreta de Active Directory®; el dispositivo o su propietario se encuentran ubicados en un grupo de seguridad de Active Directory.
- El dispositivo cliente pertenece a un determinado propietario o el propietario del dispositivo está incluido en un grupo de seguridad interno de Kaspersky Security Center.
- Al propietario del dispositivo cliente se le ha asignado un rol específico.

Directivas en la jerarquía de grupos de administración

Si va a crear una directiva en un grupo de administración de nivel bajo, esta nueva directiva hereda todos los perfiles de la directiva activa en el grupo de nivel más alto. Los perfiles con nombres idénticos se combinan. Los perfiles de directiva para el grupo de nivel superior tienen la prioridad más alta. Por ejemplo, en el grupo de administración *A*, la directiva *P(A)* tiene los perfiles *X1*, *X2* y *X3* (en orden descendente de prioridad). En el grupo de administración *B*, que es un subgrupo del grupo *A*, la directiva *P(B)* se ha creado con los perfiles *X2*, *X4* y *X5*. A continuación, se modificará la directiva *P(B)* con la directiva *P(A)* de modo que la lista de perfiles de la directiva *P(B)* quedará así: *X1*, *X2*, *X3*, *X4*, *X5* (en orden decreciente de prioridad). La prioridad del perfil *X2* dependerá del estado inicial de *X2* de la directiva *P(B)* y *X2* de la directiva *P(A)*. Después de crearse la directiva *P(B)*, la directiva *P(A)* deja de mostrarse en el subgrupo *B*.

La directiva activa se recalcula cada vez que inicia el Agente de red, habilita y deshabilita el modo sin conexión o modifica la lista de etiquetas asignadas al dispositivo cliente. Por ejemplo, el tamaño de RAM se ha aumentado en el dispositivo, y eso ha activado el perfil de directiva aplicable a dispositivos con tamaño de RAM grande.

Propiedades y restricciones de los perfiles de directiva

Los perfiles tienen estas propiedades:

- Los perfiles de una directiva inactiva no influyen en absoluto en los dispositivos cliente.
- Si se establece una directiva en el estado **Directiva fuera de la oficina**, los perfiles de la directiva también se aplicarán cuando se desconecte un dispositivo de la red corporativa.

- Los perfiles no admiten el análisis estático de acceso a archivos ejecutables.
- Un perfil de directiva no puede contener parámetros de notificaciones de evento.
- Si se utiliza el puerto UDP 15000 para conectar un dispositivo al Servidor de administración, el perfil de directiva correspondiente se activa en el plazo de un minuto tras asignar una etiqueta al dispositivo.
- Puede usar reglas para la conexión entre el Agente de red y el Servidor de administración al crear reglas de activación de perfil de directiva.

Crear perfil de directiva

Solo se pueden crear perfiles para las directivas de las siguientes aplicaciones:

- Kaspersky Endpoint Security 10 Service Pack 1 para Windows y versiones posteriores
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Complemento Kaspersky Mobile Device Management 10, con Service Pack 1-10 y Service Pack 3 Maintenance Release 1
- Complemento de Kaspersky Device Management for iOS
- Kaspersky Security for Virtualization 5.1 Light Agent para Windows y Linux

Crear perfil de directiva:

1. En el árbol de consola, seleccione el grupo de administración para cuya directiva desee crear un perfil de directiva.
2. En el espacio de trabajo del grupo de administración, seleccione la ficha **Directivas**.
3. Seleccione una directiva y vaya a la ventana de propiedades de la directiva mediante el menú contextual.
4. Abra la sección **Perfiles de directiva** en la ventana de propiedades de la directiva y haga clic en el botón **Agregar**.

   Se ejecutará el Asistente para nuevo perfil de directiva.
5. En la ventana **Nombre de perfil de directiva** del Asistente, especifique lo siguiente:

   a. Nombre del perfil de directiva

      El nombre de un perfil no puede tener más de 100 caracteres.

   b. Estado de perfil de la directiva (*Activado* o *Desactivado*)

      Recomendamos que cree y active perfiles de directiva inactivos solo después de que haya terminado con la configuración y las condiciones de la activación del perfil de directiva.
6. Seleccione la casilla de verificación **Después de cerrar el nuevo Asistente de perfiles de directivas, proceda a configurar la regla de activación de perfiles de directivas** para iniciar el Asistente de nueva regla de activación de perfil de directiva. Siga los pasos del Asistente.
7. Edite la configuración del perfil de la directiva en la ventana de propiedades del perfil de directiva, de la manera que lo requiera.

8. Guarde los cambios haciendo clic en **Aceptar**.

   El perfil se guarda. El perfil se activará en los dispositivos que cumplan las reglas de activación.

Puede crear varios perfiles para una única directiva. Los perfiles que se han creado para una directiva se muestran en las propiedades de la directiva, en la sección **Perfiles de directiva**. Puede modificar un perfil de directiva y cambiar la prioridad del perfil, así como eliminar el perfil.

Modificación de un perfil de directiva

Modificación de la configuración de un perfil de directiva

La capacidad de editar un perfil de directiva solo está disponible para las directivas de Kaspersky Endpoint Security para Windows.

Para modificar un perfil de directiva, siga estos pasos:

1. En el árbol de consola, seleccione el grupo de administración cuyo perfil de directiva se tenga que modificar.
2. En el espacio de trabajo del grupo, seleccione la tabla **Directivas**.
3. Seleccione una directiva y vaya a la ventana de propiedades de la directiva mediante el menú contextual.
4. Abra la sección **Perfiles de directiva** en las propiedades de la directiva.

   Esta sección contiene una lista de perfiles que se han creado para la directiva. Los perfiles aparecen en la lista según sus prioridades.
5. Seleccione un perfil de directiva y haga clic en el botón **Propiedades**.
6. Configure el perfil en la ventana de propiedades:
   - Si fuera necesario, cambie en la sección **General** el nombre del perfil y habilite o deshabilite el perfil con la casilla de verificación **Activar perfil**.
   - En la sección **Reglas de activación**, modifique las reglas de activación del perfil.
   - Modifique la configuración de la directiva en las secciones correspondientes.
7. Haga clic en **Aceptar**.

La configuración que ha modificado se aplicará después de que el dispositivo se sincronice con el Servidor de administración (si el perfil de directiva está activo) o cuando se active una regla de activación (si el perfil de directiva no está activo).

Cambio de la prioridad de un perfil de directiva

La prioridad de los perfiles de directiva determina el orden de activación de los perfiles de un dispositivo cliente. Se recurre a las prioridades si se establecen reglas de activación idénticas para distintos perfiles de directiva.

Por ejemplo, en el caso de que se hayan creado dos perfiles de directiva: *Perfil 1* y *Perfil 2*, que difieren en los respectivos valores del mismo ajuste (*Valor 1* y *Valor 2*). La prioridad del *Perfil 1* es superior a la del *Perfil 2*. También hay otros perfiles con prioridades inferiores a la del *Perfil 2*. Las reglas de activación de esos perfiles son idénticas.

Cuando se aplica una regla de activación, se activará el *Perfil 1*. El ajuste del dispositivo utilizará el *Valor 1*. Si elimina el *Perfil 1*, el *Perfil 2* tendrá la prioridad más alta, de modo que el ajuste utilizará el *Valor 2*.

En la lista de perfiles de directiva, los perfiles se muestran de acuerdo con sus respectivas prioridades. El perfil con la prioridad más alta se coloca primero. Puede cambiar la prioridad de un perfil usando los siguientes botones:  y  .

Eliminación de un perfil de directiva

Para eliminar un perfil de directiva, siga estos pasos:

1. En el árbol de consola, seleccione el grupo de administración del que desee eliminar un perfil de directiva.
2. En el espacio de trabajo del grupo de administración, seleccione la ficha **Directivas**.
3. Seleccione una directiva y vaya a la ventana de propiedades de la directiva mediante el menú contextual.
4. Abra la sección **Perfiles de directiva** en las propiedades de la directiva de Kaspersky Endpoint Security.
5. Seleccione el perfil de directiva que desea eliminar y haga clic en el botón **Eliminar**.

De este modo se eliminará el perfil de la directiva. El estado activo pasará, o bien a otro perfil de directiva cuyas reglas de activación se aplican en el dispositivo, o bien a la directiva.

Creación de una regla de activación de perfil de directiva

Para crear una regla de activación de perfil de directiva:

1. En el árbol de consola, seleccione el grupo de administración para el que tenga que crear un perfil de directiva.
2. En el espacio de trabajo del grupo, seleccione la tabla **Directivas**.
3. Seleccione una directiva y vaya a la ventana de propiedades de la directiva mediante el menú contextual.
4. Seleccione la sección **Perfiles de directiva** en la ventana de propiedades de la directiva.
5. Seleccione el perfil de la directiva para el cual tiene que crear una regla de activación, y haga clic en el botón **Propiedades**.

   Se abre la ventana de propiedades de perfiles de directiva.

   Si la lista de perfiles de directiva está vacía, puede crear un perfil de directiva.
6. Seleccione la sección **Reglas de activación**, y haga clic en el botón **Agregar**.

   Se inicia el Asistente de nueva regla de activación de perfil de directiva.
7. En la ventana **Reglas de activación de perfiles de directivas**, seleccione las casillas al lado de las condiciones que deben afectar a la activación del perfil de la directiva que está creando:

   - Reglas generales de activación de perfiles de directivas

Seleccione esta casilla para configurar reglas de activación de perfiles de directiva del dispositivo según el estado del modo desconectado del dispositivo, la regla para la conexión con el Servidor de administración y las etiquetas asignadas al dispositivo.

- **Reglas para el uso de Active Directory**

  Seleccione esta casilla para configurar reglas de activación de un perfil de directiva en el dispositivo según la presencia del dispositivo en una unidad organizativa de Active Directory, o la pertenencia del dispositivo (o su propietario) a un grupo de seguridad de Active Directory.

- **Reglas para un propietario del dispositivo específico**

  Seleccione esta casilla para configurar reglas para la activación del perfil de la directiva en el dispositivo según el propietario del dispositivo.

- **Reglas para especificaciones de hardware**

  Seleccione esta casilla para configurar reglas de activación del perfil de la directiva en el dispositivo según el volumen de memoria y el número de procesadores lógicos.

El número de ventanas adicionales del Asistente depende de la configuración que seleccione en este paso. Puede modificar las reglas de activación de perfil de la directiva más adelante.

8. En la ventana **Condiciones generales**, especifique la siguiente configuración:

   - En el campo **El dispositivo está desconectado**, en la lista desplegable especifique la condición de la presencia del dispositivo en la red:

     - **Sí**

       El dispositivo está en una red externa, lo que significa que el Servidor de administración no está disponible.

     - **No**

       El dispositivo está en la red, lo que significa que el Servidor de administración está disponible.

     - **No se ha seleccionado ningún valor**

       No se aplica el criterio.

   - En el cuadro **El dispositivo se encuentra en la ubicación de red especificada**, use las listas desplegables para configurar la activación del perfil de la directiva si la regla de conexión del Servidor de administración se ejecuta/no se ejecuta en este dispositivo:

     - **Ejecutado (=) / No ejecutado (#)**

       La condición de la activación del perfil de directiva (si la regla se ejecuta o no).

- Nombre de regla

  Descripción de la ubicación de la red del dispositivo para la conexión con el Servidor de administración, cuyas condiciones se deben cumplir (o no se debe cumplir) para la activación del perfil de la directiva.

  Se puede crear o configurarse una descripción de la ubicación de la red de dispositivos para la conexión con un Servidor de administración en una regla de conmutación de Agente de red.

Se muestra la ventana **Condiciones generales** si la casilla **Reglas generales de activación de perfiles de directivas** está seleccionada.

9. En la ventana **Las condiciones que utilizan etiquetas**, especifique la siguiente configuración:

   - Lista de etiquetas

     En la lista de etiquetas, puede especificar la regla para incluir dispositivos en el perfil de la directiva seleccionando las casillas junto a las etiquetas correspondientes.

     Puede añadir nuevas etiquetas a la lista al introducirlas en el campo sobre la lista y hacer clic en el botón **Añadir**.

     El perfil de la directiva incluye los dispositivos con descripciones que contienen todas las etiquetas seleccionadas. El criterio no se aplica si las casillas están vacías. De forma predeterminada, estas casillas están en blanco.

   - Aplicar a los dispositivos que no tengan etiquetas especificadas

     Active esta opción si tiene que cambiar su selección de etiquetas.

     Si se selecciona esta opción, el perfil de la directiva incluirá los dispositivos con descripciones que no contengan ninguna de las etiquetas seleccionadas. Si esta opción está desactivada, el software no se actualiza.

     Esta opción está desactivada de forma predeterminada.

   La ventana **Las condiciones que utilizan etiquetas** se muestra si la casilla de verificación **Reglas generales de activación de perfiles de directivas** está seleccionada.

10. En la ventana **Condiciones que utilizan Active Directory**, especifique la siguiente configuración:

    - Pertenencia del propietario del dispositivo en el grupo de seguridad de Active Directory

      Si se selecciona esta opción, el perfil de directiva se activa en el dispositivo cuyo propietario pertenece al grupo de seguridad especificado. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

    - Pertenencia del dispositivo al grupo de seguridad de Active Directory

      Si se selecciona esta opción, el perfil de directiva se activa en el dispositivo. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

    - Asignación de dispositivos en la unidad organizativa de Active Directory

Si se selecciona esta opción, se activa el perfil de directiva en el dispositivo, que se incluye en la unidad organizativa de Active Directory especificada. Si esta opción está desactivada, el criterio de activación del perfil no se aplica.

Esta opción está desactivada de forma predeterminada.

La ventana **Condiciones que utilizan Active Directory** se muestra si la casilla de verificación **Reglas para el uso de Active Directory** está seleccionada.

11. En la ventana **Condiciones que utilizan el propietario del dispositivo**, especifique la siguiente configuración:

- Propietario del dispositivo

  Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según su propietario. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

  - El dispositivo pertenece al propietario especificado (símbolo "=").
  - El dispositivo no pertenece al propietario especificado (símbolo "#").

    Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar el propietario del dispositivo cuando la opción está activada. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

- El propietario del dispositivo está incluido en un grupo de seguridad interna

  Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según la pertenencia del propietario del dispositivo a un grupo interno de seguridad de Kaspersky Security Center. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

  - El propietario del dispositivo es un miembro del grupo de seguridad especificado (símbolo "=").
  - El propietario del dispositivo no es un miembro del grupo de seguridad especificado (símbolo "#").

    Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar un grupo de seguridad de Kaspersky Security Center. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

- Activar perfil de directiva según rol del propietario del dispositivo

  Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según la función del propietario. Añada la función de manera manual desde la lista de funciones existentes.

  Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado.

La ventana **Condiciones que utilizan el propietario del dispositivo** se abre si la casilla de verificación **Reglas para un propietario del dispositivo específico** está seleccionada.

12. En la ventana **Condiciones que utilizan especificaciones del equipo**, especifique la siguiente configuración:

- Tamaño de RAM, en MB

Active esta opción para configurar y activar la regla de activación de perfil en el dispositivo según el volumen de RAM disponible en ese dispositivo. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

- El tamaño de la RAM del dispositivo es menor que el valor especificado (signo "<").
- El tamaño de la RAM del dispositivo es mayor que el valor especificado (signo ">").

Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar el volumen de RAM en el dispositivo. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

- Número de procesadores lógicos

Active esta opción de verificación para configurar y activar la regla de activación de perfil en el dispositivo según el número de procesadores lógicos de dicho dispositivo. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

- El número de procesadores lógicos en el dispositivo es menor o igual que el valor especificado (signo "<").
- El número de procesadores lógicos en el dispositivo es mayor o igual que el valor especificado (signo ">").

Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar la cantidad de procesadores lógicos en el dispositivo. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

La ventana **Condiciones que utilizan especificaciones del equipo** se muestra si la casilla de verificación **Reglas para especificaciones de hardware** está seleccionada.

13. En la ventana **Nombre de la regla de activación de perfiles de directivas**, en el campo **Nombre de la regla**, especifique un nombre para la regla.

El perfil se guardará. El perfil se activará en el dispositivo cuando se activen las reglas de activación.

Las reglas de activación del perfil de directiva creadas para el perfil se muestran en las propiedades del perfil de directiva en la sección **Reglas de activación**. Puede modificar o eliminar cualquier regla de activación de perfil de directiva.

Se pueden activar simultáneamente varias reglas de activación.

Reglas de movimiento de dispositivos

Recomendamos que automatice la asignación de dispositivos a grupos de administración mediante *reglas de movimiento de dispositivos*. Una regla de movimiento de dispositivo consiste en tres partes principales: nombre, condición de ejecución (expresión lógica con atributos del dispositivo) y grupo de administración de destino. Una regla mueve un dispositivo al grupo de administración de destino si los atributos del dispositivo cumplen la condición de ejecución de la regla.

Todas las reglas de movimiento de dispositivos tienen prioridades. El Servidor de administración comprueba los atributos del dispositivo en cuanto a si cumplen la condición de ejecución de cada regla, en orden ascendente de prioridad. Si los atributos del dispositivo cumplen la condición de ejecución de una regla, el dispositivo se mueve al grupo de destino, por lo que el procesamiento de la regla está completo para ese dispositivo. Si los atributos del dispositivo cumplen las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, el que tiene el rango más alto en la lista de reglas).

Las reglas de movimiento de dispositivos se pueden crear implícitamente. Por ejemplo, en las propiedades de un paquete de instalación o una tarea de instalación remota, puede especificar el grupo de administración al cual el dispositivo se debe mover después de que el Agente de red se instala en él. Además, el administrador de Kaspersky Security Center puede crear reglas de movimiento de dispositivos explícitamente en la lista de reglas de movimiento. La lista se ubica en la Consola de administración, en las propiedades del grupo **Dispositivos no asignados**.

De forma predeterminada, una regla de movimiento de dispositivo está destinada para la asignación inicial única de dispositivos a grupos de administración. La regla mueve dispositivos del grupo **Dispositivos no asignados** solo una vez. Si esta regla movió un dispositivo una vez, la regla nunca lo moverá nuevamente, aun si devuelve el dispositivo al grupo **Dispositivos no asignados** manualmente. Esta es la forma recomendada de aplicar reglas de movimiento.

Puede mover dispositivos que ya se hayan asignado a algunos de los grupos de administración. Para hacer esto, en las propiedades de una regla, borre la casilla de verificación **Mover solo dispositivos que no pertenezcan a ningún grupo de administración**.

Aplicar reglas de movimiento a dispositivos que ya se han asignado a algunos de los grupos de administración aumenta considerablemente la carga en el Servidor de administración.

Puede crear una regla de movimiento que afectaría un solo dispositivo repetidamente.

Recomendamos encarecidamente que evite mover un dispositivo solo desde un grupo a otro repetidamente (por ejemplo, a fin de aplicar una directiva especial a ese dispositivo, ejecutar una tarea de grupo especial o actualizar el dispositivo a través de un punto de distribución específico).

Tales situaciones no se admiten, porque aumentan la carga en Servidor de administración y el tráfico de red a un grado extremo. Estas situaciones también entran en conflicto con los principios de funcionamiento de Kaspersky Security Center (en particular, en el área de derechos de acceso, eventos e informes). Otra solución se debe encontrar, por ejemplo, a través del uso de perfiles de directiva, tareas para selecciones de dispositivos, asignación de agentes de red según el guion estándar, etcétera.

Reglas de movimiento de dispositivos de clonación

Cuando tiene que crear varias reglas de movimiento de dispositivos con configuraciones similares, puede clonar una regla existente y luego cambiar la configuración de la regla clonada. Por ejemplo, esto es útil cuando debe tener varias reglas idénticas de movimiento de dispositivos con diferentes rangos de IP y grupos objetivo.

Para clonar una regla móvil de dispositivo:

1. Abra la ventana principal de la aplicación.
2. En la carpeta **Dispositivos no asignados**, haga clic en **Configurar reglas**.

   Se abrirá la ventana Propiedades: **Dispositivos no asignados**.

3. En la sección **Mover dispositivos**, seleccione la regla de movimiento del dispositivo que desea clonar.

4. Haga clic en **Clonar regla**.

   Al final de la lista se añadirá un clon de la regla de movimiento del dispositivo seleccionado.

Se crea una nueva regla en el estado desactivado. Puede editar y activar la regla en cualquier momento.

Clasificación del software

La herramienta principal para supervisar la ejecución de aplicaciones son las *categorías de Kaspersky* (en adelante, también denominadas *categorías KL*). Las categorías KL ayudan a los administradores de Kaspersky Security Center a simplificar la asistencia de la clasificación del software y minimizar el tráfico que va a dispositivos administrados.

Las categorías de usuario solo se deben crear para aplicaciones que no pueden clasificarse en ninguna de las categorías KL existentes (por ejemplo, para el software hecho a la medida). Las categorías de usuario se crean basándose en el paquete de instalación de una aplicación (MSI) o una carpeta con paquetes de instalación.

Si una recopilación grande del software está disponible, que no se ha clasificado mediante categorías KL, puede ser útil crear una categoría que se actualiza automáticamente. Las sumas de comprobación de archivos ejecutables se añadirán automáticamente a esta categoría en cada modificación de la carpeta que contiene paquetes de distribución.

No es posible crear ninguna categoría de software que se actualice automáticamente sobre la base de las carpetas Mis documentos, %windir% y %ProgramFiles%. El grupo de archivos en estas carpetas está sujeto a cambios frecuentes, lo que lleva a un aumento en la carga en el Servidor de administración y un mayor tráfico de red. Debe crear una carpeta dedicada con la recopilación de software y periódicamente añadir nuevos elementos a ella.

Requisitos previos para instalar aplicaciones en dispositivos de una organización cliente

El proceso de instalación remota de aplicaciones en dispositivos de una organización cliente es idéntico al proceso de instalación remota dentro de una empresa.

Para instalar aplicaciones en los dispositivos de una organización cliente, se deben realizar las siguientes acciones:

- Antes de instalar las aplicaciones en los dispositivos de la organización cliente por primera vez, instale en ellos el Agente de red.

  Al configurar el paquete de instalación del Agente de red del proveedor de servicios de Kaspersky Security Center, debe ajustar los siguientes parámetros en la ventana de propiedades del paquete de instalación:

  - En la sección **Conexión**, en la cadena **Servidor de administración**, especifique la dirección del mismo Servidor de administración virtual que se especificó durante la instalación local del Agente de red al punto de distribución.

  - En la sección **Avanzado**, seleccione la casilla de verificación **Conectar con el Servidor de administración usando una puerta de enlace de conexión**. En la cadena **Dirección de la puerta de enlace de conexión**,

especifique la dirección del punto de distribución. Puede utilizar tanto la dirección IP del dispositivo como el nombre del dispositivo en la red de Windows.

- Seleccione **Usando recursos del sistema operativo mediante puntos de distribución** como método de descarga para el paquete de instalación del Agente de red. Puede seleccionar el método de descarga de esta manera:
  - Si instala la aplicación utilizando la tarea de instalación remota, puede especificar el método de descarga de las siguientes maneras:
    - Al crear una tarea de instalación remota en la ventana **Configuración**.
    - En la ventana de propiedades de la tarea de instalación remota, en la sección **Configuración**.
  - Si instala aplicaciones con el Asistente de instalación remota, puede seleccionar el método de descarga en la ventana **Configuración** de este Asistente.
- La cuenta que utiliza el punto de distribución para la autorización debe tener acceso al recurso Admin$ en todos los dispositivos cliente.

Visualización y cambio de la configuración de la aplicación local

El sistema de administración de Kaspersky Security Center permite administrar de forma remota la configuración de una aplicación local en dispositivos, a través de la Consola de administración.

Configuración de la aplicación local es la configuración de una aplicación específica para un dispositivo. Se puede utilizar Kaspersky Security Center para especificar la configuración de una aplicación local en los dispositivos incluidos en los grupos de administración.

En las respectivas Guías se proporcionan descripciones detalladas de las aplicaciones Kaspersky.

Para visualizar o cambiar los parámetros locales de una aplicación:

1. En el espacio de trabajo del grupo al que pertenece el dispositivo cliente requerido, seleccione la ficha **Dispositivos**.
2. En la ventana de propiedades del dispositivo cliente, en la sección **Aplicaciones**, seleccione la aplicación correspondiente.
3. Abra la ventana de propiedades de la aplicación haciendo doble clic sobre el nombre de la aplicación o pulsando el botón **Propiedades**.

La ventana de parámetros locales de la aplicación seleccionada se abrirá para poder visualizar y editar dichos parámetros.

Se pueden cambiar los valores de los parámetros cuya modificación no esté bloqueada por una directiva de grupo (es decir, aquellos marcados con el candado (🔒) en una directiva).

Actualización de Kaspersky Security Center y de las aplicaciones administradas

Esta sección describe los pasos que debe seguir para actualizar Kaspersky Security Center y las aplicaciones administradas.

Escenario: actualización periódica de las bases de datos y aplicaciones de Kaspersky

Esta sección proporciona un escenario para la actualización regular de las bases de datos, módulos de software y aplicaciones de Kaspersky. Una vez completado el escenario de configuración de la protección de red, debe mantener la fiabilidad del sistema de protección para garantizar que los Servidores de administración y los dispositivos administrados estén protegidos contra diversas amenazas, entre ellas virus, ataques de red y ataques de phishing.

La protección de la red se mantiene actualizada mediante actualizaciones periódicas de lo siguiente:

- Bases de datos y módulos de software de Kaspersky
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad

Cuando complete este escenario, puede estar seguro de lo siguiente:

- Su red está protegida por el software más reciente de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad.
- Las bases de datos antivirus y otras bases de datos de Kaspersky críticas para la seguridad de la red estarán siempre actualizadas.

Requisitos previos

Los dispositivos administrados deben tener conexión con el Servidor de administración. Si no tienen conexión, considere actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky de forma manual o directamente desde los servidores de actualización de Kaspersky.

El Servidor de administración debe tener una conexión a Internet.

Antes de comenzar, asegúrese de haber hecho lo siguiente:

1. Desplegado las aplicaciones de seguridad de Kaspersky en los dispositivos administrados según el escenario de implementación de aplicaciones de Kaspersky a través de Kaspersky Security Center 14 Web Console.
2. Creado y configurado todas las directivas, perfiles de directivas y tareas requeridas de acuerdo con el escenario de configuración de la protección de red.
3. Asignado una cantidad apropiada de puntos de distribución de acuerdo con la cantidad de dispositivos administrados y la topología de la red.

La actualización de bases de datos y aplicaciones de Kaspersky sucede en etapas:

1. **Elección de un esquema de actualización**

   Hay varios esquemas que puede usar para instalar actualizaciones para los componentes de Kaspersky Security Center y las aplicaciones de seguridad. Elija el esquema o varios esquemas que cumplan con los requisitos de su red.

2. **Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración**

   Esta tarea se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el Asistente, cree la tarea ahora.

   Esta tarea es necesaria para descargar actualizaciones de los servidores de actualización de Kaspersky al repositorio del Servidor de administración, así como para actualizar las bases de datos y módulos de software de Kaspersky para Kaspersky Security Center. Una vez que se descarguen las actualizaciones, se pueden propagar a los dispositivos administrados.

   Si su red tiene puntos de distribución asignados, las actualizaciones se descargan automáticamente desde el repositorio del Servidor de administración a los repositorios de los puntos de distribución. En este caso, los dispositivos administrados incluidos en la cobertura de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.

   Instrucciones:

   - Consola de administración: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración
   - Kaspersky Security Center 14 Web Console: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración

3. **Creación de la tarea para descargar actualizaciones a los repositorios de los puntos de distribución (opcional)**

   De forma predeterminada, las actualizaciones se descargan a los puntos de distribución desde el Servidor de administración. Puede configurar Kaspersky Security Center para descargar las actualizaciones a los puntos de distribución directamente desde los servidores de actualización de Kaspersky. La descarga a los repositorios de puntos de distribución es preferible si el tráfico entre el Servidor de administración y los puntos de distribución es más costoso que el tráfico entre los puntos de distribución y los servidores de actualización de Kaspersky o si su Servidor de administración no tiene acceso a Internet.

   Cuando su red ha asignado puntos de distribución y se crea la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*, los puntos de distribución descargan actualizaciones de los servidores de actualización de Kaspersky y no del repositorio del Servidor de administración.

   Instrucciones:

   - Consola de administración: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución
   - Kaspersky Security Center 14 Web Console: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución

4. **Configurar puntos de distribución**

   Cuando su red tenga puntos de distribución asignados, asegúrese de que la opción **Desplegar actualizaciones** esté habilitada en las propiedades de todos los puntos de distribución requeridos. Cuando esta opción está deshabilitada para un punto de distribución, los dispositivos incluidos en la cobertura del punto de distribución se actualizan desde el repositorio del Servidor de administración.

   Si desea que los dispositivos administrados reciban actualizaciones solo desde los puntos de distribución, habilite la opción **Distribuir archivos solo mediante puntos de distribución** en la directiva del Agente de red.

5 Optimización del proceso de actualización con el modelo sin conexión de la descarga de actualizaciones o los archivos diff (opcional)

Puede optimizar el proceso de actualización utilizando el modelo sin conexión de la descarga de actualizaciones (habilitado de forma predeterminada) o utilizando archivos diff. Para cada segmento de red, debe elegir cuál de estas dos características habilitar, ya que no pueden funcionar simultáneamente.

Cuando el modelo sin conexión de la descarga de actualizaciones está habilitado, el Agente de red descarga las actualizaciones necesarias en el dispositivo administrado una vez que las actualizaciones se descargan en el repositorio del Servidor de administración, antes de que la aplicación de seguridad solicite las actualizaciones. Esto mejora la fiabilidad del proceso de actualización. Para usar esta función, active la opción **Descargar actualizaciones y bases de datos antivirus del Servidor de administración (recomendado)** en la directiva del Agente de red.

Si no utiliza el modelo sin conexión de la descarga de actualizaciones, puede optimizar el tráfico entre el Servidor de administración y los dispositivos administrados mediante el uso de archivos diff. Cuando esta función está habilitada, el Servidor de administración o un punto de distribución descarga archivos diferenciales en lugar de archivos completos de bases de datos o módulos de software de Kaspersky. Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o un módulo de software. Por lo tanto, un archivo diff ocupa menos espacio que un archivo completo. Esto reduce el tráfico entre el Servidor de administración o los puntos de distribución y los dispositivos administrados. Para usar esta función, active la opción **Descargar archivos de comparación** en las propiedades de la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de puntos de distribución.

Instrucciones:

- Utilización de archivos diff para actualizar bases de datos y módulos de software de Kaspersky
- Consola de administración: Activación y desactivación del modelo sin conexión de descarga de actualizaciones
- Kaspersky Security Center 14 Web Console: Activación y desactivación del modelo sin conexión de descarga de actualizaciones

6 Verificación de las actualizaciones descargadas (opcional)

Antes de instalar las actualizaciones descargadas, puede verificar las actualizaciones mediante la tarea de *Verificación de actualizaciones*. Esta tarea ejecuta de forma secuencial las tareas de actualización de dispositivos y las tareas de análisis antivirus configuradas a través de la configuración para la colección especificada de dispositivos de prueba. Al obtener los resultados de la tarea, el Servidor de administración inicia o bloquea la propagación de la actualización a los dispositivos restantes.

La tarea Verificación de actualizaciones se puede ejecutar como parte de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En las propiedades de la tarea *Descargar actualizaciones en el repositorio de tareas del Servidor de administración*, active la opción **Verificar actualizaciones antes de distribuir** en la Consola de administración o la opción **Ejecutar verificación de actualizaciones** en Kaspersky Security Center 14 Web Console.

Instrucciones:

- Consola de administración: Verificación de actualizaciones descargadas
- Kaspersky Security Center 14 Web Console: Verificación de las actualizaciones descargadas

7 Aprobar y rechazar actualizaciones de software

De forma predeterminada, las actualizaciones de software descargadas tienen el estado *No definido*. Puede cambiar el estado a *Aprobado* o *Rechazado*. Las actualizaciones aprobadas siempre están instaladas. Si una actualización requiere revisar y aceptar los términos del Contrato de licencia de usuario final, primero debe aceptar los términos. Después de eso, la actualización se puede propagar a los dispositivos administrados. Las actualizaciones no definidas solo se pueden instalar en el Agente de red y otros componentes de Kaspersky Security Center de acuerdo con la configuración de la directiva del Agente de red. Las actualizaciones para las que establece el estado *Rechazado* no se instalarán en los dispositivos. Si previamente se instaló una actualización rechazada para una aplicación de seguridad, Kaspersky Security Center intentará desinstalar la actualización de todos los dispositivos. Las actualizaciones para los componentes de Kaspersky Security Center no se pueden desinstalar.

Instrucciones:

- Consola de administración: Aprobar y rechazar actualizaciones de software
- Kaspersky Security Center 14 Web Console: Aprobar y rechazar actualizaciones de software

8. **Configuración de la instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center**

   A partir de la versión 10 Service Pack 2, las actualizaciones y parches descargados para el Agente de red y otros componentes de Kaspersky Security Center se instalan automáticamente. Si dejó la opción **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir** activada en las propiedades del Agente de red, entonces todas las actualizaciones se instalarán automáticamente después de que se descarguen en el repositorio (o varios repositorios). Si esta opción está desactivada, los parches de Kaspersky que se hayan descargado y etiquetado con el estado *Indeterminado* solo se instalarán después de que el administrador cambie su estado a *Aprobados*.

   Para versiones del Agente de red anteriores a 10 Service Pack 2, asegúrese de que la opción **Actualizar módulos del Agente de red** esté activada en las propiedades de *Descargar actualizaciones al repositorio de la tarea del Servidor de administración* o *Descargar actualizaciones a los repositorios de puntos de distribución*.

   Instrucciones:

   - Consola de administración: Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center
   - Kaspersky Security Center 14 Web Console: Habilitar y deshabilitar la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center

9. **Instalación de actualizaciones para el Servidor de administración**

   Las actualizaciones de software para el Servidor de administración no dependen de los estados de actualización. No se instalan automáticamente y deben ser aprobados previamente por el administrador en la pestaña **Supervisión** en la Consola de administración (**Servidor de administración** `<nombre del servidor>` → **Supervisión**) o en la sección **NOTIFICACIONES** en Kaspersky Security Center 14 Web Console (**SUPERVISIÓN E INFORMES** → **NOTIFICACIONES**). Después de eso, el administrador debe ejecutar explícitamente la instalación de las actualizaciones.

10. **Configuración de instalación automática de actualizaciones para las aplicaciones de seguridad**

    Cree las tareas de actualización para las aplicaciones administradas para proporcionar actualizaciones oportunas a las aplicaciones, los módulos de software y las bases de datos de Kaspersky, incluidas las bases de datos antivirus. Para garantizar actualizaciones oportunas, le recomendamos que seleccione la opción **Cuando se descargan nuevas actualizaciones en el repositorio** al configurar la planificación de tareas.

    Si su red incluye dispositivos solo IPv6 y quiere actualizar regularmente las aplicaciones de seguridad instaladas en dichos dispositivos, asegúrese de que el Servidor de administración versión que no sea anterior a 13.2 y el Agente de red (versión que no sea anterior a 13.2) estén instalados en los dispositivos administrados.

    De forma predeterminada, las actualizaciones para Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Security para Linux se instalan solo después de cambiar el estado de la actualización a *Aprobado*. Puede cambiar la configuración de actualización en la tarea de actualización.

Si una actualización requiere revisar y aceptar los términos del Contrato de licencia de usuario final, primero debe aceptar los términos. Después de eso, la actualización se puede propagar a los dispositivos administrados.

Instrucciones:

- Consola de administración: Instalación automática de actualizaciones de Kaspersky Endpoint Security en dispositivos
- Kaspersky Security Center 14 Web Console: Instalación automática de actualizaciones de Kaspersky Endpoint Security en dispositivos

Resultados

Una vez completado el escenario, Kaspersky Security Center se configura para actualizar las bases de datos de Kaspersky y las aplicaciones instaladas de Kaspersky después de que las actualizaciones se descargan en el repositorio del Servidor de administración o en los repositorios de los puntos de distribución. Después, puede proceder a monitorear el estado de la red.

Acerca de la actualización de las bases de datos, módulos de software y aplicaciones de Kaspersky

Para asegurarse de que la protección de sus Servidores de administración y dispositivos administrados esté actualizada, debe proporcionar actualizaciones oportunas de las siguientes:

- Bases de datos y módulos de software de Kaspersky

  Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center comprueba si se puede acceder a los servidores de Kaspersky. Si no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza el DNS público. Esto es necesario para asegurarse de que las bases de datos antivirus estén actualizadas y se mantenga el nivel de seguridad para los dispositivos administrados.

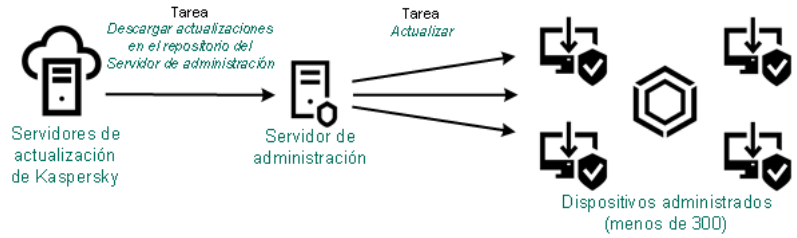
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad

Dependiendo de la configuración de su red, puede utilizar los siguientes esquemas de descarga y distribución de las actualizaciones necesarias para los dispositivos administrados:

- Mediante el uso de una sola tarea: *Descargar actualizaciones en el repositorio del Servidor de administración*
- Mediante el uso de dos tareas:
  - La tarea *Descargar actualizaciones en el repositorio del Servidor de administración*
  - La tarea *Descargar actualizaciones en los repositorios de puntos de distribución*
- Manualmente a través de una carpeta local, una carpeta compartida o un servidor FTP
- Directamente desde los servidores de actualización de Kaspersky a Kaspersky Endpoint Security para Windows en los dispositivos administrados

Uso de la tarea Descargar actualizaciones en el repositorio del Servidor de administración

En este esquema, Kaspersky Security Center descarga actualizaciones a través de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En redes pequeñas que contienen menos de 300 dispositivos administrados en un solo segmento de red o menos de 10 dispositivos administrados en cada segmento de red, las actualizaciones se distribuyen a los dispositivos administrados directamente desde el repositorio del Servidor de administración (ver la siguiente figura).

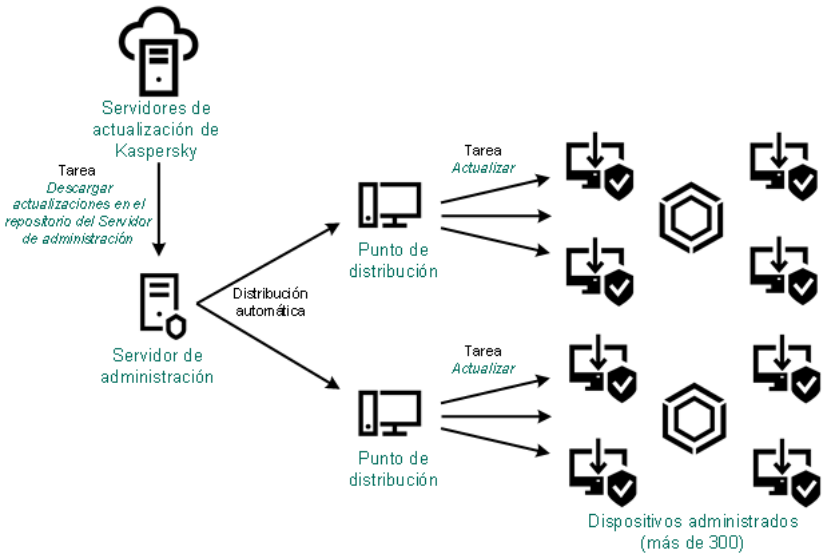


Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración sin puntos de distribución

De forma predeterminada, el Servidor de administración se comunica con los servidores de actualización de Kaspersky y descarga las actualizaciones utilizando el protocolo HTTPS. Puede configurar Servidor de administración para que utilice el protocolo HTTP en lugar del HTTPS.

Si su red contiene más de 300 dispositivos administrados en un solo segmento de red o si su red consta de varios segmentos de red con más de 9 dispositivos administrados en cada segmento de red, le recomendamos que utilice puntos de distribución para propagar las actualizaciones a los dispositivos administrados (ver la siguiente figura). Los puntos de distribución reducen la carga en el Servidor de administración y optimizan el tráfico entre el Servidor de administración y los dispositivos administrados. Puede calcular el número y la configuración de los puntos de distribución necesarios para su red.

En este esquema, las actualizaciones se descargan automáticamente del repositorio del Servidor de administración a los repositorios de los puntos de distribución. Los dispositivos administrados incluidos en la cobertura de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.



Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración con puntos de distribución

Una vez que se complete la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las siguientes actualizaciones se descargan en el repositorio del Servidor de administración:

- Bases de datos y módulos de software de Kaspersky para Kaspersky Security Center

  Estas actualizaciones se instalan automáticamente.

- Bases de datos y módulos de software de Kaspersky para las aplicaciones de seguridad en los dispositivos administrados

  Estas actualizaciones se instalan a través de Actualizar tarea de Kaspersky Endpoint Security para Windows.

- Actualizaciones para el Servidor de administración

  Estas actualizaciones no se instalan automáticamente. El administrador debe aprobar y ejecutar explícitamente la instalación de las actualizaciones.

  > Se requieren derechos de administrador local para instalar parches en el Servidor de administración.

- Actualizaciones para los componentes de Kaspersky Security Center

  De forma predeterminada, estas actualizaciones se instalan automáticamente. Puede cambiar la configuración en la directiva del Agente de red.

- Actualizaciones para las aplicaciones de seguridad

  De forma predeterminada, Kaspersky Endpoint Security para Windows instala solo las actualizaciones que usted apruebe. (Puede aprobar las actualizaciones a través de la consola de administración o a través de Kaspersky Security Center 14 Web Console). Las actualizaciones se instalan a través de la tarea Actualizar y se pueden configurar en las propiedades de esta tarea.

> La tarea del Servidor de administración Descargar actualizaciones en el repositorio no está disponible en los Servidores de administración virtuales. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas en el Servidor de administración principal.

Puede configurar las actualizaciones para verificar su operatividad y errores en un conjunto de dispositivos de prueba. Si la verificación es exitosa, las actualizaciones se distribuyen a otros dispositivos administrados.

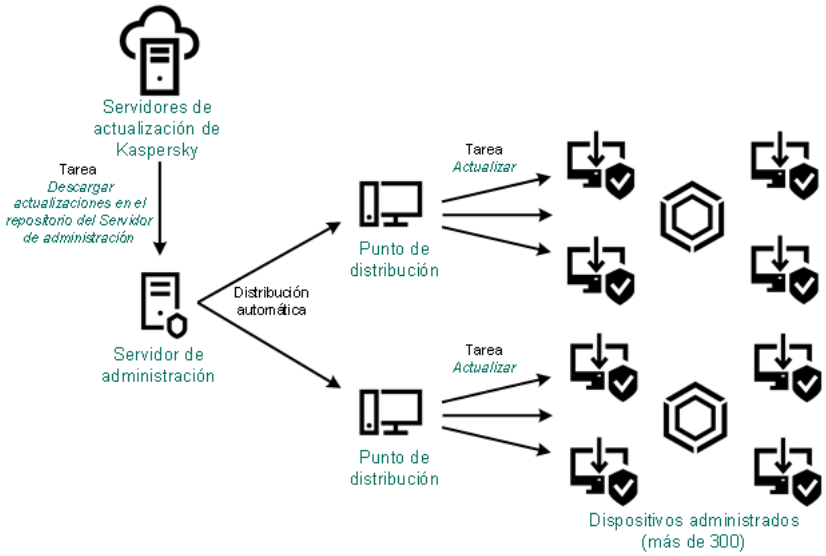
Cada aplicación de Kaspersky solicita actualizaciones requeridas del Servidor de administración. El Servidor de administración añade estas solicitudes y descarga solo aquellas actualizaciones que son solicitadas por cualquier aplicación. Esto garantiza que las mismas actualizaciones no se descarguen varias veces y que las actualizaciones innecesarias no se descarguen en absoluto. Cuando se ejecuta la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, el Servidor de administración envía la siguiente información a los servidores de actualización de Kaspersky automáticamente para garantizar la descarga de versiones relevantes de las bases de datos de Kaspersky y los módulos de software:

- Id. y versión de la aplicación
- ID de instalación de la aplicación
- Id. de clave activa
- Id. de ejecución de la tarea *Descargar actualizaciones al repositorio del Servidor de administración*

Ninguna información transmitida contiene datos personales u otros datos confidenciales. AO Kaspersky Lab protege la información de acuerdo con los requisitos establecidos por la ley.

Usando dos tareas: la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de puntos de distribución

Puede descargar actualizaciones a los repositorios de puntos de distribución directamente desde los servidores de actualizaciones de Kaspersky en lugar del repositorio del Servidor de administración y después distribuir las actualizaciones a los dispositivos administrados (consulte la siguiente figura). La descarga a los repositorios de puntos de distribución es preferible si el tráfico entre el Servidor de administración y los puntos de distribución es más costoso que el tráfico entre los puntos de distribución y los servidores de actualización de Kaspersky o si su Servidor de administración no tiene acceso a Internet.



Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de puntos de distribución

De forma predeterminada, el Servidor de administración y los puntos de distribución se comunican con los servidores de actualización de Kaspersky y descargan las actualizaciones utilizando el protocolo HTTPS. Puede configurar el Servidor de administración y/o los puntos de distribución para utilizar el protocolo HTTP en lugar de HTTPS.

Para implementar este esquema, cree la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* además de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Después de esto, los puntos de distribución descargarán actualizaciones desde servidores de actualizaciones de Kaspersky y no desde el repositorio del Servidor de administración.

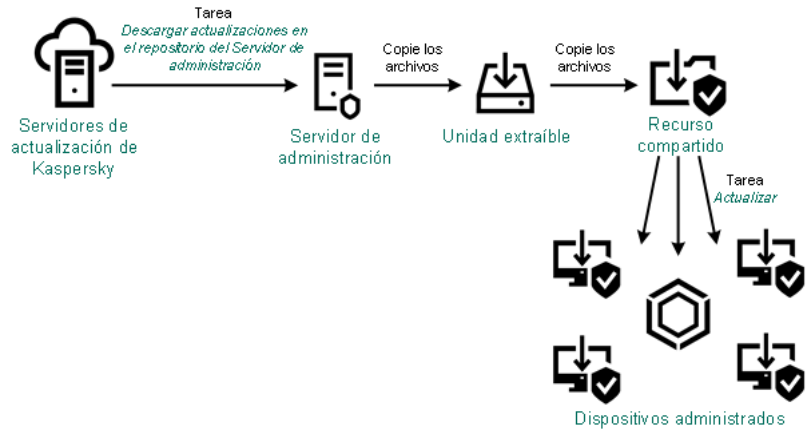
Los dispositivos de punto de distribución con macOS no pueden descargar actualizaciones de los servidores de actualización de Kaspersky.

Si uno o más dispositivos incluidos en la cobertura de la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* ejecutan macOS, la tarea se completa con el estado *Fallo*, incluso si se completa correctamente en todos los dispositivos de Windows.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* también es necesaria para este esquema, ya que esta tarea se utiliza para descargar las bases de datos y los módulos de software de Kaspersky para Kaspersky Security Center.

Manualmente a través de una carpeta local, una carpeta compartida o un servidor FTP

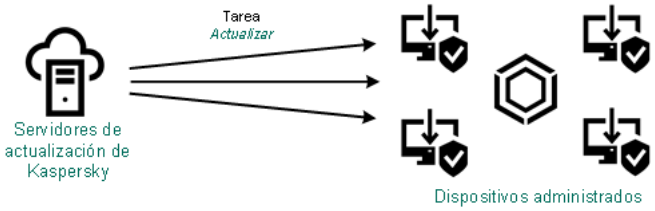
Si los dispositivos cliente no tienen una conexión con el Servidor de administración, puede usar una carpeta local o un recurso compartido como fuente para actualizar las bases de datos, módulos de software y aplicaciones de Kaspersky. En este esquema, debe copiar las actualizaciones requeridas desde el repositorio del Servidor de administración a una unidad extraíble, luego copiar las actualizaciones a la carpeta local o al recurso compartido especificado como origen de actualizaciones en la configuración de Kaspersky Endpoint Security para Windows (ver la siguiente figura).



Actualización a través de una carpeta local, una carpeta compartida o un servidor FTP

Directamente desde los servidores de actualización de Kaspersky a Kaspersky Endpoint Security para Windows en los dispositivos administrados

En los dispositivos administrados, puede configurar Kaspersky Endpoint Security para Windows para recibir actualizaciones directamente desde los servidores de actualización de Kaspersky (ver la siguiente figura).



Actualizar aplicaciones de seguridad directamente desde los servidores de actualización de Kaspersky

En este esquema, la aplicación de seguridad no utiliza los repositorios proporcionados por Kaspersky Security Center. Para recibir actualizaciones directamente de los servidores de actualización de Kaspersky, especifique los servidores de actualización de Kaspersky como origen de actualizaciones en la interfaz de la aplicación de seguridad. Para obtener una descripción completa de la configuración, consulte la documentación de Kaspersky Endpoint Security para Windows.

Acerca de la utilización de archivos diff para actualizar bases de datos y módulos de software de Kaspersky

Cuando Kaspersky Security Center descarga actualizaciones de los servidores de actualización de Kaspersky, optimiza el tráfico mediante el uso de archivos diff. También puede habilitar el uso de archivos diff por dispositivos (Servidores de administración, puntos de distribución y dispositivos cliente) que aceptan actualizaciones de otros dispositivos en su red.

Acerca de la característica de descarga de archivos diff

Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o un módulo de software. El uso de archivos diff ahorra tráfico dentro de la red de su empresa porque los archivos diff ocupan menos espacio que los archivos completos de bases de datos y módulos de software. Si la función de *descarga de archivos diff* está activada en el Servidor de administración o un punto de distribución, los archivos diff se guardan en este Servidor de administración o punto de distribución. Como resultado, los dispositivos que toman actualizaciones de este Servidor de administración o punto de distribución pueden usar los archivos diff guardados para actualizar sus bases de datos y módulos de software.

Para optimizar el uso de los archivos diff, le recomendamos que sincronice el programa de actualización de los dispositivos con el programa de actualización del Servidor de administración o el punto de distribución desde el cual los dispositivos reciben actualizaciones. Sin embargo, el tráfico se puede guardar incluso si los dispositivos se actualizan varias veces con menos frecuencia que el Servidor de administración o el punto de distribución desde el que reciben actualizaciones los dispositivos.

La función de descarga de archivos diff solo se puede activar en los Servidores de administración y los puntos de distribución de las versiones a partir de la versión 11. Para guardar archivos diff en Servidores de administración y puntos de distribución de versiones anteriores, actualícelos a la versión 11 o versiones posteriores.

La función de descarga de archivos diff es incompatible con el modelo de descarga de actualizaciones sin conexión. Significa que los Agentes de red que usan el modelo de descarga de actualizaciones sin conexión no descargan archivos diff, incluso si la función de descarga de archivos diff está activada en el Servidor de administración o el punto de distribución que entrega actualizaciones a estos Agentes de redes.

Los puntos de distribución no utilizan la multidifusión IP para la distribución automática de archivos diff.

Activación de la función de descarga de archivos diff: escenario

Requisitos previos

Los requisitos previos para el escenario son los siguientes:

- Los Servidores de administración y los puntos de distribución se actualizan a la versión 11 o versiones posteriores.
- El modelo de descarga de actualizaciones sin conexión está desactivado en la configuración de la directiva del Agente de red.

Etapas

1. **Activar la función en el Servidor de administración**

   Active la función en la configuración de las actualizaciones de descarga en el repositorio de la tarea del Servidor de administración.

2. **Activar la función para un punto de distribución**

   Habilite la función para un punto de distribución que recibe actualizaciones a través de la tarea Descargar actualizaciones en los repositorios de puntos de distribución.

A continuación, active la función para un punto de distribución que recibe actualizaciones del Servidor de administración.

La función está activada en la configuración de directivas del Agente de red y, si los puntos de distribución se asignan manualmente y si desea anular la configuración de directivas, en la sección **Puntos de distribución** de las propiedades del Servidor de administración.

Para verificar que la función de descarga de archivos diff esté activada con éxito, puede medir el tráfico interno antes y después de realizar el escenario.

Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración

El Asistente de inicio rápido de Kaspersky Security Center crea automáticamente la tarea del Servidor de administración Descargar actualizaciones en el repositorio del Servidor de administración. Puede crear únicamente una tarea del Servidor de administración de descarga de actualizaciones al repositorio. Por eso se puede crear una tarea del Servidor de administración para descargar actualizaciones en el repositorio solo si tal tarea se eliminó de la lista de tareas del Servidor de administración.

Para crear actualizaciones de descarga en el repositorio de la tarea del Servidor de administración:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. Inicie la creación de la tarea por alguno de los siguientes medios:
   - En el menú contextual de la carpeta **Tareas** en el árbol de consola, seleccione **Nuevo** → **Tarea**.
   - En el espacio de trabajo de la carpeta **Tareas**, haga clic en el botón **Crear una tarea**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. En la página del Asistente **Seleccionar el tipo de tarea**, seleccione **Descargar actualizaciones en el repositorio del Servidor de administración**.
4. En la página del Asistente **Configuración**, especifique la configuración de la tarea de la siguiente manera:
   - **Orígenes de actualizaciones**

Los siguientes recursos pueden utilizarse como un origen de actualizaciones para el Servidor de administración:

- Servidores de actualización de Kaspersky

  Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación. De forma predeterminada, el Servidor de administración se comunica con los servidores de actualización de Kaspersky y descarga las actualizaciones utilizando el protocolo HTTPS. Puede configurar Servidor de administración para que utilice el protocolo HTTP en lugar del HTTPS.

  Seleccionado de forma predeterminada.

- Servidor de administración principal

  Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

- Carpeta local o de red

  Una carpeta local o de red que contiene las últimas actualizaciones. Una carpeta de red puede ser un servidor FTP o HTTP o un recurso compartido SMB. Si una carpeta de red requiere autenticación, solo se admite el protocolo SMB. Cuando se selecciona una carpeta local, debe especificar una carpeta en un dispositivo que tenga el Servidor de administración instalado.

  Un servidor FTP o HTTP o una carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura creada al usar los servidores de actualización de Kaspersky.

Si activa la opción **No usar servidor proxy** para los orígenes de actualizaciones Servidores de actualización de Kaspersky o Carpeta local o de red, el Servidor de administración no utilizará un servidor proxy para descargar actualizaciones.

- **Otros parámetros**:

  - Forzar actualización en los Servidores de administración secundarios

    Si esta opción está activada, el Servidor de administración inicia las tareas de actualización en los Servidores de administración secundarios tan pronto como se descargan nuevas actualizaciones. De lo contrario, las tareas de actualización en los Servidores de administración secundarios comienzan de acuerdo con sus programaciones.

    Esta opción está desactivada de forma predeterminada.

  - Copiar las actualizaciones descargadas en carpetas adicionales

Una vez que el Servidor de administración recibe actualizaciones, las copia en las carpetas especificadas. Utilice esta opción si desea administrar de manera manual la distribución de actualizaciones en su red.

Por ejemplo, puede querer usar esta opción en la siguiente situación: la red de su organización consta de varias subredes independientes y los dispositivos de cada una de las subredes no tienen acceso a otras subredes. Sin embargo, los dispositivos en todas las subredes tienen acceso a un recurso compartido de red común. En este caso, configura el Servidor de administración en una de las subredes para descargar actualizaciones de los servidores de actualización de Kaspersky, active esta opción y luego especifique este recurso compartido de red. En las actualizaciones descargadas de las tareas del repositorio para otros Servidores de administración, especifique el mismo recurso compartido de red que el origen de actualización.

Esta opción está desactivada de forma predeterminada.

- **No forzar la actualización de dispositivos y Servidores de administración secundarios a menos que se complete la copia**

  Las tareas de descarga de actualizaciones a dispositivos cliente y Servidores de administración secundarios comienzan solo después de que esas actualizaciones se copien de la carpeta de actualización principal a carpetas de actualización adicionales.

  Esta opción debe estar activada si los dispositivos cliente y los Servidores de administración secundarios descargan actualizaciones de carpetas de red adicionales.

  Esta opción está desactivada de forma predeterminada.

- **Actualizar módulos del Agente de red (para versiones del Agente de red anteriores a la 10, Service Pack 2)**

  Si esta opción está habilitada, las actualizaciones para los módulos de software del Agente de red se instalan automáticamente después de que el Servidor de administración complete la tarea Descargar actualizaciones en el repositorio. De lo contrario, las actualizaciones recibidas para los módulos del Agente de red se pueden instalar de manera manual.

  Esta opción solo se aplica a las versiones del Agente de red anteriores a la 10 Service Pack 2. A partir de la versión 10 Service Pack 2, los Agentes de red se actualizan automáticamente.

  Esta opción está activada de forma predeterminada.

- **Descargar actualizaciones utilizando el esquema antiguo**

A partir de la versión 14, Kaspersky Security Center descarga las actualizaciones de bases de datos y los módulos de software utilizando el nuevo esquema. Para que la aplicación descargue actualizaciones utilizando el nuevo esquema, el origen de actualización debe contener archivos de actualización con metadatos que sean compatibles con el nuevo esquema. Si el origen de actualización contiene archivos de actualización con metadatos que solo son compatibles con el esquema anterior, active la opción **Descargar actualizaciones utilizando el esquema antiguo**. De lo contrario, la tarea de descarga de la actualización no funcionará.

Por ejemplo, debe activar esta opción cuando se especifica una carpeta local o de red como fuente de actualización y los archivos de actualización en esta carpeta fueron descargados por una de las siguientes aplicaciones:

- Utilidad Kaspersky Update

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13.2 o una versión anterior

  Por ejemplo, su Servidor de administración 1 no tiene conexión a Internet. En este caso, puede descargar actualizaciones utilizando un Servidor de administración 2 que tenga conexión a Internet y luego colocar las actualizaciones en una carpeta local o de red para usarlas como fuente de actualización para el Servidor de administración 1. Si el Servidor de administración 2 tiene la versión 13.2 o anterior, active la **Descargar actualizaciones utilizando el esquema antiguo** opción en la tarea para el Servidor de administración 1.

Esta opción está desactivada de forma predeterminada.

5. En la página **Configurar programación de tareas** del Asistente, puede crear una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

- **Inicio programado:**

  Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

  - **Cada N horas**

    La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

    De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

  - **Cada N días**

    La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

    De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

  - **Cada N semanas**

    La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

    De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para la protección del perímetro
- Antivirus para sistemas de correo

De forma predeterminada, están seleccionados todos los tipos de aplicación.

Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- **Usar un retraso aleatorio automático para el inicio de las tareas**

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

6. En la página del Asistente **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).

7. En la página **Finalizar la creación de tareas** del Asistente haga clic en el botón **Finalizar** para cerrar el Asistente.

   Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

Una vez que finaliza el Asistente, las **Descargar actualizaciones en el repositorio del Servidor de administración** aparecen en la lista de tareas del Servidor de administración en el espacio de trabajo.

Además de la configuración que especifique durante la creación de la tarea, puede cambiar otras propiedades de una tarea creada.

Cuando un Servidor de administración realiza la tarea del Servidor de administración de descargar actualizaciones en el repositorio, las actualizaciones de las bases de datos y módulos de software se descargan del origen de actualizaciones y se almacenan en la carpeta compartida de un Servidor de administración. Si crea esta tarea para un grupo de administración, solo se aplicará a los Agentes de red incluidos en el grupo de administración especificado.

Las actualizaciones se distribuyen en los dispositivos cliente y en los Servidores de administración secundarios desde la carpeta compartida del Servidor de administración.

Creación de la tarea de descarga de actualizaciones en los repositorios del punto de distribución

Los dispositivos de punto de distribución con macOS no pueden descargar actualizaciones de los servidores de actualización de Kaspersky.

Si uno o más dispositivos incluidos en la cobertura de la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* ejecutan macOS, la tarea se completa con el estado *Fallo*, incluso si se completa correctamente en todos los dispositivos de Windows.

Puede crear la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* para un grupo de administración. Esta tarea se ejecutará para puntos de distribución incluidos en el grupo de administración especificado.

Puede usar esta tarea, por ejemplo, si el tráfico entre el Servidor de administración y los puntos de distribución es más costoso que el tráfico entre los puntos de distribución y los servidores de actualización de Kaspersky o si su Servidor de administración no tiene acceso a Internet.

Para crear la tarea de Descarga de actualizaciones en los repositorios del punto de distribución para un grupo de administración seleccionado:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. En el espacio de trabajo de esta carpeta, haga clic en el botón **Crear una tarea**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. En la página **Seleccionar el tipo de tarea** del Asistente, seleccione el nodo **Servidor de administración de Kaspersky Security Center 14**, expanda la carpeta **Avanzado** y luego seleccione la tarea **Descargar actualizaciones en los repositorios de puntos de distribución**.
4. En la página del Asistente **Configuración**, especifique la configuración de la tarea de la siguiente manera:

   - Orígenes de actualizaciones

     Los recursos siguientes pueden utilizarse como origen de actualizaciones para el punto de distribución:

     - Servidores de actualización de Kaspersky

       Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación.

       Esta opción está seleccionada de forma predeterminada.

     - Servidor de administración principal

       Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

     - Carpeta local o de red

       Una carpeta local o de red que contiene las últimas actualizaciones. Una carpeta de red puede ser un servidor FTP o HTTP o un recurso compartido SMB. Si una carpeta de red requiere autenticación, solo se admite el protocolo SMB. Cuando se selecciona una carpeta local, debe especificar una carpeta en un dispositivo que tenga el Servidor de administración instalado.

       > Un servidor FTP o HTTP o una carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura creada al usar los servidores de actualización de Kaspersky.

     Si activa la opción **No usar servidor proxy** para los orígenes de actualización Servidores de actualización de Kaspersky o Carpeta local o de red, un punto de distribución no usa un servidor proxy para descargar actualizaciones, incluso si ha activado la opción **Usar servidor proxy** la configuración de la directiva del Agente de red para el punto de distribución.

   - Carpeta para almacenar actualizaciones

     La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

   - Descargar actualizaciones utilizando el esquema antiguo

A partir de la versión 14, Kaspersky Security Center descarga las actualizaciones de bases de datos y los módulos de software utilizando el nuevo esquema. Para que la aplicación descargue actualizaciones utilizando el nuevo esquema, el origen de actualización debe contener los archivos de actualización cuyos metadatos sean compatibles con el nuevo esquema. Si el origen de actualización contiene archivos de actualización cuyos metadatos son compatibles solo con el esquema anterior, active la **Descargar actualizaciones utilizando el esquema antiguo** opción. De lo contrario, la tarea de descarga de la actualización no funcionará.

Por ejemplo, debe activar esta opción cuando se especifica una carpeta local o de red como fuente de actualización y los archivos de actualización en esta carpeta fueron descargados por una de las siguientes aplicaciones:

- Utilidad Kaspersky Update

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 14 o una versión anterior

  Por ejemplo, un punto de distribución está configurado para tomar las actualizaciones de una carpeta local o de red. En este caso, puede descargar actualizaciones utilizando un Servidor de administración que tenga conexión a Internet y luego colocar las actualizaciones en la carpeta local en el punto de distribución. Si el Servidor de administración tiene la versión 14 o anterior, active la opción **Descargar actualizaciones utilizando el esquema antiguo** en la tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*.

Esta opción está desactivada de forma predeterminada.

5. En la página **Seleccione el grupo de administración** del Asistente, haga clic en **Examinar** y seleccione el grupo de administración al que se aplica la tarea.

6. En la página **Configurar programación de tareas** del Asistente, puede crear una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

   - **Inicio programado:**

     Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

     - **Cada N horas**

       La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

       De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

     - **Cada N días**

       La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

       De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

     - **Cada N semanas**

La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- **Usar un retraso aleatorio automático para el inicio de las tareas**

Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

7. En la página del Asistente **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).

8. En la página **Finalizar la creación de tareas** del Asistente haga clic en el botón **Finalizar** para cerrar el Asistente.

   Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

Cuando el Asistente completa su operación, la **Descargar actualizaciones en los repositorios de puntos de distribución** aparece en la lista de tareas del Agente de red en el grupo de administración de destino y en el espacio de trabajo **Tareas** de la consola.

Además de la configuración que especifique durante la creación de la tarea, puede cambiar otras propiedades de una tarea creada.

Cuando se realiza la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*, las actualizaciones para bases de datos y módulos del software se descargan desde el origen de actualizaciones y se almacenan en la carpeta compartida. Las actualizaciones descargadas solo se utilizarán por puntos de distribución que se incluyen en el grupo de administración especificado y que no tienen una tarea de descarga de actualización explícitamente definida para ellos.

En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Puntos de distribución**. En las propiedades de cada punto de distribución, en la sección **Fuente de actualización** puede especificar la fuente de actualización (**Descargar del Servidor de administración** o **Utilizar la tarea para la descarga forzada de actualizaciones**). De forma predeterminada, **Descargar del Servidor de administración** se selecciona para un punto de distribución asignado manualmente o automáticamente. Estos puntos de distribución usarán los resultados de la tarea *Descarga de actualizaciones en los repositorios de puntos de distribución*.

Las propiedades de cada punto de distribución especifican la carpeta de la red que se ha configurado para ese punto de distribución individualmente. Los nombres de carpetas pueden variar para puntos de distribución diferentes. Por esta razón, no recomendamos que cambie la carpeta de la red en las propiedades de la tarea si la tarea se ha creado para un grupo de dispositivos.

Puede cambiar la carpeta de la red con actualizaciones en las propiedades de la tarea *Descarga de actualizaciones en los repositorios de puntos de distribución* si está creando una tarea local para un dispositivo.

Configuración de las actualizaciones de descarga en el repositorio de la tarea del Servidor de administración

Para configurar las actualizaciones de descarga en el repositorio de la tarea del Servidor de administración:

1. En el espacio de trabajo de la carpeta de árbol de consola **Tareas**, seleccione la tarea **Descargar actualizaciones en el repositorio del Servidor de administración** de la lista de tareas.

2. Abra la ventana de propiedades de la tarea por alguno de los siguientes medios:

   - Seleccione **Propiedades** en el menú contextual de la tarea.

   - Haga clic en el enlace **Configurar tarea** en el cuadro de información de la tarea seleccionada.

   Se abrirá la ventana de propiedades de la tarea Descargar actualizaciones en el repositorio del Servidor de administración. En esta ventana se puede configurar la forma de descargar las actualizaciones en el repositorio del Servidor de administración.

Verificación de las actualizaciones descargadas

Antes de instalar actualizaciones en los dispositivos administrados, primero puede verificar si las actualizaciones son operativas y los errores a través de la tarea de *Verificación de actualizaciones*. La tarea *Verificación de actualizaciones* se realiza automáticamente como parte de la tarea *Descargar actualizaciones al repositorio del Servidor de administración*. El Servidor de administración descarga las actualizaciones del origen, las guarda en el repositorio temporal y ejecuta la tarea de *verificación de actualizaciones*. Si la tarea termina correctamente, las actualizaciones se copiarán del repositorio temporal a la carpeta compartida del Servidor de administración (<Carpeta de instalación de Kaspersky Security Center>\Share\Updates). Se distribuirán a todos los dispositivos cliente que tengan como origen de actualizaciones ese mismo Servidor de administración.

Si, como resultado de la tarea *Verificación de actualizaciones*, se muestra que las actualizaciones ubicadas en el repositorio temporal son incorrectas o si la tarea *Verificación de actualizaciones* se ha completado con errores, las actualizaciones de este tipo no se copiarán a la carpeta compartida. El Servidor de administración guardará el conjunto de actualizaciones anterior. Además, las tareas que tienen el tipo de programación **Cuando se descargan nuevas actualizaciones en el repositorio** no se inician. Si el análisis de las nuevas actualizaciones se realiza con éxito, dichas operaciones se realizarán en el siguiente inicio de la tarea *Descargar de actualizaciones en el repositorio del Servidor de administración*.

Se considerará que un conjunto de actualizaciones es incorrecto si se cumple una de las siguientes condiciones en al menos un dispositivo de prueba:

- Se produjo un error en la tarea de actualización.

- El estado de protección en tiempo real de la aplicación de seguridad ha cambiado después de aplicarse las actualizaciones.
- Se ha detectado un objeto infectado mientras se ejecutaba la tarea de análisis a petición.
- Se ha producido un error en el tiempo de ejecución de una aplicación Kaspersky.

Si ninguna de las condiciones indicadas es verdadera para ningún dispositivo de prueba, se considerará que el conjunto de actualizaciones es válido y que la tarea *Verificación de actualizaciones* ha finalizado correctamente.

Antes de empezar a crear la tarea *Verificación de actualizaciones*, realice los requisitos previos:

1. Cree un grupo de administración con varios dispositivos de prueba. Necesitará este grupo para verificar las actualizaciones en él.

   Recomendamos utilizar los dispositivos con la protección más fiable y con la configuración de aplicaciones más común en la red. Este enfoque aumenta la calidad y la probabilidad de detección de virus durante los análisis y reduce al mínimo el riesgo de falsos positivos. Si se detectan virus en los dispositivos cliente, se considerará que la tarea *Verificación de actualizaciones* no se ha realizado correctamente.

2. Cree las tareas *Actualizar* y *Análisis antivirus* para una aplicación compatible con Kaspersky Security Center, por ejemplo, Kaspersky Endpoint Security para Windows o Kaspersky Security para Windows Server. Al crear las tareas *Actualizar* y *Análisis antivirus*, especifique el grupo de administración con los dispositivos de prueba.

   La tarea *Verificación de actualizaciones* ejecuta secuencialmente las tareas *Actualizar* y *Análisis antivirus* en los dispositivos de prueba para verificar que todas las actualizaciones sean válidas. Además, al crear la tarea *Verificación de actualizaciones*, debe especificar las tareas *Actualizar* y *Análisis antivirus*.

3. Cree la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

Para que Kaspersky Security Center verifique las actualizaciones descargadas antes de distribuirlas a los dispositivos cliente:

1. En el espacio de trabajo de la carpeta **Tareas**, seleccione la tarea *Descargar actualizaciones en el repositorio del Servidor de administración* de la lista de tareas.
2. Abra la ventana de propiedades de la tarea por alguno de los siguientes medios:
   - Seleccione **Propiedades** en el menú contextual de la tarea.
   - Haciendo clic en el vínculo **Configurar tarea** en el cuadro de información de la tarea seleccionada.
3. Si la tarea *Verificar actualizaciones* existe, haga clic en el botón **Examinar**. En la ventana que se abre, seleccione la tarea *Verificar actualizaciones* en el grupo de administración con dispositivos de prueba.
4. Si no todavía no ha creado la tarea *Verificar actualizaciones*, haga clic en el botón **Crear**.

   Se iniciará el Asistente para crear tareas de verificación de actualizaciones. Siga las instrucciones del Asistente.
5. Haga clic en **Aceptar** para cerrar la ventana de propiedades de *Descargar actualizaciones al repositorio de la tarea del Servidor de administración*.

La verificación de actualización automática está habilitada. Ahora, puede ejecutar la tarea *Descargar actualizaciones al repositorio del Servidor de administración*, que comenzará con la verificación de actualización.

Configuración de directivas de prueba y tareas auxiliares

Cuando se crea una tarea *Verificación de actualizaciones*, el Servidor de administración genera unas directivas de prueba, tareas de actualización de grupo auxiliares y tareas de análisis a petición.

Las tareas de actualización de grupo auxiliares y las tareas de análisis a petición tardan cierto tiempo. Estas tareas se llevan a cabo cuando se ejecuta la tarea *Verificación de actualizaciones*. La tarea *Verificación de actualizaciones* se realiza como parte de la tarea Descargar actualizaciones en el repositorio. La duración de la tarea Descargar actualizaciones en el repositorio incluye las tareas de actualización de grupo auxiliares y las de análisis a petición.

Se pueden modificar los parámetros de las directivas de prueba y de las tareas auxiliares.

Para modificar los parámetros de una directiva de prueba o de una tarea auxiliar:

1. En el árbol de consola, seleccione el grupo para el que se creará la tarea *Verificación de actualizaciones*.
2. En el espacio de trabajo del grupo, seleccione una de las siguientes fichas:
   - **Directivas**: Si quiere editar los parámetros de una directiva de prueba.
   - **Tareas**: Si quiere modificar los parámetros de una tarea auxiliar.
3. En la ficha del espacio de trabajo seleccione la directiva o tarea a la que quiera modificar los parámetros.
4. Abra la ventana de propiedades de la directiva (o tarea) por alguno de los siguientes medios:
   - Seleccionando **Propiedades** en el menú contextual de la directiva (tarea).
   - Haga clic en el enlace **Configurar directiva** (**Configurar tarea**) en el cuadro de información para la directiva seleccionada (tarea).

Para verificar las actualizaciones correctamente, debe imponer las siguientes restricciones sobre las modificaciones de las directivas de prueba y de las tareas auxiliares:

- En los parámetros de las tareas auxiliares:
  - Guarde todas las tareas con los niveles de importancia **Evento crítico** y **Fallo operativo** en el Servidor de administración. Usando los eventos de estos tipos, el Servidor de administración analiza el funcionamiento de las aplicaciones.
  - Utilice el Servidor de administración como el origen de las actualizaciones.
  - Especifique el tipo de planificación de tareas: **Manualmente**.
- En los parámetros de las directivas de prueba:
  - Desactive las tecnologías de aceleración de análisis iChecker y iSwift (**Protección esencial frente a amenazas → Protección frente a amenazas en archivos → Configuración → Adicional → Tecnologías de análisis**).
  - Seleccione qué hacer con los objetos infectados: **Desinfectar; eliminar si falla la desinfección** / **Desinfectar; bloquear si falla la desinfección** / **Bloquear**. (**Protección esencial frente a amenazas → Protección frente a amenazas en archivos → Acción sobre la detección de amenazas**).
- En los parámetros de las directivas de prueba y de las tareas auxiliares:

Si es necesario reiniciar el dispositivo después de la instalación de las actualizaciones de módulos de software, deberá realizarse inmediatamente. Si no se reinicia el dispositivo, es imposible probar este tipo de actualizaciones. Para algunas aplicaciones, la instalación de actualizaciones que requieren un reinicio puede prohibirse o configurarse para solicitar primero la configuración del usuario. Estas restricciones deberían deshabilitarse en los parámetros de las directivas de prueba y de las tareas auxiliares.

Visualización de actualizaciones descargadas

Para ver la lista de actualizaciones descargadas,

En el árbol de consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Actualizaciones de módulos de software y bases de datos de Kaspersky**.

El espacio de trabajo de la carpeta **Actualizaciones de módulos de software y bases de datos de Kaspersky** muestra la lista de actualizaciones guardadas en el Servidor de administración.

Instalación automática de actualizaciones de Kaspersky Endpoint Security en dispositivos

Puede configurar las actualizaciones automáticas de bases de datos y módulos de software de Kaspersky Endpoint Security en los dispositivos cliente.

Para configurar la descarga y la instalación automática de actualizaciones de Kaspersky Endpoint Security en dispositivos cliente:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. Para crear una tarea **Actualizar**, siga uno de estos procedimientos:
   - Seleccione **Nuevo → Tarea** en el menú contextual de la carpeta **Tareas** en el árbol de la consola.
   - Haga clic en el botón **Nueva tarea** en el espacio de trabajo de la carpeta **Tareas**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. En la página **Seleccionar el tipo de tarea**, seleccione **Kaspersky Endpoint Security** como tipo de tarea y luego seleccione **Actualizar** como el subtipo de tarea.
4. Siga el resto de instrucciones del Asistente.

   Una vez que haya finalizado el Asistente, se crea una tarea de actualización para Kaspersky Endpoint Security. La tarea recién creada se muestra en la lista de tareas en el espacio de trabajo de la carpeta **Tareas**.
5. En el espacio de trabajo de la carpeta **Tareas**, seleccione la tarea de actualización que ha creado.
6. En el menú contextual de la tarea, seleccione **Propiedades**.
7. En la ventana de propiedades de la tarea que se abre, en el panel **Secciones**, seleccione **Opciones**.

   En la sección **Opciones**, puede configurar la tarea de actualización en modo local u móvil:

- **Configuración de actualización para modo local**: se establece una conexión entre el Servidor de administración y el dispositivo.

- **Configuración de actualización para el modo móvil**: no se establece conexión entre Kaspersky Security Center y el dispositivo (por ejemplo, cuando el dispositivo no está conectado a Internet).

8. Haga clic en el botón **Configuración** para seleccionar la fuente de actualizaciones.

9. Seleccione la opción **Descargar actualizaciones del módulo de la aplicación** para descargar e instalar actualizaciones del módulo de software junto con las bases de datos de la aplicación.

   Si se selecciona la casilla, Kaspersky Endpoint Security informa al usuario de que existen actualizaciones del módulo de software disponibles y las incluye en el paquete de actualización cuando se ejecuta la tarea correspondiente. Configure el uso de los módulos de actualización:

   - **Instalar actualizaciones críticas y aprobadas**: Si hay actualizaciones disponibles para los módulos de software, Kaspersky Endpoint Security instala automáticamente aquellos que tienen un estado *Crítico*; las actualizaciones restantes se instalarán después de que las apruebe.

   - **Instalar solo las actualizaciones aprobadas**: Si hay disponibles actualizaciones de módulos de software, Kaspersky Endpoint Security las instala después de que se apruebe su instalación; se instalarán localmente a través de la interfaz de la aplicación o a través de Kaspersky Security Center.

   Si actualizar el módulo de software requiere revisar y aceptar las condiciones del Contrato de licencia y la Política de privacidad, la aplicación instala las actualizaciones una vez que el usuario ha aceptado las condiciones del Contrato de licencia y la Política de privacidad.

10. Seleccione la opción **Copiar actualizaciones a la carpeta** para que la aplicación guarde las actualizaciones descargadas en una carpeta y luego haga clic en el botón **Examinar** para especificar la carpeta.

11. Haga clic en **Aceptar**.

Al ejecutar la tarea **Actualizar**, la aplicación envía solicitudes a los servidores de actualización de Kaspersky.

Algunas actualizaciones requieren la instalación de las últimas versiones de complementos de administración.

Modelo de descarga de actualizaciones sin conexión

A veces, el Agente de red de dispositivos administrados no se pueden conectar al Servidor de administración para recibir actualizaciones. Por ejemplo, Agente de red puede haberse instalado en un equipo portátil que a veces no tiene conexión a Internet ni acceso a la red local. También es posible que el administrador limite el tiempo de conexión de los dispositivos a la red. En estos casos, los dispositivos del Agente de red instalado no puede recibir actualizaciones del Servidor de administración según la programación existente. Si ha configurado la actualización de aplicaciones administradas (como Kaspersky Endpoint Security) utilizando Agente de red, cada actualización requerirá una conexión al Servidor de administración. Cuando no se establece conexión entre Agente de red y el Servidor de administración, la actualización no es posible. Puede configurar la conexión entre Agente de red y el Servidor de administración para que el primero conecte con el segundo en intervalos de tiempo especificados. En el peor de los casos, si los intervalos de conexión especificados se cubren con períodos en los que no hay conexión disponible, las bases de datos nunca se actualizarán. Además, pueden surgir problemas cuando varias aplicaciones administradas intentan acceder simultáneamente al Servidor de administración para recibir actualizaciones. En este caso, el Servidor de administración puede dejar de responder a solicitudes (de forma parecida a un ataque DDoS).

Para evitar problemas como los descritos anteriormente, el modelo de descarga de actualizaciones sin conexión y módulos de aplicaciones administradas se implementa en Kaspersky Security Center. Este modelo proporciona un mecanismo para la distribución de actualizaciones, sin tener en cuenta problemas temporales causados por la inaccesibilidad de canales de comunicación del Servidor de administración. El modelo también reduce la carga en el Servidor de administración.

Funcionamiento del modelo de descarga de actualizaciones sin conexión

Cuando el Servidor de administración recibe actualizaciones, notifica al Agente de red (en los dispositivos donde está instalado) las actualizaciones que serán necesarias para las aplicaciones administradas. Cuando el Agente de red recibe la información sobre las actualizaciones, descarga por anticipado los archivos relevantes desde el Servidor de administración. En la primera conexión con el Agente de red, el Servidor de administración inicia una descarga de actualización. Una vez que el Agente de red descarga todas las actualizaciones a un dispositivo cliente, las actualizaciones estarán disponibles para las aplicaciones en ese dispositivo.

Cuando una aplicación administrada de un dispositivo cliente intenta acceder al Agente de red para descargar actualizaciones, el Agente de red comprueba si tiene todas las actualizaciones necesarias. Si las actualizaciones se reciben desde el Servidor de administración no más de 25 horas antes de que la aplicación administrada las solicite, el Agente de red no se conecta al Servidor de administración, sino que proporciona actualizaciones desde el caché local a la aplicación administrada. Es posible que la conexión con el Servidor de administración no se establezca cuando el Agente de red proporciona actualizaciones para las aplicaciones en los dispositivos cliente, pero no se requiere conexión para la actualización.

Para distribuir la carga en el Servidor de administración, el Agente de red se conecta al Servidor de administración y descargan actualizaciones en un orden aleatorio durante el intervalo de tiempo especificado por el Servidor de administración. Este intervalo de tiempo depende de la cantidad de dispositivos con Agente de red que descarguen actualizaciones y del tamaño de esas actualizaciones. Para reducir la carga del Servidor de administración, puede utilizar el Agente de red como puntos de distribución.

Si el modelo de descarga de actualizaciones sin conexión está desactivado, las actualizaciones se distribuyen de acuerdo con el programa de la tarea de descarga de actualizaciones.

De forma predeterminada, el modelo de descarga de actualizaciones sin conexión está habilitado.

El modelo de descarga de actualizaciones sin conexión solo se usa con los dispositivos administrados en los cuales la tarea para recuperar actualizaciones mediante aplicaciones administradas tiene la opción **Cuando se descargan nuevas actualizaciones en el repositorio** seleccionada como tipo de planificación. Para los demás dispositivos administrados, la planificación estándar se utiliza para recuperar actualizaciones desde el Servidor de administración en modo tiempo real.

Recomendamos que desactive el modelo de descarga de actualizaciones sin conexión usando la configuración de las directivas del Agente de red de los grupos de administración correspondientes en estos casos: si las aplicaciones administradas tienen configurada la recuperación de actualizaciones no desde el Servidor de administración, sino desde los servidores de Kaspersky o desde una carpeta de la red, y si la tarea de descarga de actualizaciones tiene la opción **Cuando se descargan nuevas actualizaciones en el repositorio** seleccionada como tipo de planificación.

Activación y desactivación del modelo de descarga de actualizaciones sin conexión

Recomendamos que evite deshabilitar el modelo de descarga de actualizaciones sin conexión. Desactivarlo puede causar fallos en la entrega de actualización a dispositivos. En ciertos casos, un especialista del Servicio de soporte técnico de Kaspersky puede recomendar que desactive la casilla **Descargar actualizaciones y bases de datos antivirus desde el Servidor de administración con antelación**. Luego, se tendrá que asegurar de que se haya configurado la tarea para recibir actualizaciones para aplicaciones de Kaspersky.

Para habilitar o deshabilitar el modelo de descarga de actualizaciones sin conexión para un grupo de administración:

1. En el árbol de consola, seleccione el grupo de administración para el que desea configurar el modelo de descarga de actualizaciones sin conexión.
2. En el espacio de trabajo del grupo, abra la ficha **Directivas**.
3. En la ficha **Directivas** seleccione la directiva del Agente de red.
4. En el menú contextual de la directiva, seleccione **Propiedades**.

   Abra la ventana de propiedades de la directiva del Agente de red.
5. En la ventana de propiedades de la directiva, seleccione la ficha **Administrar parches y actualizaciones**.
6. Seleccione o borre la casilla de verificación **Descargar actualizaciones y bases de datos antivirus del Servidor de administración (recomendado)** para habilitar o deshabilitar respectivamente el modelo de descarga de actualizaciones sin conexión.

   De forma predeterminada, el modelo de descarga de actualizaciones sin conexión está habilitado.

Se habilitará o deshabilitará el modelo de descarga de actualizaciones sin conexión.

Actualización automática y parches para componentes de Kaspersky Security Center

De forma predeterminada, cualquier actualización y parche que se haya descargado se instala automáticamente para los siguientes componentes de la aplicación (a partir de la versión 10 Service Pack 2):

- Agente de red para Windows
- Consola de administración

- Servidor de dispositivos móviles de Exchange
- Servidor de MDM para iOS

La actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center están disponibles solo para dispositivos que ejecutan Windows. Puede deshabilitar la actualización automática y los parches para estos componentes. En este caso, cualquier actualización y parche que se haya descargado se instalarán únicamente después de que cambie su estado a *Aprobado*. Las actualizaciones y los parches con el estado *Sin definir* no se instalarán.

Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center

La instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center está habilitada de forma predeterminada durante la instalación del Agente de red en el dispositivo. Puede deshabilitarla durante la instalación del Agente de red o más adelante usando una directiva.

Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center durante instalación local del Agente de red en un dispositivo, realice lo siguiente:

1. Inicie la instalación local del Agente de red en el dispositivo.
2. En el paso **Configuración avanzada**, desactive la casilla **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir**.
3. Siga las instrucciones del Asistente.

Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center deshabilitados en el dispositivo. Puede habilitar la actualización automática y los parches más adelante usando una directiva.

Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center durante la instalación del Agente de red en el dispositivo mediante un paquete de instalación, realice lo siguiente:

1. En el árbol de consola, seleccione la carpeta **Instalación remota → Paquetes de instalación**.
2. En el menú contextual del paquete **Agente de red de Kaspersky Security Center <número de versión>**, seleccione **Propiedades**.
3. En las propiedades del paquete de instalación, en la sección **Configuración**, borre la casilla de verificación **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir**.

Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center deshabilitados de este paquete. Puede habilitar la actualización automática y los parches más adelante usando una directiva.

Si esta casilla se seleccionó (o se desactivó) durante la instalación del Agente de red en el dispositivo, puede habilitar posteriormente (o deshabilitar) la actualización automática usando la directiva del Agente de red.

Para habilitar o deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center usando la directiva del Agente de red, realice lo siguiente:

1. En el árbol de consola, seleccione el grupo de administración para el que desea habilitar o deshabilitar la actualización automática y los parches.
2. En el espacio de trabajo del grupo, abra la ficha **Directivas**.
3. En la ficha **Directivas** seleccione la directiva del Agente de red.
4. En el menú contextual de la directiva, seleccione **Propiedades**.

   Abra la ventana de propiedades de la directiva del Agente de red.
5. En la ventana de propiedades de la directiva, seleccione la ficha **Administrar parches y actualizaciones**.
6. Seleccione o borre la casilla de verificación **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir** para activar o desactivar respectivamente actualizaciones y parches automáticos.
7. Configure el bloqueo para esta casilla.

La directiva se aplicará a los dispositivos seleccionados y la actualización automática y los parches para los componentes de Kaspersky Security Center se habilitarán (o se deshabilitarán) en estos dispositivos.

Distribución automática de las actualizaciones

Kaspersky Security Center permite la distribución e instalación automática de actualizaciones en dispositivos cliente y Servidores de administración secundarios.

Distribución automática de actualizaciones en dispositivos cliente

Para distribuir las actualizaciones de la aplicación seleccionada en los dispositivos cliente automática e inmediatamente después de la descarga de las actualizaciones en el repositorio del Servidor de administración:

1. Conecte al Servidor de administración que administra los dispositivos cliente.
2. Cree una tarea de despliegue de actualizaciones para los dispositivos cliente seleccionados de una de las siguientes formas:

   - Si necesita distribuir actualizaciones en los dispositivos cliente que pertenecen al grupo de administración seleccionado, cree una tarea para el grupo seleccionado.
   - Si necesita distribuir actualizaciones en los dispositivos cliente que pertenecen a diferentes grupos de administración o que no pertenecen a ninguno, cree una tarea para dispositivos específicos.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones y realice estos pasos:

   a. En la ventana del Asistente **Tipo de tarea** del nodo de la aplicación requerida, seleccione la tarea de despliegue de actualizaciones.

El nombre de la tarea de despliegue de actualizaciones mostrado en la ventana **Tipo de tarea** depende de la aplicación para la que cree la tarea. Para obtener información detallada acerca de los nombres de tareas de actualización de las aplicaciones Kaspersky seleccionadas, consulte las Guías correspondientes.

b. En la ventana del Asistente de **Programación**, en el campo **Inicio programado**, seleccione **Cuando se descargan nuevas actualizaciones en el repositorio**.

La tarea de distribución de actualizaciones recién creada se iniciará en los dispositivos seleccionados cada vez que se descarguen las actualizaciones en el repositorio del Servidor de administración.

Si ya se ha creado una tarea de distribución de actualizaciones de la aplicación requerida para los dispositivos seleccionados, con el fin de distribuir actualizaciones automáticamente en los dispositivos cliente, en la ventana de propiedades de la tarea de la sección **Programación**, seleccione la opción **Cuando se descargan nuevas actualizaciones en el repositorio** en el campo **Inicio programado**.

Distribución automática de actualizaciones en Servidores de administración secundarios

Para distribuir las actualizaciones de la aplicación seleccionada en los Servidores de administración secundarios inmediatamente después de la descarga de las actualizaciones en el repositorio del Servidor de administración principal:

1. En el árbol de consola, en el nodo del Servidor de administración principal, seleccione la carpeta **Tareas**.
2. En la lista de tareas del espacio de trabajo, seleccione la tarea del Servidor de administración de actualizaciones de descarga al repositorio del Servidor de administración.
3. Abra la sección **Configuración** de la tarea seleccionada por alguno de los siguientes medios:
   - Seleccione **Propiedades** en el menú contextual de la tarea.
   - Haga clic en el enlace **Modificar configuración** en el cuadro de información de la tarea seleccionada.
4. En la sección **Configuración** de la ventana de propiedades de la tarea, seleccione la subsección **Otros parámetros** y haga clic en el enlace **Configurar**.
5. En la ventana **Otros parámetros** que se abrirá, seleccione la casilla **Forzar actualización en los Servidores de administración secundarios**.

En los parámetros de la tarea de descarga de actualizaciones del Servidor de administración, en la ficha **Configuración** de la ventana propiedades de la tarea, seleccione la casilla **Forzar actualización en los Servidores de administración secundarios**.

Después de que el Servidor de administración principal recupera las actualizaciones, las tareas de descarga de actualizaciones se iniciarán automáticamente en los Servidores de administración secundarios sin tener en cuenta la planificación.

Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. Kaspersky Security Center seleccionará por sí mismo a qué dispositivos se les deben asignar puntos de distribución.

Para asignar puntos de distribución automáticamente:

1. Abra la ventana principal de la aplicación.
2. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración para el que desea asignar puntos de distribución automáticamente.
3. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
4. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Puntos de distribución**.
5. En la parte derecha de la ventana, seleccione la opción **Asignar automáticamente puntos de distribución**.

   Si la asignación automática de dispositivos para que actúen como puntos de distribución está activada, no se pueden configurar los puntos de distribución manualmente ni editar la lista de puntos de distribución.

6. Haga clic en **Aceptar**.

El Servidor de administración asigna y configura puntos de distribución automáticamente.

Asignación manual de un dispositivo a un punto de distribución

Kaspersky Security Center le permite asignar dispositivos para actuar como puntos de distribución.

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center seleccionará por sí mismo a qué dispositivos se les deben asignar puntos de distribución. Sin embargo, si tiene que optar por no asignar automáticamente puntos de distribución por cualquier motivo (por ejemplo, si desea usar servidores asignados exclusivamente), puede asignar puntos de distribución manualmente después de calcular su número y configuración.

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Para designar manualmente un dispositivo para actuar como punto de distribución:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Puntos de distribución** y haga clic en el botón **Agregar**. Este botón está disponible si **Asignar manualmente puntos de distribución** ha sido seleccionado.

   Se abre la ventana **Agregar un punto de distribución**.

4. En la ventana **Agregar un punto de distribución**, realice las siguientes acciones:

   a. Seleccione un dispositivo que actuará como punto de distribución (seleccione uno en un grupo de administración o especifique la dirección IP de un dispositivo). Al seleccionar un dispositivo, recuerde las características de operación de puntos de distribución y el conjunto de requisitos para el dispositivo que actúa como punto de distribución.

   b. Indique los dispositivos específicos a los que el punto de distribución distribuirá actualizaciones. Puede especificar un grupo de administración o una descripción de ubicación de red.

5. Haga clic en **Aceptar**.

   El punto de distribución que ha añadido se mostrará en la lista de puntos de distribución, en la sección **Puntos de distribución**.

6. Seleccione el punto de distribución añadido en la lista y haga clic en el botón **Propiedades** para abrir su ventana de propiedades.

7. Configure el punto de distribución perfil en la ventana de propiedades:

   - La sección **General** contiene los parámetros que regulan la interacción del punto de distribución con los dispositivos cliente.

     - **Puerto SSL**

       El número del puerto SSL para la conexión cifrada entre los dispositivos cliente y el punto de distribución usando SSL.

       De forma predeterminada, se utiliza el puerto 13000.

     - **Usar difusión múltiple**

       Si se selecciona esta opción, se utilizará la multidifusión IP para la distribución automática de paquetes de instalación en dispositivos cliente dentro del grupo.

       La multidifusión IP disminuye el tiempo requerido para instalar una aplicación desde un paquete de instalación hacia un grupo de dispositivos cliente, pero aumenta el tiempo de instalación cuando instala una aplicación en un único dispositivo cliente.

     - **Dirección IP de difusión múltiple**

       La dirección IP que se utilizará para la multidifusión. Puede definir una dirección IP en el rango de 224.0.0.0 – 239.255.255.255

       De manera predeterminada, Kaspersky Security Center asigna automáticamente una dirección IP de multidifusión única dentro del rango dado.

     - **Número de puerto de multidifusión IP**

       Número del puerto para multidifusión IP.

       De forma predeterminada el número de puerto es el 15001. Si el dispositivo que tiene el Servidor de administración instalado está configurado como punto de distribución, de forma predeterminada se utiliza el puerto 13001 para la conexión SSL.

     - **Desplegar actualizaciones**

Las actualizaciones se distribuyen a los dispositivos administrados desde los siguientes orígenes:

- Este punto de distribución, si esta opción está activada.
- Otros puntos de distribución, Servidor de administración o servidores de actualización de Kaspersky, si esta opción está desactivada.

Si usa puntos de distribución para implementar actualizaciones, puede ahorrar tráfico dado que se reduce la cantidad de descargas. Además, puede aliviar la carga en el Servidor de administración y reubicarla entre los puntos de distribución. Puede calcular el número de puntos de distribución de su red para optimizar el tráfico y la carga.

Si desactiva esta opción, puede aumentar el número de descargas de actualizaciones y la carga en el Servidor de administración. Esta opción está activada de forma predeterminada.

- **Desplegar paquetes de instalación**

  Los paquetes de instalación se distribuyen a los dispositivos administrados desde las siguientes fuentes:

  - Este punto de distribución, si esta opción está activada.
  - Otros puntos de distribución, Servidor de administración o servidores de actualización de Kaspersky, si esta opción está desactivada.

  Si usa puntos de distribución para implementar paquetes de instalación, puede ahorrar tráfico dado que se reduce la cantidad de descargas. Además, puede aliviar la carga en el Servidor de administración y reubicarla entre los puntos de distribución. Puede calcular el número de puntos de distribución de su red para optimizar el tráfico y la carga.

  Si desactiva esta opción, puede aumentar la cantidad de descargas de paquetes de instalación y la carga en el Servidor de administración. Esta opción está activada de forma predeterminada.

- **Use este punto de distribución como servidor push**

  En Kaspersky Security Center, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil. Por ejemplo, se debe activar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se activa el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede activar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

  Si administra dispositivos con KasperskyOS instalado, o tiene pensado hacerlo, debe utilizar un punto de distribución como servidor push. También puede utilizar un punto de distribución como servidor push si desea enviar notificaciones push a los dispositivos cliente.

- **Puerto del servidor push**

  El puerto del punto de distribución que los dispositivos cliente usarán para la conexión. De forma predeterminada, se utiliza el puerto 13295.

- En la sección **Cobertura**, especifique el ámbito en el que el punto de distribución distribuirá actualizaciones (grupos de administración y/o ubicación de la red).
- En la sección **Proxy de KSN**, puede configurar la aplicación para utilizar el punto de distribución para reenviar solicitudes de KSN desde los dispositivos administrados.

- **Activar el proxy de KSN en el punto de distribución**

  El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico en la red.

  El punto de distribución envía a Kaspersky las estadísticas de KSN, que se incluyen en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se guarda en %Archivos de programa%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Esta opción está desactivada de forma predeterminada. Esta opción solo se activa si las opciones **Utilizar el Servidor de administración como servidor proxy** y **Acepto usar Kaspersky Security Network** están activadas en la ventana de propiedades del Servidor de administración.

  Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y activar el proxy de KSN en ese nodo.

- **Reenviar solicitudes de KSN al Servidor de administración**

  El punto de distribución reenvía las solicitudes KSN de los dispositivos administrados al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- **Acceder a la nube de KSN / KSN privada directamente a través de Internet**

  El punto de distribución reenvía las solicitudes de KSN de los dispositivos administrados a KSN Cloud o KSN privada. Las solicitudes de KSN generadas en el punto de distribución también se envían directamente a KSN Cloud o KSN privada.

  Los puntos de distribución que tienen instalado el Agente de red versión 11 (o versiones anteriores) no pueden acceder a KSN Privada directamente. Si desea reconfigurar los puntos de distribución para enviar solicitudes KSN a KSN Privada, active la opción **Reenviar solicitudes de KSN al Servidor de administración** para cada punto de distribución.

  Los puntos de distribución que tienen instalado el Agente de red versión 12 (o versiones posteriores) pueden acceder a KSN privada directamente.

- **Ignorar la configuración del servidor proxy KSC al conectarse a KSN privada**

  Active esta opción si tiene las opciones del servidor proxy configuradas en las propiedades del punto de distribución o en la directiva de Agente de red, pero su arquitectura de red requiere que use KSN privada directamente. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a la KSN privada.

- **Puerto TCP**

  El número del puerto de TCP que los dispositivos administrados utilizarán para conectar al Servidor proxy de KSN. El número de puerto predeterminado es el 13111.

- **Puerto UDP**

  Si necesita que los dispositivos administrados se conecten al Servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado de conexión al Servidor proxy de KSN es 15111.

- En la sección **Detección de dispositivos**, configure el sondeo de los dominios de Windows, Active Directory y rangos IP por parte del punto de distribución.

  - **Dominios de Windows**

    Puede habilitar la detección de dispositivos para los dominios de Windows y establecer la programación para el descubrimiento.

  - **Active Directory**

    Puede activar el sondeo de red para Active Directory y establecer la programación para el sondeo.

    Si selecciona la casilla de verificación **Activar sondeo de red**, puede seleccionar una de las siguientes opciones:

    - **Analizar el dominio actual de Active Directory**.
    - **Analizar el bosque de dominio de Active Directory**.
    - **Analizar solo los dominios seleccionados de Active Directory**. Si selecciona esta opción, añada uno o más dominios de Active Directory a la lista.

  - **Rangos IP**

    Puede activar la detección de dispositivos para los rangos IPv4 y las redes IPv6.

    Si activa la opción **Activar rango de sondeo**, puede añadir rangos analizados y establecer la programación para ellos. Puede añadir rangos de IP a la lista de intervalos analizados.

    Si activa la opción **Activar el sondeo con la tecnología Zeroconf**, el punto de distribución automáticamente sondea la red IPv6 mediante el uso de las redes de configuración cero (también denominadas *Zeroconf*). En este caso, los rangos de IP especificados se ignoran, porque el punto de distribución sondea toda la red.

- En la sección **Avanzado**, especifique la carpeta que debe utilizar el punto de distribución para almacenar datos distribuidos.

  - **Usar carpeta predeterminada**

    Si selecciona esta opción, la aplicación usará la carpeta de instalación de Agente de red en el punto de distribución.

  - **Usar carpeta especificada**

    Si se selecciona esta opción, se podrá especificar la ruta de la carpeta en el campo siguiente. Puede ser una carpeta local en el punto de distribución, o bien un directorio remoto en cualquier dispositivo de la red corporativa.

    La cuenta de usuario utilizada en el punto de distribución para ejecutar el Agente de red debe tener acceso de lectura y escritura a la carpeta especificada.

Los dispositivos seleccionados se comportan como puntos de distribución.

Solo los dispositivos con sistema operativo Windows pueden determinar su ubicación de red. No se puede determinar la ubicación de red para dispositivos que ejecuten otros sistemas operativos.

Eliminación de un dispositivo de la lista de puntos de distribución

Para eliminar un dispositivo de la lista de puntos de distribución:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, en la sección **Puntos de distribución**, seleccione un dispositivo que funcione como punto de distribución y haga clic en el botón **Quitar**.

El dispositivo se eliminará de la lista de puntos de distribución y dejará de actuar como punto de distribución.

Un dispositivo no se puede eliminar desde la lista de puntos de distribución si el Servidor de administración lo ha asignado automáticamente.

Descargar actualizaciones por puntos de distribución

Kaspersky Security Center permite que los puntos de distribución reciban actualizaciones del Servidor de administración, de los servidores de Kaspersky o de una carpeta local o en red.

Para configurar la descarga de actualizaciones para un punto de distribución:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, en la sección **Puntos de distribución**, seleccione el punto de distribución a través del cual se entregarán las actualizaciones a los dispositivos cliente en el grupo.
4. Haga clic en el botón **Propiedades** para abrir la ventana de propiedades del punto de distribución seleccionado.
5. En la ventana de propiedades del punto de distribución, seleccione la sección **Orígenes de actualizaciones**.
6. Seleccione una fuente de actualización para el punto de distribución:
   - Para permitir al punto de distribución recibir actualizaciones del Servidor de administración, seleccione **Recuperar del Servidor de administración**:
     - **Descargar archivos diff**

       Esta opción habilita la función de descarga de archivos diff.

       Esta opción está activada de forma predeterminada.

- Para permitir que el punto de distribución reciba actualizaciones mediante una tarea, seleccione **Utilizar la tarea para la descarga forzada de actualizaciones**:
  - Haga clic en el botón **Examinar** si dicha tarea ya existe en el dispositivo y seleccione la tarea en la lista que aparece.
  - Haga clic en el botón **Nueva tarea** para crear una tarea si aún no existe dicha tarea en el dispositivo. Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

  La tarea de Descargar actualizaciones en los repositorios de puntos de distribución es una tarea local. Se debe crear una nueva tarea para cada dispositivo que actúe como punto de distribución.

El punto de distribución recibirá actualizaciones del origen especificado.

Eliminación de actualizaciones de software desde el repositorio

Para eliminar actualizaciones de software del repositorio del Servidor de administración:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.
2. En el espacio de trabajo de la carpeta **Actualizaciones de software**, seleccione la actualización que desea eliminar.
3. En el menú contextual de la actualización, seleccione **Eliminar archivos de actualización**.

Las actualizaciones de software se eliminarán del repositorio del Servidor de administración.

Instalación de parches para una aplicación de Kaspersky en modo de clúster

Kaspersky Security Center solo admite la instalación manual de parches para Aplicaciones de Kaspersky en modo de clúster.

Para instalar un parche para una Aplicación de Kaspersky:

1. Descargue el parche a cada nodo del clúster.
2. Ejecute la instalación del parche en el nodo activo.
3. Espere que el parche se instale correctamente.
4. Ejecute el parche consecutivamente en todos los subnodos del clúster.

   Si está ejecutando el parche desde la línea de comandos, use la clave `-CLUSTER_SECONDARY_NODE`.

   El parche ahora está instalado en todos los nodos del clúster.
5. Ejecutar manualmente los servicios del clúster de Kaspersky.

Cada nodo del clúster se muestra en la Consola de administración como un dispositivo con el Agente de red instalado.

Para obtener información sobre los parches instalados, vea la carpeta **Actualizaciones de software** o el informe sobre las versiones de actualizaciones para módulos de software de las aplicaciones de Kaspersky.

Administrar aplicaciones de terceros en dispositivos cliente

Kaspersky Security Center permite administrar las aplicaciones de Kaspersky y de otros vendedores que estén instaladas en los dispositivos cliente.

El administrador puede realizar las siguientes acciones:

- Crear categorías de aplicaciones basadas en criterios específicos.
- Administrar categorías de aplicaciones mediante reglas creadas especialmente para este fin.
- Administrar la ejecución de aplicaciones en los dispositivos.
- Realizar un inventario y mantener un registro del software instalado en los dispositivos.
- Reparar vulnerabilidades en el software instalado en los dispositivos.
- Instalar actualizaciones de Windows Update y otros desarrolladores de software en los dispositivos.
- Supervisar el uso de claves de licencia para grupos de aplicaciones con licencia.

Instalar actualizaciones de software de terceros

Kaspersky Security Center le permite administrar las actualizaciones de software instaladas en los dispositivos cliente y reparar las vulnerabilidades en las aplicaciones de Microsoft y los productos de otros desarrolladores de software mediante la instalación de las actualizaciones requeridas.

Kaspersky Security Center busca actualizaciones con la tarea de búsqueda correspondiente y las descarga en el repositorio de las actualizaciones. Una vez que finalice la búsqueda de actualizaciones, la aplicación proporciona al administrador información acerca de las actualizaciones y vulnerabilidades disponibles en las aplicaciones que se pueden reparar mediante dichas actualizaciones.

La información sobre las actualizaciones disponibles para Microsoft Windows la proporciona el servicio de Windows Update. El Servidor de administración se puede usar como servidor de Windows Server Update Services (WSUS). Para utilizar el Servidor de administración como servidor de WSUS, debe configurar la sincronización de las actualizaciones con Windows Update. Tras configurar la sincronización de los datos con Windows Update, el Servidor de administración proporciona actualizaciones a los servicios de Windows Update en los dispositivos de forma centralizada y con la frecuencia definida.

Además, también puede administrar actualizaciones de software con una directiva de Agente de red. Para ello, debe crear una directiva de Agente de red y configurar la actualización de software en las ventanas correspondientes del Asistente de nueva directiva.

El administrador puede ver una lista de actualizaciones disponibles en la subcarpeta **Actualizaciones de software** que se encuentra en la carpeta **Administración de aplicaciones**. Esta carpeta incluye una lista de actualizaciones para las aplicaciones de Microsoft y los productos de otros desarrolladores de software recuperadas por el Servidor de administración y que se pueden distribuir a los dispositivos. Después de consultar la información acerca de las actualizaciones disponibles, el administrador puede instalarlas en los dispositivos.

Kaspersky Security Center actualiza algunas aplicaciones quitando la versión anterior de la aplicación e instalando la nueva.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Por razones de seguridad, las tecnologías de Kaspersky analizan automáticamente en busca de malware cualquier actualización de software de terceros que instale mediante la función Administración de vulnerabilidades y parches. Estas tecnologías se utilizan para la verificación automática de archivos e incluyen análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno aislado y aprendizaje automático.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Además, los expertos de Kaspersky no buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en dichas actualizaciones, ni realizan otros tipos de análisis de las actualizaciones distintos a los especificados en el párrafo anterior.

Antes de instalar las actualizaciones en todos los dispositivos, puede realizar una instalación de prueba para asegurarse de que las actualizaciones instaladas no provocan ningún error en el funcionamiento de las aplicaciones de los dispositivos.

Puede encontrar los detalles del software de terceros que se puede actualizar a través de Kaspersky Security Center en el sitio web del Servicio de Soporte Técnico, ubicado en la sección Administración del servidor de la página de Kaspersky Security Center.

Escenario: actualización de software de terceros

Esta sección proporciona un escenario para actualizar software de terceros instalado en los dispositivos cliente. Software de terceros incluye aplicaciones de Microsoft y de otros proveedores. El servicio de Windows Update proporciona actualizaciones para las aplicaciones de Microsoft.

Requisitos previos

El Servidor de administración debe tener una conexión a Internet para instalar actualizaciones de software de terceros que no sean software de Microsoft.

De forma predeterminada, el Servidor de administración no requiere conexión a Internet para instalar actualizaciones de software de Microsoft en los dispositivos administrados. Por ejemplo, los dispositivos administrados pueden descargar las actualizaciones de software de Microsoft directamente desde los servidores de Microsoft Update o desde Windows Server con Microsoft Windows Server Update Services (WSUS) implementado en la red de su organización. El Servidor de administración debe estar conectado a Internet cuando utilice el Servidor de administración como servidor WSUS.

Etapas

La actualización de software de terceros se efectúa en etapas:

1. **Buscar actualizaciones requeridas**

   Para buscar las actualizaciones de software de terceros necesarias para los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el Asistente de inicio rápido del Servidor de administración. Si no ejecutó el Asistente, cree la tarea o ejecute el Asistente de inicio rápido ahora.

   Instrucciones:

   - Consola de administración: Análisis de aplicaciones para buscar vulnerabilidades, Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center 14 Web Console: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de actualizaciones encontradas**

   Vea la lista de **ACTUALIZACIONES DE SOFTWARE** y decida las actualizaciones que se instalarán. Para ver información detallada sobre cada actualización, haga clic en el nombre de la actualización en la lista. Para cada actualización de la lista, también puede ver las estadísticas sobre la instalación de la actualización en los dispositivos cliente.

   Instrucciones:

   - Consola de administración: Visualización de información acerca de las actualizaciones disponibles
   - Kaspersky Security Center 14 Web Console: Visualización de información sobre actualizaciones de software de terceros disponibles

3. **Configurar la instalación de actualizaciones**

   Una vez que Kaspersky Security Center recibe la lista de actualizaciones de software de terceros, usted puede instalarlas en los dispositivos cliente mediante las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Instalar actualizaciones de Windows Update*. Cree una de estas tareas. Puede crear estas tareas en la ficha **TAREAS** o desde la lista **ACTUALIZACIONES DE SOFTWARE**.

   La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft, incluidas las actualizaciones que proporciona el servicio Windows Update y las actualizaciones de productos de otros proveedores. Tenga en cuenta que esta tarea se puede crear únicamente si tiene la licencia para la función Administración de vulnerabilidades y parches.

   La tarea *Instalar actualizaciones de Windows Update* no requiere una licencia, pero se puede usar para instalar únicamente actualizaciones de Windows Update.

   Para instalar algunas actualizaciones de software, debe aceptar el Contrato de licencia de usuario final (EULA) para el software de instalación. Si rechaza el EULA, la actualización de software no se instalará.

   Puede iniciar una tarea de instalación de actualizaciones según una programación. Cuando especifique la programación de tareas, asegúrese de que la tarea de instalación de actualización comience después de que se complete la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

   Instrucciones:

   - Consola de administración: Reparación de las vulnerabilidades en las aplicaciones, Visualización de información acerca de las actualizaciones disponibles

- Kaspersky Security Center 14 Web Console: Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades, Crear la tarea Instalar actualizaciones de Windows Update, Visualización de información sobre actualizaciones de software de terceros disponibles

4. **Programar las tareas**

   Para asegurarse de que la lista de actualizaciones esté siempre actualizada, programe la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para que se ejecute de forma automática ocasionalmente. La frecuencia predeterminada es una vez a la semana.

   Si ha creado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Al programar la tarea *Instalar actualizaciones de Windows Update*, tenga en cuenta que debe definir la lista de actualizaciones para esta tarea cada vez antes de iniciarla.

   Cuando programe las tareas, asegúrese de que una tarea de instalación de actualización comience después de que se complete la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

5. **Aprobar y rechazar actualizaciones de software (opcional)**

   Si ha creado la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades, puede especificar reglas para instalar la actualización en las propiedades de la tarea. Si ha creado la tarea Instalar actualizaciones de Windows Update, omita este paso.

   Para cada regla, puede definir las actualizaciones que desea instalar según el estado de la actualización: *Sin definir*, *Aprobada* o *Rechazada*. Por ejemplo, puede que quiera crear una tarea específica para servidores y establecer una regla para dicha tarea que permita la instalación únicamente de actualizaciones de Windows Update y de aquellas que tengan el estado *Aprobada*. Después, debe establecer manualmente el estado *Aprobada* para las actualizaciones que desea instalar. En este caso, las actualizaciones de Windows Update que tienen el estado *Sin definir* o *Rechazada* no se instalarán en los servidores que haya especificado en la tarea.

   El uso del estado *Aprobado* para administrar la instalación de actualizaciones es eficiente para una pequeña cantidad de actualizaciones. Para instalar varias actualizaciones, utilice las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y corregir vulnerabilidades*. Le recomendamos que asigne el estado *Aprobado* solo a aquellas actualizaciones específicas que no cumplan con los criterios especificados en las reglas. Cuando aprueba manualmente una gran cantidad de actualizaciones, el rendimiento del Servidor de administración disminuye y puede provocar una sobrecarga en el Servidor de administración.

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *No definido*. Puede cambiar el estado a *Aprobado* o *Rechazado* en la lista **ACTUALIZACIONES DE SOFTWARE** (**OPERACIONES** → **ADMINISTRACIÓN DE PARCHES** → **ACTUALIZACIONES DE SOFTWARE**).

   Instrucciones:

   - Consola de administración: Aprobar y rechazar actualizaciones de software
   - Kaspersky Security Center 14 Web Console: Aprobar y rechazar actualizaciones de software de terceros

6. **Configuración del Servidor de administración para que funcione como un servidor del Servicio de Windows Server Update (WSUS) (opcional)**

   De manera predeterminada, las actualizaciones de Windows Update se descargan a los dispositivos administrados desde los servidores de Microsoft. Puede cambiar esta configuración para utilizar el Servidor de administración como servidor WSUS. En este caso, el Servidor de administración sincroniza los datos de la actualización con Windows Update en la frecuencia especificada y proporciona actualizaciones de modo centralizado a Windows Update en los dispositivos en red.

   Para utilizar el Servidor de administración como servidor WSUS, cree la tarea Realizar la sincronización de Windows Update y seleccione la casilla de verificación **Utilizar el Servidor de administración como servidor WSUS** en la directiva del Agente de red.

   Instrucciones:

   - Consola de administración: Sincronización de actualizaciones de Windows Update con el Servidor de administración, Configuración de actualizaciones de Windows en una directiva del Agente de red

- Kaspersky Security Center 14 Web Console: Creación de la tarea de sincronización Realizar la actualización de Windows Update

7. **Ejecutar una tarea de instalación de actualización**

   Inicie las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Instalar actualizaciones de Windows Update*. Cuando inicia estas tareas, las actualizaciones se descargan e instalan en los dispositivos administrados. Una vez completada la tarea, asegúrese de que tenga el estado *Completado correctamente* en la lista de tareas.

8. **Crear el informe sobre los resultados de la instalación de actualizaciones de software de terceros (opcional)**

   Para ver estadísticas detalladas sobre la instalación de la actualización, genere **Informe sobre los resultados de la instalación de actualizaciones de software de otros fabricantes**.

   Instrucciones:

   - Consola de administración: Creación y visualización de un informe
   - Kaspersky Security Center 14 Web Console: Generación y visualización de un informe

Resultados

Si ha creado y configurado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las actualizaciones se instalan en los dispositivos administrados automáticamente. Cuando se descargan actualizaciones nuevas en el repositorio del Servidor de administración, Kaspersky Security Center verifica si cumplen con los criterios especificados en las reglas de actualización. Todas las actualizaciones nuevas que cumplan con los criterios se instalarán automáticamente la próxima vez que se ejecute la tarea.

Si ha creado la tarea *Instalar actualizaciones de Windows Update*, solo se instalarán las actualizaciones especificadas en las propiedades de la tarea *Instalar actualizaciones de Windows Update*. En el futuro, si desea instalar nuevas actualizaciones descargadas en el repositorio del Servidor de administración, debe añadir las actualizaciones necesarias a la lista de actualizaciones en la tarea existente o crear una nueva tarea *Instalar actualizaciones de Windows Update*.

Visualización de información sobre actualizaciones disponibles para aplicaciones de terceros

Para ver una lista de actualizaciones disponibles para las aplicaciones de terceros instaladas en dispositivos cliente,

En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.

En el espacio de trabajo de la carpeta, puede visualizar una lista de las actualizaciones disponibles para las aplicaciones instaladas en los dispositivos.

Siga estos pasos para consultar las propiedades de una actualización:

En el espacio de trabajo de la carpeta **Actualizaciones de software**, seleccione **Propiedades** en el menú contextual de la actualización.

Puede verse la siguiente información en la ventana de propiedades de la actualización:

- En la sección **Control de aplicaciones** puede ver el **Actualizar el estado de autorización**:
  - **Sin definir**: la actualización está disponible en la lista de actualizaciones, pero no está aprobada para su instalación.
  - **Aprobada**: la actualización está disponible en la lista de actualizaciones y aprobada para su instalación.
  - **Rechazada**: se rechaza la instalación de la actualización.
- En la sección **Atributos**, puede ver los valores del campo **Instalado automáticamente**:
  - El valor **Automáticamente** se muestra si la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* puede instalar actualizaciones de la aplicación. La tarea instala automáticamente las nuevas actualizaciones de la dirección web proporcionada por el proveedor de software de terceros.
  - El valor **Manualmente** se muestra si Kaspersky Security Center no puede instalar las actualizaciones de la aplicación de modo automático. Puede instalar las actualizaciones de manera manual.

  El campo **Instalado automáticamente** no se muestra para las actualizaciones de la aplicación de Windows.
- Lista de dispositivos cliente para los cuales se destina la actualización.
- Lista de componentes del sistema (requisitos previos) que se deben instalar antes de la actualización (si existe).
- Vulnerabilidades de software que solucionará la actualización.

Aprobar y rechazar actualizaciones de software

La configuración de una tarea de instalación de actualizaciones puede requerir la aprobación de las actualizaciones que se van a instalar. Puede aprobar las actualizaciones que deben instalarse y rechazar las actualizaciones que no deben instalarse.

Por ejemplo, es posible que desee verificar primero la instalación de actualizaciones en un entorno de prueba y asegurarse de que no interfieran con el funcionamiento de los dispositivos y solo entonces permitir la instalación de estas actualizaciones en los dispositivos cliente.

El uso del estado *Aprobado* para administrar la instalación de actualizaciones de terceros es eficiente para una pequeña cantidad de actualizaciones. Para instalar varias actualizaciones de terceros, utilice las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y corregir vulnerabilidades*. Le recomendamos que asigne el estado *Aprobado* solo a aquellas actualizaciones específicas que no cumplan con los criterios especificados en las reglas. Cuando aprueba manualmente una gran cantidad de actualizaciones, el rendimiento del Servidor de administración disminuye y puede provocar una sobrecarga en el Servidor de administración.

Aprobar o rechazar una o varias actualizaciones:

1. En el árbol de consola, seleccione el nodo **Avanzado → Administración de aplicaciones → Actualizaciones de software**.
2. En el espacio de trabajo de la carpeta **Actualizaciones de software**, haga clic en el botón **Actualizar** en la esquina superior derecha. Aparece una lista de actualizaciones.
3. Seleccione las actualizaciones que desea aprobar o rechazar.

El cuadro de información para los objetos seleccionados aparece en el lado derecho del espacio de trabajo.

4. En la lista desplegable **Actualizar el estado de autorización**, seleccione **Aprobada** para aprobar las actualizaciones seleccionadas o **Rechazada** para rechazar las actualizaciones seleccionadas.

   El valor predeterminado es **Sin definir**.

Las actualizaciones para las que establece el estado **Aprobada** se colocan en una cola para la instalación.

Las actualizaciones para las cuales configure el estado **Rechazada** se desinstalarán (si es posible) de todos los dispositivos en los cuales se instalaron anteriormente. Además, no se instalarán en otros dispositivos en el futuro.

Algunas actualizaciones para aplicaciones de Kaspersky no pueden desinstalarse. Si configura el estado **Rechazada** para ellas, Kaspersky Security Center no desinstalará estas actualizaciones de los dispositivos en los cuales se hayan instalado anteriormente. Sin embargo, estas actualizaciones nunca se instalarán en otros dispositivos en el futuro. Si no se puede desinstalar una actualización para las aplicaciones de Kaspersky, esta propiedad se muestra en la ventana de propiedades de actualización: en el panel **Secciones**, seleccione **General**, y la propiedad aparecerá en **Requisitos de instalación** en el espacio de trabajo. Si configura el estado **Rechazada** para las actualizaciones de software de terceros, estas actualizaciones no se instalarán en los dispositivos cuya instalación se haya planeado pero aún no se haya realizado. Las actualizares permanecerán en los dispositivos en los cuales ya se hayan instalado. Si debe eliminarlas, puede eliminarlas manualmente en forma local.

Sincronización de actualizaciones de Windows Update con el Servidor de administración

Si ha seleccionado **Utilizar el Servidor de administración como servidor WSUS** en la ventana **Configuración de la administración de actualizaciones** del Asistente de inicio rápido, se crea automáticamente la tarea de sincronización Windows Update. Puede ejecutar la tarea en la carpeta **Tareas**. La funcionalidad de una actualización de software de Microsoft solo estará disponible una vez finalizada correctamente la tarea **Realizar la sincronización de Windows Update**.

La tarea **Realizar la sincronización de Windows Update** solo descarga metadatos de los servidores de Microsoft. Si la red no usa ningún servidor WSUS, cada dispositivo cliente descargará por su cuenta las actualizaciones de Microsoft desde servidores externos.

Siga estos pasos para crear una tarea de sincronización de Windows Update con el Servidor de administración:

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.

2. Haga clic en el botón **Acciones adicionales** y seleccione **Configurar la sincronización de Windows Update** en la lista desplegable.

   El Asistente crea la tarea **Realizar la sincronización de Windows Update** mostrada en la carpeta **Tareas**.

   Se inicia el Asistente para la creación de tareas de recuperación de datos del centro de actualizaciones de Windows. Siga las instrucciones del Asistente.

Además, también puede crear la tarea de sincronización de Windows Update en la carpeta **Tareas** haciendo clic en el enlace **Crear una tarea**.

Microsoft elimina periódicamente las actualizaciones obsoletas de los servidores de la empresa, por lo que la cantidad de actualizaciones actuales siempre se sitúa entre 200.000 y 300.000. En Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 y en las versiones anteriores, se conservaban todas las actualizaciones sin eliminar aquellas que se quedaban obsoletas. Por ese motivo, el tamaño de la base de datos aumentaba continuamente. Para reducir el uso de espacio en disco y el tamaño de la base de datos, en Kaspersky Security Center 10 Service Pack 3 se ha incluido la eliminación de actualizaciones obsoletas que ya no están presentes en los servidores de actualizaciones de Microsoft.

Al ejecutar la tarea **Realizar la sincronización de Windows Update**, la aplicación recibe una lista de actualizaciones en vigor desde un servidor de actualizaciones de Microsoft. A continuación, Kaspersky Security Center recopila una lista de actualizaciones que se han quedado obsoletas. En el próximo inicio de la tarea **Buscar vulnerabilidades y actualizaciones requeridas**, Kaspersky Security Center marca todas las actualizaciones obsoletas y define un plazo para eliminarlas. En el próximo inicio de la tarea **Realizar la sincronización de Windows Update**, se eliminan todas las actualizaciones marcadas para su eliminación hace 30 días. Kaspersky Security Center también comprueba si hay actualizaciones obsoletas que se marcaron para su eliminación hace más de 180 días y luego elimina esas actualizaciones más antiguas.

Cuando se completa la tarea **Realizar la sincronización de Windows Update** y se eliminan las actualizaciones obsoletas, la base de datos puede seguir teniendo los códigos hash correspondientes a los archivos de las actualizaciones eliminadas, así como los archivos correspondientes en los archivos %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (si se descargaron antes). Puede ejecutar la tarea **Mantenimiento del Servidor de administración** para eliminar estos registros obsoletos de la base de datos y los archivos correspondientes.

Paso 1. Definir la reducción de tráfico

Cuando Kaspersky Security Center sincroniza actualizaciones con Servidores de actualizaciones de Microsoft Windows, la información sobre todos los archivos se guarda en la base de datos del Servidor de administración. Todos los archivos necesarios para una actualización también se descargan en la unidad de disco durante la interacción con el Agente de Windows Update. En particular, Kaspersky Security Center guarda la información sobre archivos de actualización express en la base de datos y los descarga cuando sea necesario. Descargar archivos de actualización express supone reducir el espacio libre en la unidad de disco.

Para evitar una disminución en el volumen del espacio de disco y reducir el tráfico, puede desactivar la opción **Descargar archivos de instalación rápida**.

Si selecciona esta opción, los archivos de actualización rápida se descargan al ejecutar la tarea. Esta opción no está seleccionada de forma predeterminada.

Paso 2. Aplicaciones

En esta sección se pueden seleccionar las aplicaciones para las que se descargarán las actualizaciones.

Si la casilla **Todas las aplicaciones** se selecciona, las actualizaciones se descargarán para todas las aplicaciones existentes y para todas las aplicaciones que se puedan lanzar en el futuro.

De forma predeterminada, la casilla de verificación **Todas las aplicaciones** está seleccionada.

Paso 3. Categorías de actualización

En esta sección puede seleccionar las categorías de actualizaciones que se descargarán en el Servidor de administración.

Si la casilla **Todas las categorías** se selecciona, las actualizaciones se descargarán para todas las categorías de actualizaciones existentes y para todas las categorías que puedan aparecer en el futuro.

De forma predeterminada, la casilla de verificación **Todas las categorías** está seleccionada.

Paso 4. Idiomas de actualizaciones

En esta ventana puede especificar los idiomas de localización que se descargarán en el Servidor de administración. Seleccione una de las opciones siguientes para descargar idiomas de localización de actualizaciones:

- **Descargar todos los idiomas, incluso los nuevos**

  Si esta opción está seleccionada, todos los idiomas de localización disponibles de las actualizaciones que se descargarán en el Servidor de administración. Esta opción está seleccionada de forma predeterminada.

- **Descargar los idiomas seleccionados**

  Si esta opción está seleccionada, puede realizar selecciones en la lista de idiomas de localización de las actualizaciones que se deben descargar en el Servidor de administración.

Paso 5. Selección de una cuenta para iniciar la tarea

En la ventana **Seleccionar una cuenta para ejecutar la tarea**, puede especificar qué cuenta utilizar al ejecutar la tarea. Seleccione una de las siguientes opciones:

- **Cuenta preconfigurada**

  La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

  - **Cuenta**

    Cuenta bajo la que se ejecuta la tarea.

  - **Contraseña**

    La contraseña de la cuenta bajo la cual la tarea se ejecutará.

Paso 6. Configuración de la planificación del inicio de una tarea

En la página **Configurar programación de tareas** del Asistente, puede crear una planificación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

- **Inicio programado:**

  Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

  - **Cada N horas**

    La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

    De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

  - **Cada N días**

    La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

    De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

  - **Cada N semanas**

    La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

    De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

  - **Cada N minutos**

    La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

    De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

  - **Diario (no compatible con horario de verano)**

    La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

    No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

    De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

  - **Semanalmente**

    La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

  - **Por días de la semana**

La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Una vez**

  La tarea se ejecuta una vez en la fecha y a la hora especificadas.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

Esta opción está activada de forma predeterminada.

- **Usar un retraso aleatorio automático para el inicio de las tareas**

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

Paso 7. Definición del nombre de la tarea

En la ventana **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. Un nombre de tarea no puede tener más de 100 caracteres y no puede incluir ningún carácter especial (`"*<>?\:|`). El valor predeterminado es *Sincronizar Windows Update*.

Paso 8. Finalización de la creación de la tarea

En la ventana **Finalizar la creación de tareas**, haga clic en el botón **Finalizar** para cerrar el Asistente.

Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

La tarea recién creada de sincronización de Windows Update se muestra en la lista de tareas de la carpeta **Tareas** del árbol de consola.

Instalación manual de actualizaciones en dispositivos

Si ha seleccionado **Buscar e instalar las actualizaciones requeridas** en la página **Configuración de la administración de actualizaciones** del Asistente de inicio rápido, se crea automáticamente la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades. Puede ejecutar o detener la tarea en la carpeta **Dispositivos administrados** de la ficha **Tareas**.

Si ha seleccionado **Buscar actualizaciones requeridas** en el Asistente de inicio rápido, puede instalar las actualizaciones de software en dispositivos cliente a través de la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

Puede hacer lo siguiente:

- Crear una tarea para instalar actualizaciones.
- Añadir una regla para instalar una actualización en una tarea de instalación de la actualización existente.
- En la configuración de una tarea de instalación de actualización existente, configure una instalación de prueba de actualizaciones.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Instalar actualizaciones creando una tarea de instalación

Puede hacer lo siguiente:

- Crear una tarea para instalar ciertas actualizaciones.
- Seleccione una actualización y cree una tarea para instalarla y actualizaciones similares.

Instalar actualizaciones específicas:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.
2. En el espacio de trabajo, seleccione las actualizaciones que desea instalar.
3. Realice una de las siguientes acciones:
   - Haga clic con el botón derecho en una de las actualizaciones seleccionadas en la lista y luego seleccione **Instalar actualización** → **Nueva tarea**.

- Haga clic en el enlace **Instalar actualización (crear tarea)** en el cuadro de información para las actualizaciones seleccionadas.

4. Haga su elección en el aviso que se muestra sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si acepta la instalación de versiones sucesivas e incrementales de la aplicación, si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de una manera sencilla, sin instalar versiones sucesivas. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

   Se inicia el Asistente para crear tarea de reparación de vulnerabilidades e instalación de actualizaciones. Avance a través del Asistente utilizando el botón **Siguiente**.

5. En la página del Asistente **Selección de una opción de reinicio del sistema operativo**, seleccione la acción a realizar cuando el sistema operativo en los dispositivos cliente deba reiniciarse después de la operación:

   - **No reiniciar el dispositivo**

     Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

   - **Reiniciar el dispositivo**

     Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

   - **Solicitar al usuario una acción**

     En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

     Esta opción está seleccionada de forma predeterminada.

     - **Repetir solicitud cada (min)**

       Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

       Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

       Si esta opción está desactivada, la solicitud se muestra solo una vez.

     - **Reiniciar después de (min)**

Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- Forzar el cierre de las aplicaciones en sesiones bloqueadas

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

6. En la página **Configurar programación de tareas** del Asistente, puede crear una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

   - Inicio programado:

     Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

     - Cada N horas

       La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

       De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

     - Cada N días

       La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

       De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

     - Cada N semanas

       La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

       De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

     - Cada N minutos

La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para la protección del perímetro
- Antivirus para sistemas de correo

De forma predeterminada, están seleccionados todos los tipos de aplicación.

Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- **Usar un retraso aleatorio automático para el inicio de las tareas**

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

7. En la página del Asistente **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).

8. En la página **Finalizar la creación de tareas** del Asistente haga clic en el botón **Finalizar** para cerrar el Asistente.

   Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

Una vez que finaliza el Asistente, aparece **Instalar actualizaciones requeridas y reparar vulnerabilidades**, en la carpeta **Tareas**.

Puede activar la instalación automática de componentes del sistema (requisitos previos) antes de la instalación de una actualización en Instalar actualizaciones necesarias y corregir las propiedades de la tarea de vulnerabilidades. Cuando esta opción se activa, todos los componentes requeridos del sistema se instalan antes de la actualización. Una lista de los componentes requeridos se puede encontrar en las propiedades de la actualización.

En las propiedades de Instalar actualizaciones requeridas y reparar la tarea de vulnerabilidades, puede permitir la instalación de actualizaciones que actualizan la aplicación a una nueva versión.

Si la configuración de la tarea proporciona reglas para la instalación de actualizaciones de terceros, el Servidor de administración descargará todas las actualizaciones relevantes desde los sitios web de sus proveedores. Las actualizaciones se guardan en el repositorio del Servidor de administración y se las distribuye e instala en los dispositivos donde sean aplicables.

Si la configuración de la tarea proporciona reglas para la instalación de actualizaciones de Microsoft y el Servidor de administración actúa como servidor WSUS, el Servidor de administración descargará todas las actualizaciones correspondientes al repositorio y luego las distribuirá a los dispositivos administrados. Si la red no usa ningún servidor WSUS, cada dispositivo cliente descargará por su cuenta las actualizaciones de Microsoft desde servidores externos.

Para instalar una actualización determinada y similares:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.

2. En el espacio de trabajo, seleccione la actualización que desea instalar.

3. Haga clic en el botón **Ejecutar Asistente de instalación de actualización**.

   Se inicia el Asistente de instalación de actualizaciones.

Las funciones del Asistente de instalación de actualizaciones solo están disponibles bajo la licencia de Administración de vulnerabilidades y parches.

Avance a través del Asistente utilizando el botón **Siguiente**.

4. En la página **Buscar tareas de instalación de actualizaciones existentes**, especifique la siguiente configuración:

   - **Buscar tareas que instalen esta actualización**

     Si esta opción está activada, el Asistente de instalación de actualizaciones busca las tareas existentes que instalan la actualización seleccionada.

     Si esta opción está desactivada o si la búsqueda no recupera tareas aplicables, el Asistente para la instalación de actualizaciones le solicitará que cree una regla o una tarea para instalar la actualización.

     Esta opción está activada de forma predeterminada.

   - **Aprobar instalación de actualización**

     La actualización seleccionada será aprobada para su instalación. Active esta opción si algunas reglas aplicadas de instalación de actualizaciones solo permiten la instalación de actualizaciones aprobadas.

     Esta opción está desactivada de forma predeterminada.

5. Si elige buscar tareas de instalación de actualización existentes y si la búsqueda recupera algunas tareas, puede ver las propiedades de estas tareas o iniciarlas de forma manual. No se requieren más acciones.

   De lo contrario, haga clic en el botón **Nueva tarea de actualización**.

6. Seleccione el tipo de regla de instalación que se añadirá a la nueva tarea y luego haga clic en el botón **Finalizar**.

7. Haga su elección en el aviso que se muestra sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si acepta la instalación de versiones sucesivas e incrementales de la aplicación, si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de una manera sencilla, sin instalar versiones sucesivas. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

   Se inicia el Asistente para crear tarea de reparación de vulnerabilidades e instalación de actualizaciones. Avance a través del Asistente utilizando el botón **Siguiente**.

8. En la página del Asistente **Selección de una opción de reinicio del sistema operativo**, seleccione la acción a realizar cuando el sistema operativo en los dispositivos cliente deba reiniciarse después de la operación:

   - **No reiniciar el dispositivo**

     Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

   - **Reiniciar el dispositivo**

     Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

  En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

    Si esta opción está desactivada, la solicitud se muestra solo una vez.

  - **Reiniciar después de (min)**

    Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

    Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

9. En la página del Asistente **Seleccionar a qué dispositivos se asignará la tarea**, seleccione una de las siguientes opciones:

   - **Seleccionar dispositivos de red detectados por el Servidor de administración**

     La tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración así como dispositivos no asignados.

     Por ejemplo, es posible que desee usar esta opción en una tarea de instalación del Agente de red en dispositivos no asignados.

   - **Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista**

Puede especificar nombres NetBIOS, nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.

Es posible que desee utilizar esta opción para ejecutar una tarea para una subred específica. Por ejemplo, es posible que desee instalar una aplicación determinada en dispositivos de contadores o analizar dispositivos en una subred que probablemente esté infectada.

- Asignar tarea a una selección de dispositivos

  La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

- Asignar tarea a un grupo de administración

  La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para dispositivos incluidos en un grupo de administración específico.

10. En la página **Configurar programación de tareas** del Asistente, puede crear una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

    - Inicio programado:

      Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

      - Cada N horas

        La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

        De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

      - Cada N días

        La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

        De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

      - Cada N semanas

        La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

        De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente** (seleccionado de manera predeterminada)

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para la protección del perímetro
- Antivirus para sistemas de correo

De forma predeterminada, están seleccionados todos los tipos de aplicación.

Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

11. En la página del Asistente **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).

12. En la página **Finalizar la creación de tareas** del Asistente haga clic en el botón **Finalizar** para cerrar el Asistente.

    Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

Cuando el Asistente finaliza, la tarea **Instalar actualizaciones necesarias y corregir vulnerabilidades** se crea y se muestra en la carpeta **Tareas**.

Además de la configuración que especifique durante la creación de la tarea, puede cambiar otras propiedades de una tarea creada.

La actualización a una nueva versión de la aplicación puede provocar el mal funcionamiento de las aplicaciones dependientes en los dispositivos.

Instalar una actualización añadiendo una regla a una tarea de instalación existente

Para instalar una actualización añadiendo una regla a una tarea de instalación existente:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.

2. En el espacio de trabajo, seleccione la actualización que desea instalar.

3. Haga clic en el botón **Ejecutar Asistente de instalación de actualización**.

   Se inicia el Asistente de instalación de actualizaciones.

   Las funciones del Asistente de instalación de actualizaciones solo están disponibles bajo la licencia de Administración de vulnerabilidades y parches.

   Avance a través del Asistente utilizando el botón **Siguiente**.

4. En la página **Buscar tareas de instalación de actualizaciones existentes**, especifique la siguiente configuración:

   - Buscar tareas que instalen esta actualización

Si esta opción está activada, el Asistente de instalación de actualizaciones busca las tareas existentes que instalan la actualización seleccionada.

Si esta opción está desactivada o si la búsqueda no recupera tareas aplicables, el Asistente para la instalación de actualizaciones le solicitará que cree una regla o una tarea para instalar la actualización.

Esta opción está activada de forma predeterminada.

- **Aprobar instalación de actualización**

  La actualización seleccionada será aprobada para su instalación. Active esta opción si algunas reglas aplicadas de instalación de actualizaciones solo permiten la instalación de actualizaciones aprobadas.

  Esta opción está desactivada de forma predeterminada.

5. Si elige buscar tareas de instalación de actualización existentes y si la búsqueda recupera algunas tareas, puede ver las propiedades de estas tareas o iniciarlas de forma manual. No se requieren más acciones.

   De lo contrario, haga clic en el botón **Agregar una regla de instalación de actualizaciones**.

6. Seleccione la tarea a la que desea añadir una regla y luego haga clic en el botón **Agregar regla**.

   Además, puede ver las propiedades de las tareas existentes, iniciarlas de forma manual o crear una nueva tarea.

7. Seleccione el tipo de regla que se añadirá a la tarea seleccionada y luego haga clic en el botón **Finalizar**.

8. Haga su elección en el aviso que se muestra sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si acepta la instalación de versiones sucesivas e incrementales de la aplicación, si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de una manera sencilla, sin instalar versiones sucesivas. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

Se agrega una nueva regla para instalar la actualización a la tarea **Instalar actualizaciones necesarias y corregir vulnerabilidades**.

Configurando una instalación de prueba de actualizaciones

Siga estos pasos para configurar una instalación de prueba de las actualizaciones:

1. En el árbol de consola, seleccione la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades** de la carpeta **Dispositivos administrados**, en la ficha **Tareas**.

2. En el menú contextual de la tarea, seleccione **Propiedades**.

   Se abre la ventana de propiedades de la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.

3. En la ventana de propiedades de la tarea, en la sección **Instalación de prueba**, seleccione una de las opciones disponibles para la instalación de prueba:

   - **No analizar**. Seleccione esta opción si no desea realizar una instalación de prueba de las actualizaciones.

   - **Ejecute el análisis en dispositivos seleccionados**. Seleccione esta opción si desea probar la instalación de actualizaciones en determinados dispositivos. Haga clic en el botón **Agregar** y seleccione los dispositivos en los que desea realizar una instalación de prueba de las actualizaciones.

- **Ejecutar el análisis en dispositivos del grupo especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en un grupo de dispositivos. En el campo **Especificar un grupo de prueba**, especifique un grupo de dispositivos en los que desee realizar una instalación de prueba.

- **Ejecutar el análisis en el porcentaje de dispositivos especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en parte de los dispositivos. En el campo **Porcentaje de dispositivos de prueba del total de dispositivos de destino**, especifique el porcentaje de equipos en el que desea realizar una instalación de prueba de las actualizaciones.

4. Al seleccionar cualquier opción, excepto **No analizar**, en el campo **Cantidad de tiempo para decidir si se desea continuar con la instalación, en horas**, especifique el número de horas que deben transcurrir desde la instalación de prueba de actualizaciones hasta el inicio de la instalación de las actualizaciones en todos los dispositivos.

Configuración de actualizaciones de Windows en una directiva del Agente de red

Para configurar las actualizaciones de Windows en una directiva del Agente de red:

1. En el árbol de consola, seleccione **Dispositivos administrados**.

2. En el espacio de trabajo, seleccione la ficha **Directivas**.

3. Seleccione una directiva del Agente de red.

4. En el menú contextual de la directiva, seleccione **Propiedades**.

   Se abrirá la ventana de propiedades para la directiva del Agente de red.

5. En el panel **Secciones**, seleccione **Vulnerabilidades y actualizaciones de software**.

6. Seleccione la opción **Utilizar el Servidor de administración como servidor WSUS** para descargar las actualizaciones de Windows en el Servidor de administración y, a continuación, distribuirlas a los dispositivos cliente mediante Agente de red.

   Si esta opción no está seleccionada, las actualizaciones de Windows no se descargan al Servidor de administración. En este caso, los dispositivos cliente reciben actualizaciones de Windows directamente desde los servidores de Microsoft.

7. Seleccione el conjunto de actualizaciones que los usuarios pueden instalar de forma manual en sus dispositivos mediante Windows Update.

   > En los dispositivos que ejecutan Windows 10, si Windows Update ya encontró actualizaciones para el dispositivo, la nueva opción que seleccione en **Permitir a los usuarios administrar la instalación de las actualizaciones de Windows Update** se aplicará solo después de que se hayan instalado las actualizaciones encontradas.

   Seleccione un elemento en la lista desplegable:

   - Permitir que los usuarios instalen todas las actualizaciones de Windows Update aplicables

Los usuarios pueden instalar todas las actualizaciones de Microsoft Windows Update que sean aplicables a sus dispositivos.

Seleccione esta opción si no desea interferir en la instalación de actualizaciones.

Cuando el usuario instala actualizaciones de Microsoft Windows Update manualmente, las actualizaciones pueden descargarse de los servidores de Microsoft en lugar de hacerlo desde el Servidor de administración. Esto es posible si el Servidor de administración aún no ha descargado estas actualizaciones. La descarga de actualizaciones de los servidores de Microsoft genera un tráfico adicional.

- **Permitir que los usuarios instalen solo actualizaciones aprobadas de Windows Update**

  Los usuarios pueden instalar todas las actualizaciones de Microsoft Windows Update que sean aplicables a sus dispositivos y que sean aprobadas por usted.

  Por ejemplo, es posible que desee verificar primero la instalación de actualizaciones en un entorno de prueba y asegurarse de que no interfieran con el funcionamiento de los dispositivos y solo entonces permitir la instalación de estas actualizaciones aprobadas en los dispositivos cliente.

  Cuando el usuario instala actualizaciones de Microsoft Windows Update manualmente, las actualizaciones pueden descargarse de los servidores de Microsoft en lugar de hacerlo desde el Servidor de administración. Esto es posible si el Servidor de administración aún no ha descargado estas actualizaciones. La descarga de actualizaciones de los servidores de Microsoft genera un tráfico adicional.

- **No permitir que los usuarios instalen actualizaciones de Windows Update**

  Los usuarios no pueden instalar actualizaciones de Microsoft Windows Update en sus dispositivos de manera manual. Todas las actualizaciones aplicables se instalan según lo configurado por usted.

  Seleccione esta opción si desea administrar la instalación de actualizaciones de forma centralizada.

  Por ejemplo, es posible que desee optimizar el programa de actualización para que la red no se sobrecargue. Puede programar actualizaciones fuera de horario, para que no interfieran con la productividad del usuario.

8. Seleccione el modo de búsqueda de Windows Update:

- **Activo**

  Si se selecciona esta opción, el Servidor de administración, secundado por el Agente de red, iniciará una solicitud de un agente de Windows Update en el dispositivo cliente al origen de actualizaciones: Servidores de Windows Update o WSUS. A continuación, el Agente de red transmite la información que recibe del Agente de Windows Update al Servidor de administración.

  La opción solo se activa si se selecciona la opción **Conectar al servidor de actualizaciones para actualizar los datos** de la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

  Esta opción está seleccionada de forma predeterminada.

- **Pasivo**

Si se selecciona esta opción, el Agente de red transmite periódicamente al Servidor de administración información sobre las actualizaciones recuperadas en la última sincronización del Agente de Windows Update con el origen de actualizaciones. Si no se realiza ninguna sincronización del Agente de Windows Update con un origen de actualizaciones, la información sobre actualizaciones del Servidor de administración se volverá anticuada.

Seleccione esta opción si desea obtener actualizaciones de la memoria caché del origen de actualizaciones.

- **Desactivado**

  Si selecciona esta opción, el Servidor de administración no solicita información alguna acerca de las actualizaciones.

  Seleccione esta opción si, por ejemplo, desea probar primero las actualizaciones en su dispositivo local.

9. Seleccione la opción **Analizar los archivos ejecutables para buscar vulnerabilidades al iniciarlos** si desea analizar los archivos ejecutables en busca de vulnerabilidades mientras se ejecutan.
10. Asegúrese de que la edición de todos los ajustes que haya cambiado esté bloqueada. De lo contrario, los cambios no se aplican.
11. Haga clic en **Aplicar**.

Arreglar vulnerabilidades de software de terceros

Esta sección describe las características de Kaspersky Security Center que se relacionan con la reparación de vulnerabilidades en el software instalado en dispositivos administrados.

Escenario: búsqueda y reparación de vulnerabilidades de software de terceros

Esta sección proporciona un escenario para encontrar y corregir vulnerabilidades en los dispositivos administrados que ejecutan Windows. Puede encontrar y corregir vulnerabilidades de software en el sistema operativo y en el software de terceros, incluido el software de Microsoft.

Requisitos previos

- Kaspersky Security Center se ha implementado en su organización.
- Hay dispositivos administrados que ejecutan Windows en su organización.
- Se requiere conexión a Internet para que el Servidor de administración realice las siguientes tareas:
  - Para hacer una lista de reparaciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente la lista.
  - Para reparar vulnerabilidades en software de terceros que no sea el software de Microsoft.

Etapas

Encontrar y corregir vulnerabilidades de software transcurre en etapas:

1. **Análisis en busca de vulnerabilidades en el software instalado en los dispositivos administrados**

   Para buscar vulnerabilidades en el software instalado en los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el Asistente, hágalo ahora o cree la tarea manualmente.

   Instrucciones:

   - Consola de administración: Análisis de aplicaciones para buscar vulnerabilidades, Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center 14 Web Console: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Análisis de la lista de vulnerabilidades de software detectadas**

   Vea la lista de **Vulnerabilidades de software** y decida qué vulnerabilidades se repararán. Para ver información detallada sobre cada vulnerabilidad, haga clic en el nombre de la vulnerabilidad en la lista. Para cada vulnerabilidad de la lista, también puede ver las estadísticas sobre la vulnerabilidad en los dispositivos administrados.

   Instrucciones:

   - Consola de administración: visualización de vulnerabilidades de software de información, visualización de estadísticas de vulnerabilidades en dispositivos administrados
   - Kaspersky Security Center 14 Web Console: Consultar información sobre vulnerabilidades de software, Visualización de estadísticas de vulnerabilidades en dispositivos administrados

3. **Configuración de reparación de vulnerabilidades**

   Cuando se detectan las vulnerabilidades de software, puede corregirlas en los dispositivos administrados mediante la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*.

   La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para actualizar y corregir vulnerabilidades en software de terceros, incluido el software de Microsoft, instalado en los dispositivos administrados. Esta tarea le permite instalar múltiples actualizaciones y corregir múltiples vulnerabilidades de acuerdo con ciertas reglas. Tenga en cuenta que esta tarea se puede crear únicamente si tiene la licencia para la función Administración de vulnerabilidades y parches. Para corregir vulnerabilidades de software, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* utiliza actualizaciones de software recomendadas.

   La tarea *Reparar vulnerabilidades* no requiere la opción de licencia para la función Administración de vulnerabilidades y parches. Para utilizar esta tarea, debe especificar manualmente las correcciones del usuario para las vulnerabilidades en el software de terceros que figuran en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza correcciones recomendadas para el software de Microsoft y correcciones de usuario para software de terceros.

   Puede iniciar el Asistente de reparación de vulnerabilidades que crea una de estas tareas automáticamente, o puede crear una de estas de forma manual.

   Instrucciones:

   - Consola de administración: selección de soluciones de usuario para vulnerabilidades en software de terceros, reparación de vulnerabilidades en aplicaciones

- Kaspersky Security Center 14 Web Console: selección de soluciones de usuario para vulnerabilidades en el software de terceros, reparación de vulnerabilidades en software de terceros, creación de la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

4. **Programar las tareas**

   Para asegurarse de que la lista de vulnerabilidades esté siempre actualizada, programe la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para ejecutarla automáticamente de vez en cuando. La frecuencia media recomendada es de una vez a la semana.

   Si ha creado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* puede programarla para que se ejecute con la misma frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* o con menos frecuencia. Al programar la tarea *Reparar vulnerabilidades*, tenga en cuenta que debe seleccionar soluciones para el software de Microsoft o especificar soluciones de usuario para el software de terceros cada vez antes de comenzar la tarea.

   Cuando programe las tareas, asegúrese de que una tarea para solucionar una vulnerabilidad comience después de que se complete la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

5. **Ignorar las vulnerabilidades de software (opcional)**

   Si lo desea, puede ignorar vulnerabilidades de software que reparar en todos los dispositivos administrados o solo en determinados dispositivos administrados.

   Instrucciones:

   - Consola de administración: ignorar las vulnerabilidades de software
   - Kaspersky Security Center 14 Web Console: Ignorar las vulnerabilidades de software

6. **Ejecución de una tarea de reparación de la vulnerabilidad**

   Inicie las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Reparar vulnerabilidad*. Cuando complete la tarea, asegúrese de que tenga el estado *Completado correctamente* en la lista de tareas.

7. **Crear un informe de los resultados de la reparación de vulnerabilidades de software (opcional)**

   Para ver estadísticas detalladas sobre la reparación de vulnerabilidades, genere el Informe de vulnerabilidades. El informe muestra detalles acerca de vulnerabilidades de software que no se corrigen. De esta manera, puede aprender cómo buscar y corregir vulnerabilidades de software de terceros, incluido el software de Microsoft, en su organización.

   Instrucciones:

   - Consola de administración: Creación y visualización de un informe
   - Kaspersky Security Center 14 Web Console: Generación y visualización de un informe

8. **Comprobar la configuración de la búsqueda y reparar vulnerabilidades en software de terceros**

   Asegúrese de haber hecho lo siguiente:

   - Obtenido y revisado la lista de vulnerabilidades de software detectadas en los dispositivos administrados
   - Ignorado las vulnerabilidades de software si así lo deseaba
   - Configurado la tarea para reparar vulnerabilidades
   - Programado las tareas de encontrar y reparar vulnerabilidades de software para que comiencen secuencialmente
   - Comprobado que se haya ejecutado la tarea para reparar vulnerabilidades de software

Resultados

Si ha creado y configurado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades se reparan automáticamente en los dispositivos administrados. Cuando se ejecuta la tarea, esta compara la lista de actualizaciones de software disponibles con las reglas especificadas en la configuración de la tarea. Todas las actualizaciones de software que cumplan con los criterios especificados en las reglas se descargarán en el repositorio del Servidor de administración y se instalarán para reparar las vulnerabilidades de software.

Si ha creado la tarea *Reparar vulnerabilidades*, solo se corrigen las vulnerabilidades de software de Microsoft.

Acerca de encontrar y corregir vulnerabilidades de software

Kaspersky Security Center detecta y corrige vulnerabilidades de software en dispositivos administrados que ejecutan los sistemas operativos de las familias Microsoft Windows. Se detectan vulnerabilidades en el sistema operativo y en el software de terceros, incluido el software de Microsoft.

Encontrar vulnerabilidades de software

Para encontrar vulnerabilidades de software, Kaspersky Security Center utiliza características de la base de datos de vulnerabilidades conocidas. Esta base de datos es creada por especialistas de Kaspersky. Contiene información sobre vulnerabilidades, como descripción de vulnerabilidades, fecha de detección de vulnerabilidades, nivel de gravedad de vulnerabilidades. Puede consultar los detalles de las vulnerabilidades de software en el sitio web de Kaspersky.

Kaspersky Security Center utiliza la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para buscar vulnerabilidades de software.

Corregir vulnerabilidades de software

Para corregir vulnerabilidades de software, Kaspersky Security Center utiliza actualizaciones de software emitidas por los proveedores de software. Los metadatos de las actualizaciones de software se descargan en el repositorio del Servidor de administración después de que se ejecuten las siguientes tareas:

- *Descargar actualizaciones en el repositorio del Servidor de administración*. Esta tarea tiene como objetivo la descarga de metadatos de actualizaciones para software de Kaspersky y de terceros. Esta tarea se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Puede crear la tarea Descargar actualizaciones en el repositorio del Servidor de administración manualmente.

- *Realizar la sincronización de Windows Update*. Esta tarea tiene como objetivo la descarga de metadatos de actualizaciones para software de Microsoft.

Las actualizaciones de software para corregir vulnerabilidades se pueden representar como paquetes de distribución completos o parches. Las actualizaciones de software que corrigen vulnerabilidades de software se denominan *correcciones*. Las *soluciones recomendadas* son aquellas que los especialistas de Kaspersky recomiendan para la instalación. Las *correcciones de usuario* son aquellas que se especifican manualmente para la instalación por parte de los usuarios. Para instalar un arreglo de usuario, debe crear un paquete de instalación que contenga este arreglo.

Si tiene la licencia de Kaspersky Security Center con la función Administración de vulnerabilidades y parches para corregir las vulnerabilidades de software, puede usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Esta tarea corrige automáticamente múltiples vulnerabilidades instalando las correcciones recomendadas. Para esta tarea, puede configurar manualmente ciertas reglas para corregir múltiples vulnerabilidades.

Si no tiene la licencia de Kaspersky Security Center con la función Administración de vulnerabilidades y parches para corregir las vulnerabilidades de software, puede usar la tarea *Reparar vulnerabilidades*. Mediante esta tarea, puede corregir vulnerabilidades instalando correcciones recomendadas para el software de Microsoft y correcciones de usuario para otro software de terceros.

Por razones de seguridad, las tecnologías de Kaspersky analizan automáticamente en busca de malware cualquier actualización de software de terceros que instale mediante la función Administración de vulnerabilidades y parches. Estas tecnologías se utilizan para la verificación automática de archivos e incluyen análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno aislado y aprendizaje automático.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Además, los expertos de Kaspersky no buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en dichas actualizaciones, ni realizan otros tipos de análisis de las actualizaciones distintos a los especificados en el párrafo anterior.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Para reparar algunas vulnerabilidades de software, debe aceptar el Contrato de licencia de usuario final (EULA) para instalar el software si se solicita la aceptación del EULA. Si rechaza el EULA, la vulnerabilidad de software no se repara.

Consultar información sobre vulnerabilidades de software

Para ver una lista de las vulnerabilidades detectadas en dispositivos cliente,

En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Vulnerabilidades de software**.

La página muestra una lista de vulnerabilidades en las aplicaciones detectadas en dispositivos administrados.

Siga estos pasos para obtener información acerca de una vulnerabilidad seleccionada:

Seleccione **Propiedades** en el menú contextual de la vulnerabilidad.

Se abre la ventana de la vulnerabilidad y muestra la siguiente información:

- Aplicación en la que se ha detectado la vulnerabilidad.
- Lista de los dispositivos en los cuales se detectó la vulnerabilidad.
- Información acerca de si se ha reparado la vulnerabilidad.

Realice lo siguiente para consultar el informe acerca de todas las vulnerabilidades detectadas:

En la carpeta **Vulnerabilidades de software**, haga clic en el enlace **Ver informe de vulnerabilidades**.

Se generará un informe de vulnerabilidades de las aplicaciones instaladas en los dispositivos. Puede ver este informe en el nodo con el nombre del Servidor de administración correspondiente, mediante la apertura de la ficha **Informes**.

Visualización de estadísticas de vulnerabilidades en dispositivos administrados

Puede ver estadísticas para cada vulnerabilidad de software en dispositivos administrados. Las estadísticas se representan como un diagrama. El diagrama muestra la cantidad de dispositivos con los siguientes estados:

- *Ignorado en: <número de dispositivos>*. El estado se asigna si, en las propiedades de vulnerabilidad, ha configurado manualmente la opción para ignorar la vulnerabilidad.
- *Reparado en: <número de dispositivos>*. El estado se asigna si la tarea para reparar la vulnerabilidad se ha completado correctamente.
- *Arreglo programado en:<número de dispositivos>*. El estado se asigna si ha creado la tarea para corregir la vulnerabilidad pero la tarea aún no se ha realizado.
- *Parche aplicado en:* <número de dispositivos>. El estado se asigna si ha seleccionado manualmente una actualización de software para corregir la vulnerabilidad pero este software actualizado no ha solucionado la vulnerabilidad.

Arreglo requerido en:<número de dispositivos>. El estado se asigna si la vulnerabilidad se reparó solo en la parte de los dispositivos administrados y se requiere que se repare en la parte restante de los dispositivos administrados.

Para ver las estadísticas de una vulnerabilidad en dispositivos administrados:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Vulnerabilidades de software**.

   La página muestra una lista de vulnerabilidades en las aplicaciones detectadas en dispositivos administrados.

2. Seleccione una vulnerabilidad para la que desee ver las estadísticas.

   En el bloque para trabajar con un objeto seleccionado, se muestra un diagrama de los estados de vulnerabilidad. Al hacer clic en un estado, se abre una lista de dispositivos en los que la vulnerabilidad tiene el estado seleccionado.

Análisis de aplicaciones para buscar vulnerabilidades

Si ha configurado la aplicación con el Asistente de inicio rápido, la tarea de análisis de vulnerabilidades se crea automáticamente. Puede ver la tarea en la carpeta **Dispositivos administrados**, en la ficha **Tareas**.

Para crear una tarea de análisis de vulnerabilidades en aplicaciones instaladas en dispositivos cliente:

1. En el árbol de la consola, seleccione **Avanzado** → **Administración de aplicaciones** y luego seleccione la subcarpeta **Vulnerabilidades de software**.

2. En el espacio de trabajo, seleccione **Acciones adicionales** → **Configurar el análisis de vulnerabilidades**.

   Si ya existe una tarea para el análisis de vulnerabilidades, se muestra la ficha **Tareas** de la carpeta **Dispositivos administrados**, con la tarea existente seleccionada. De lo contrario, se inicia el Asistente para la creación de tareas de búsqueda de vulnerabilidades y actualizaciones necesarias. Avance a través del Asistente utilizando el botón **Siguiente**.

3. En la ventana **Seleccionar el tipo de tarea**, seleccione **Buscar vulnerabilidades y actualizaciones necesarias**.

4. En la página del Asistente **Configuración**, especifique la configuración de la tarea de la siguiente manera:

   - **Buscar vulnerabilidades y actualizaciones en la lista de Microsoft**

     Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

     Por ejemplo, es posible que desee desactivar esta opción si tiene diferentes tareas con diferentes configuraciones para las actualizaciones de Microsoft y las actualizaciones de aplicaciones de terceros.

     Esta opción está activada de forma predeterminada.

     - **Conectar al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update en un dispositivo administrado se conecta al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como origen de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center (consulte la configuración de la directiva del Agente de red)
- Windows Server con Servicio de Windows Server Update (WSUS) de Microsoft desplegado en la red de su organización
- Servidores de actualización de Microsoft

Si se activa esta opción, el Agente de Windows Update en un dispositivo administrado se conecta al origen de actualizaciones de Microsoft para actualizar la información sobre las actualizaciones aplicables de Microsoft Windows.

Si se desactiva esta opción, el Agente de Windows Update en un dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que se recibió desde el origen de actualizaciones de Microsoft anteriormente y que se almacena en el caché del dispositivo.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Es posible que quiera desactivar esta opción si establece una conexión periódica a este origen de actualizaciones en otra tarea o en las propiedades de la directiva del Agente de red, en la sección **Vulnerabilidades y actualizaciones de software**. Si no desea desactivar esta opción, para reducir la sobrecarga del servidor, puede configurar la programación de tareas para aleatorizar el retraso del inicio de la tarea en 360 minutos.

Esta opción está activada de forma predeterminada.

La combinación de las siguientes opciones de la configuración de la directiva del Agente de red define el modo de obtener actualizaciones:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada y se selecciona la opción **Activo** en el grupo de configuración **Modo de búsqueda de Windows Update**.
- El Agente de Windows Update en un dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que se recibió del origen de actualizaciones de Microsoft anteriormente y que se almacena en el caché del dispositivo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada y se selecciona la opción **Pasivo** en el grupo de configuración **Modo de búsqueda de Windows Update** o si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está desactivada y se selecciona la opción **Activo** en el grupo de configuración **Modo de búsqueda de Windows Update**.
- Independientemente del estado de la opción **Conectar al servidor de actualizaciones para actualizar los datos** (activado o desactivado), si la opción **Desactivado**, se selecciona en el grupo de configuración **Modo de búsqueda de Windows Update**, Kaspersky Security Center no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones de terceros en la lista de Kaspersky

Si esta opción está activada, Kaspersky Security Center busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especificar rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky gestiona la lista completa de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Por ejemplo, es posible que desee desactivar esta opción si tiene diferentes tareas con diferentes configuraciones para las actualizaciones de Microsoft Windows y las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- Especificar rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos

  Las carpetas en las que Kaspersky Security Center busca aplicaciones de terceros que requieren reparación de la vulnerabilidad e instalaciones de actualizaciones. Puede usar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- Activar diagnóstico avanzado

  Si esta función está habilitada, el Agente de red escribe los seguimientos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los seguimientos se escriben en dos archivos a su vez; el tamaño total de ambos archivos se determina por el valor **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando ambos archivos están llenos, el Agente de red comienza a escribirles de nuevo. Los archivos con seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se escriben rastros adicionales.

  Al crear una tarea, no tiene que habilitar los diagnósticos avanzados. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está desactivada de forma predeterminada.

- Tamaño máximo, en MB, de los archivos de diagnóstico avanzado

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky le pidan que cambie el valor predeterminado cuando la información de los archivos de diagnóstico avanzado que les envía no es suficiente para solucionar el problema.

5. En la página **Configurar programación de tareas** del Asistente, puede crear una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

- Inicio programado:

  Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

- Cada N horas

La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

- **Cada N días**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

  De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

En los meses que faltan el día especificado, la tarea se ejecuta el último día.

De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Cuando se descargan nuevas actualizaciones en el repositorio**

  La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar este programa para la tarea de encontrar vulnerabilidades y actualizaciones necesarias.

- **Al detectar un foco de virus**

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

Esta opción está activada de forma predeterminada.

- Usar un retraso aleatorio automático para el inicio de las tareas

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

6. En la página del Asistente **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).

7. En la página **Finalizar la creación de tareas** del Asistente haga clic en el botón **Finalizar** para cerrar el Asistente.

   Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

Una vez que el Asistente completa su operación, la tarea Buscar vulnerabilidades y actualizaciones necesarias aparece en la lista de tareas en la carpeta **Dispositivos administrados**, en la ficha **Tareas**.

Además de la configuración que especifique durante la creación de la tarea, puede cambiar otras propiedades de una tarea creada.

Al completarse la tarea Buscar vulnerabilidades y actualizaciones requeridas, el Servidor de administración muestra una lista de las vulnerabilidades encontradas en las aplicaciones instaladas en el dispositivo. También muestra todas las actualizaciones de software requeridas para reparar las vulnerabilidades detectadas.

Si los resultados de la tarea contienen error el 0x80240033 "Error del Agente de Windows Update 80240033 ("No se pudieron descargar los términos de licencia")", puede resolver este problema a través del registro de Windows.

El Servidor de administración no muestra la lista de actualizaciones de software requeridas cuando ejecuta dos tareas secuencialmente: la tarea Sincronizar Windows Update con la opción **Descargar archivos de instalación rápida** desactivada y la tarea Buscar vulnerabilidades y actualizaciones requeridas. Para poder ver la lista de actualizaciones de software requeridas, debe volver a ejecutar la tarea Buscar vulnerabilidades y actualizaciones requeridas.

El Agente de red recibe la información sobre cualquier actualización de Windows disponible y otras actualizaciones de productos de Microsoft desde Windows Update o desde el Servidor de administración, si el Servidor de administración actúa como servidor WSUS. La información se transmite durante el inicio de las aplicaciones (si así lo dicta la directiva) y en cada inicio rutinario de la tarea Buscar vulnerabilidades y actualizaciones requeridas en los dispositivos cliente.

Puede encontrar los detalles del software de terceros que se puede actualizar a través de Kaspersky Security Center en el sitio web del Servicio de Soporte Técnico, ubicado en la sección **Administración del servidor** de la página de Kaspersky Security Center.

Reparación de vulnerabilidades en las aplicaciones

Si ha seleccionado **Buscar e instalar las actualizaciones requeridas** en la página **Configuración de la administración de actualizaciones** del Asistente de inicio rápido, se crea automáticamente la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**. La tarea aparece en la carpeta del espacio de trabajo **Dispositivos administrados**, en la ficha **Tareas**.

De otro modo, puede hacer lo siguiente:

- Crear una tarea para reparar vulnerabilidades instalando actualizaciones disponibles.
- Añadir una regla para reparar una vulnerabilidad a una tarea de reparación de vulnerabilidades existente.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Reparar vulnerabilidades creando una tarea de reparación de vulnerabilidades

Puede hacer lo siguiente:

- Crear una tarea para corregir múltiples vulnerabilidades que cumplan ciertas reglas.
- Seleccione una vulnerabilidad y cree una tarea para corregirla y corregir las vulnerabilidades similares.

Para corregir vulnerabilidades que cumplan ciertas reglas:

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo, seleccione la ficha **Tareas**.
3. Haga clic en el botón **Crear una tarea** para iniciar el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
4. En la página del Asistente **Seleccionar el tipo de tarea**, seleccione **Instalar actualizaciones requeridas y reparar vulnerabilidades**.
5. En la página del Asistente **Configuración**, especifique la configuración de la tarea de la siguiente manera:

- **Especificar reglas para instalar actualizaciones**

  Estas reglas se aplican a la instalación de actualizaciones en dispositivos cliente. Si no se especifican las reglas, la tarea no tiene nada que realizar. Para obtener información sobre las operaciones con reglas, consulte Reglas para la instalación de actualizaciones.

- **Iniciar la instalación al reiniciar o apagar el dispositivo**

  Si esta opción está activada, las actualizaciones se instalan cuando el dispositivo se reinicia o se apaga. De lo contrario, las actualizaciones se instalan de acuerdo con una programación.

  Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento del dispositivo.

  Esta opción está desactivada de forma predeterminada.

- **Instalar componentes generales del sistema requeridos**

  Si esta opción está activada, antes de instalar una actualización, la aplicación instala automáticamente todos los componentes generales del sistema (requisitos previos) que se requieren para instalar la actualización. Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo

  Si esta opción está desactivada, es posible que tenga que instalar los requisitos previos de manera manual.

  Esta opción está desactivada de forma predeterminada.

- **Autorizar la instalación de las nuevas versiones de la aplicación durante las actualizaciones**

  Si esta opción está activada, las actualizaciones se permiten cuando dan lugar a la instalación de una nueva versión de una aplicación de software.

  Si esta opción se desactiva, el software no se actualiza. A continuación, puede instalar nuevas versiones del software de manera manual o mediante otra tarea. Por ejemplo, puede usar esta opción si la infraestructura de su empresa no es compatible con una nueva versión del software o si desea verificar una actualización en una infraestructura de prueba.

  Esta opción está activada de forma predeterminada.

  La actualización de una aplicación puede causar un mal funcionamiento de las aplicaciones dependientes instaladas en los dispositivos cliente.

- **Descargar actualizaciones en el dispositivo sin instalarlas**

Si esta opción está activada, la aplicación descarga actualizaciones en el dispositivo pero no las instala automáticamente. A continuación, puede instalar las actualizaciones descargadas de manera manual.

Las actualizaciones de Microsoft se descargan al sistema de almacenamiento de Windows. Las actualizaciones de aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) se descargan en la carpeta especificada en el campo de **Carpeta para la descarga de actualizaciones**.

Si esta opción está desactivada, las actualizaciones se instalan en el dispositivo automáticamente.

Esta opción está desactivada de forma predeterminada.

- Carpeta para la descarga de actualizaciones

  Esta carpeta se utiliza para descargar actualizaciones de aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft).

- Activar diagnóstico avanzado

  Si esta función está habilitada, el Agente de red escribe los seguimientos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los seguimientos se escriben en dos archivos a su vez; el tamaño total de ambos archivos se determina por el valor **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando ambos archivos están llenos, el Agente de red comienza a escribirles de nuevo. Los archivos con seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se escriben rastros adicionales.

  Al crear una tarea, no tiene que habilitar los diagnósticos avanzados. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está desactivada de forma predeterminada.

- Tamaño máximo, en MB, de los archivos de diagnóstico avanzado

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky le pidan que cambie el valor predeterminado cuando la información de los archivos de diagnóstico avanzado que les envía no es suficiente para solucionar el problema.

6. En la página del Asistente **Selección de una opción de reinicio del sistema operativo**, seleccione la acción a realizar cuando el sistema operativo en los dispositivos cliente deba reiniciarse después de la operación:

- No reiniciar el dispositivo

  Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- Reiniciar el dispositivo

Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

  En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

    Si esta opción está desactivada, la solicitud se muestra solo una vez.

  - **Reiniciar después de (min)**

    Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

    Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

7. En la página **Configurar programación de tareas** del Asistente, puede crear una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

   - **Inicio programado:**

     Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

- **Cada N horas**

  La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

  De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

- **Cada N días**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

  De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

En los meses que faltan el día especificado, la tarea se ejecuta el último día.

De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

Esta opción está activada de forma predeterminada.

- Usar un retraso aleatorio automático para el inicio de las tareas

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

8. En la página del Asistente **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).

9. En la página **Finalizar la creación de tareas** del Asistente haga clic en el botón **Finalizar** para cerrar el Asistente.

   Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

Una vez que finaliza el Asistente, se crea la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**, y se la muestra en la carpeta **Tareas**.

Además de la configuración que especifique durante la creación de la tarea, puede cambiar otras propiedades de una tarea creada.

Si los resultados de la tarea contienen error el 0x80240033 "Error del Agente de Windows Update 80240033 ("No se pudieron descargar los términos de licencia")", puede resolver este problema a través del registro de Windows.

Para corregir una vulnerabilidad específica y similares:

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Vulnerabilidades de software**.
2. Seleccione la vulnerabilidad que desee reparar.
3. Haga clic en el botón **Ejecutar Asistente de reparación de vulnerabilidades**.

   Se inicia el Asistente de reparación de vulnerabilidades.

   Las funciones del Asistente de reparación de vulnerabilidades solo están disponibles bajo la licencia de Administración de vulnerabilidades y parches.

   Avance a través del Asistente utilizando el botón **Siguiente**.
4. En la ventana **Buscar tareas de reparación de vulnerabilidades existentes**, especifique los siguientes parámetros:

   - Mostrar solo las tareas que reparen esta vulnerabilidad

     Si esta opción está activada, el Asistente de reparación de vulnerabilidades busca las tareas existentes que reparan la vulnerabilidad seleccionada.

     Si esta opción está desactivada o si la búsqueda no recupera tareas, el Asistente de reparación de vulnerabilidades le solicita que cree una regla o tarea para reparar la vulnerabilidad.

     Esta opción está activada de forma predeterminada.

   - Aprobar actualizaciones que reparen esta vulnerabilidad

     Las actualizaciones que corrijan una vulnerabilidad serán aprobadas para su instalación. Activar esta opción si algunas reglas aplicadas de instalación de actualizaciones solo permiten la instalación de actualizaciones aprobadas.

     Esta opción está desactivada de forma predeterminada.
5. Si elige buscar tareas de reparación de vulnerabilidades existentes y si la búsqueda recupera algunas tareas, puede ver las propiedades de estas tareas o iniciarlas manualmente. No se requieren más acciones.

   De lo contrario, haga clic en el botón **Nueva tarea de reparación de vulnerabilidades**.
6. Seleccione el tipo de regla de reparación de vulnerabilidades que se añadirá a la nueva tarea y luego haga clic en el botón **Finalizar**.
7. Haga su elección en el aviso que se muestra sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si acepta la instalación de versiones sucesivas e incrementales de la aplicación, si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de una manera sencilla, sin instalar versiones sucesivas. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

Se inicia el Asistente para crear tarea de reparación de vulnerabilidades e instalación de actualizaciones. Avance a través del Asistente utilizando el botón **Siguiente**.

8. En la página del Asistente **Selección de una opción de reinicio del sistema operativo**, seleccione la acción a realizar cuando el sistema operativo en los dispositivos cliente deba reiniciarse después de la operación:

- **No reiniciar el dispositivo**

  Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- **Reiniciar el dispositivo**

  Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

  En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

    Si esta opción está desactivada, la solicitud se muestra solo una vez.

  - **Reiniciar después de (min)**

    Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

    Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

Esta opción está desactivada de forma predeterminada.

9. En la página del Asistente **Seleccionar a qué dispositivos se asignará la tarea**, seleccione una de las siguientes opciones:

- Seleccionar dispositivos de red detectados por el Servidor de administración

  La tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración así como dispositivos no asignados.

  Por ejemplo, es posible que desee usar esta opción en una tarea de instalación del Agente de red en dispositivos no asignados.

- Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista

  Puede especificar nombres NetBIOS, nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.

  Es posible que desee utilizar esta opción para ejecutar una tarea para una subred específica. Por ejemplo, es posible que desee instalar una aplicación determinada en dispositivos de contadores o analizar dispositivos en una subred que probablemente esté infectada.

- Asignar tarea a una selección de dispositivos

  La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

- Asignar tarea a un grupo de administración

  La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para dispositivos incluidos en un grupo de administración específico.

10. En la página **Configurar programación de tareas** del Asistente, puede crear una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

- Inicio programado:

  Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

- **Cada N horas**

  La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

  De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

- **Cada N días**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

  De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

En los meses que faltan el día especificado, la tarea se ejecuta el último día.

De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

Esta opción está activada de forma predeterminada.

- Usar un retraso aleatorio automático para el inicio de las tareas

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

11. En la página del Asistente **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).

12. En la página **Finalizar la creación de tareas** del Asistente haga clic en el botón **Finalizar** para cerrar el Asistente.

    Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

Cuando el Asistente se completa, la tarea **Instalar actualizaciones necesarias y corregir vulnerabilidades** se crea y se muestra en la carpeta **Tareas**.

Además de la configuración que especifique durante la creación de la tarea, puede cambiar otras propiedades de una tarea creada.

Reparación de una vulnerabilidad agregando una regla a una tarea de reparación de vulnerabilidades existente

Para reparar una vulnerabilidad añadiendo una regla a una tarea de reparación de vulnerabilidades existente:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Vulnerabilidades de software**.
2. Seleccione la vulnerabilidad que desee reparar.
3. Haga clic en el botón **Ejecutar Asistente de reparación de vulnerabilidades**.

   Se inicia el Asistente de reparación de vulnerabilidades.

   > Las funciones del Asistente de reparación de vulnerabilidades solo están disponibles bajo la licencia de Administración de vulnerabilidades y parches.

   Avance a través del Asistente utilizando el botón **Siguiente**.
4. En la ventana **Buscar tareas de reparación de vulnerabilidades existentes**, especifique los siguientes parámetros:

   - **Mostrar solo las tareas que reparen esta vulnerabilidad**

     Si esta opción está activada, el Asistente de reparación de vulnerabilidades busca las tareas existentes que reparan la vulnerabilidad seleccionada.

     Si esta opción está desactivada o si la búsqueda no recupera tareas, el Asistente de reparación de vulnerabilidades le solicita que cree una regla o tarea para reparar la vulnerabilidad.

     Esta opción está activada de forma predeterminada.

   - **Aprobar actualizaciones que reparen esta vulnerabilidad**

     Las actualizaciones que corrijan una vulnerabilidad serán aprobadas para su instalación. Activar esta opción si algunas reglas aplicadas de instalación de actualizaciones solo permiten la instalación de actualizaciones aprobadas.

     Esta opción está desactivada de forma predeterminada.
5. Si elige buscar tareas de reparación de vulnerabilidades existentes y si la búsqueda recupera algunas tareas, puede ver las propiedades de estas tareas o iniciarlas manualmente. No se requieren más acciones.

   De lo contrario, haga clic en el botón **Agregar regla de reparación de vulnerabilidades a tarea existente**.
6. Seleccione la tarea a la que desea añadir una regla y luego haga clic en el botón **Agregar regla**.

   Además, puede ver las propiedades de las tareas existentes, iniciarlas de forma manual o crear una nueva tarea.
7. Seleccione el tipo de regla que se añadirá a la tarea seleccionada y después haga clic en el botón **Finalizar**.
8. Haga su elección en el aviso que se muestra sobre la instalación de todas las actualizaciones de aplicaciones anteriores. Haga clic en **Sí** si acepta la instalación de versiones sucesivas e incrementales de la aplicación, si es necesario para instalar las actualizaciones seleccionadas. Haga clic en **No** si desea actualizar las aplicaciones de una manera sencilla, sin instalar versiones sucesivas. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

Se añade una nueva regla para reparar la vulnerabilidad a la tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades** existente.

Corrección de vulnerabilidades en una red aislada

Esta sección describe los pasos que puede seguir para arreglar las vulnerabilidades de software de terceros en dispositivos administrados conectados a Servidores de administración que no tienen acceso a Internet.

Escenario: corregir vulnerabilidades de software de terceros

Puede instalar actualizaciones y corregir vulnerabilidades del software de terceros instalado en dispositivos administrados en una red aislada. Dichas redes incluyen Servidores de administración y dispositivos administrados conectados a ellos que no tienen acceso a Internet. Para corregir vulnerabilidades en redes de este tipo, necesita un Servidor de administración conectado a Internet. Después, podrá descargar parches (actualizaciones necesarias) mediante el Servidor de administración con acceso a Internet y después transmitir los parches a Servidores de administración aislados.

Puede descargar las actualizaciones de software de terceros emitidas por los proveedores de software, pero no puede descargar actualizaciones para el software de Microsoft en Servidores de administración aislados mediante Kaspersky Security Center.

Para saber cómo funciona el proceso de corrección de vulnerabilidades en una red aislada, consulte la descripción y el esquema de este proceso.

Requisitos previos

Antes de comenzar, haga lo siguiente:

1. Asigne un dispositivo para conectarse a Internet y descargar parches. Este dispositivo se contará como el Servidor de administración con acceso a Internet.
2. Instale Kaspersky Security Center, no anterior a la versión 14, en los siguientes dispositivos:
   - Dispositivo asignado, que actuará como Servidor de administración con acceso a Internet
   - Dispositivos aislados, que actuarán como Servidores de administración aislados de Internet (en adelante, Servidores de administración aislados)
3. Asegúrese de que cada Servidor de administración tenga suficiente espacio en disco para descargar y almacenar actualizaciones y parches.

Etapas

La instalación de actualizaciones y la reparación de vulnerabilidades de software de terceros en los dispositivos administrados de Servidores de administración aislados tiene las siguientes etapas:

1. **Configuración del Servidor de administración con acceso a Internet**

Prepare su Servidor de administración con acceso a Internet para administrar las solicitudes de actualizaciones de software de terceros requeridas y para descargar parches.

2. **Configuración de Servidores de administración aislados**

   Prepare sus Servidores de administración aislados para que puedan formar listas de actualizaciones requeridas y administrar los parches descargados por el Servidor de administración con acceso a Internet. Una vez configuración, los Servidores de administración aislados ya no intentan descargar parches de Internet. En cambio, obtienen actualizaciones a través de parches.

3. **Transmisión de parches e instalación de actualizaciones en Servidores de administración aislados**

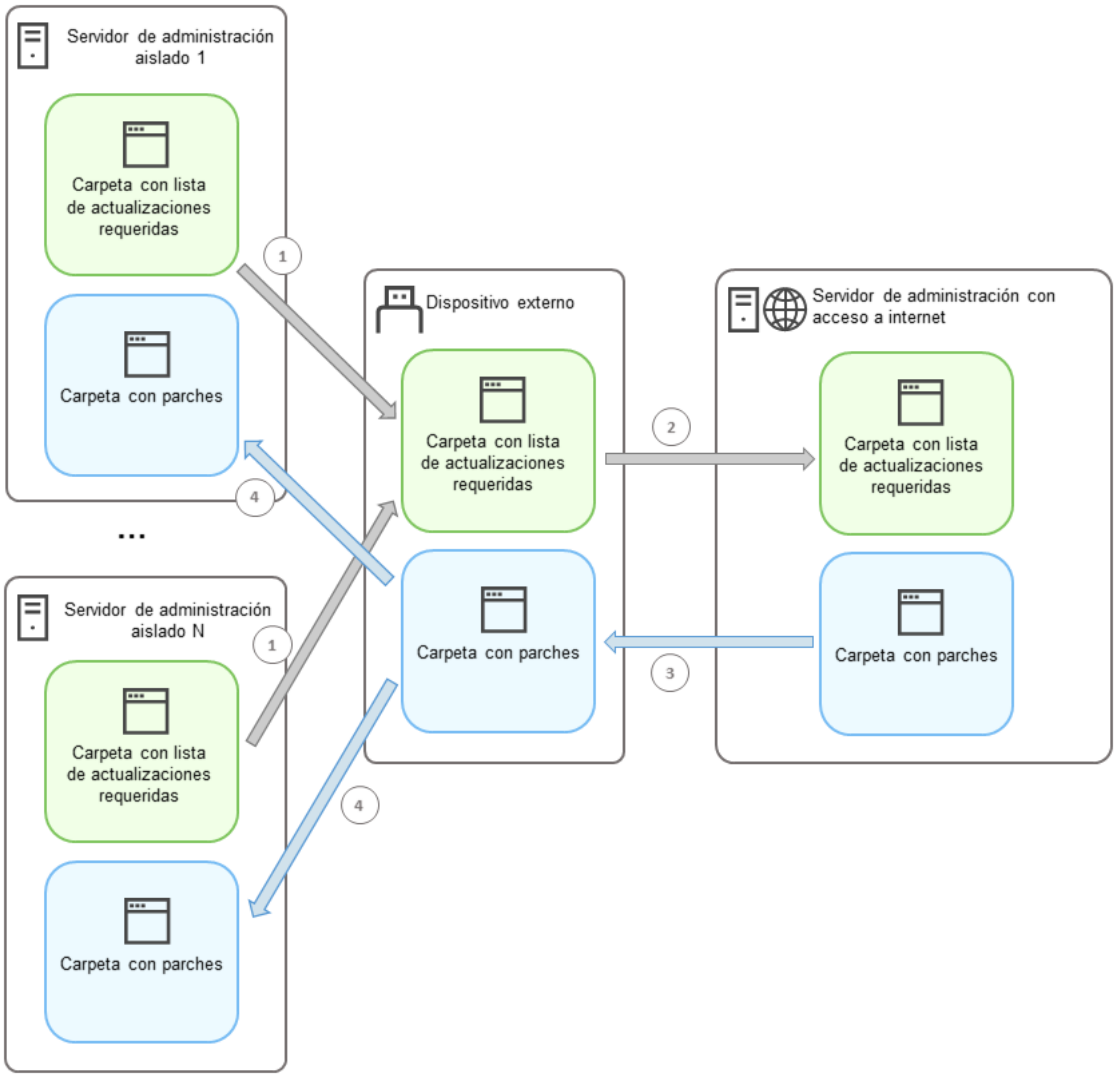
   Después de que haya terminado de configurar los Servidores de administración, puede transmitir las listas de actualizaciones y parches requeridos entre el Servidor de administración con acceso a Internet y los Servidores de administración aislados. A continuación, las actualizaciones de los parches se instalarán en los dispositivos administrados mediante la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

Resultados

Entonces, las actualizaciones de software de terceros se transmiten a Servidores de administración aislados y se instalan en dispositivos administrados conectados mediante Kaspersky Security Center. Es suficiente con configurar los Servidores de administración una vez. Después, podrá obtener actualizaciones con la frecuencia que necesite, por ejemplo, una o varias veces al día.

Acerca de la corrección de vulnerabilidades de software de terceros

El proceso de reparar vulnerabilidades de software de terceros en una red aislada se muestra en la figura y se describe a continuación. Puedes repetir este proceso periódicamente.



El proceso de transmisión de parches y la lista de actualizaciones requeridas entre el Servidor de administración con acceso a Internet y los Servidores de administración aislados

Cada Servidor de administración aislado de Internet (en adelante, Servidor de administración aislado) genera una lista de actualizaciones que deben instalarse en los dispositivos administrados conectados a este Servidor de administración. La lista de actualizaciones requeridas se almacena en una carpeta específica y presenta un conjunto de archivos binarios. Cada archivo tiene un nombre que contiene el ID del parche con la actualización necesaria. Como resultado, cada archivo de la lista apunta a un parche específico.

Al usar un dispositivo externo, transfiere la lista de actualizaciones requeridas desde el Servidor de administración aislado al Servidor de administración asignado con acceso a Internet. Después de eso, el Servidor de administración asignado descarga los parches de Internet y los coloca en una carpeta separada.

Cuando todos los parches se descargan y se ubican en la carpeta especial para ellos, mueve los parches a cada Servidor de administración aislado del que ha tomado una lista de actualizaciones necesarias. Los parches se guardan en la carpeta creada especialmente para ellos en el Servidor de administración aislado. Como resultado, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* ejecuta parches e instala actualizaciones en los dispositivos administrados de los Servidores de administración aislados.

Configuración del Servidor de administración con acceso a Internet para corregir vulnerabilidades en una red aislada

Para prepararse en la tarea de corregir vulnerabilidades y transmitir parches en una red aislada, primero configure el Servidor de administración con acceso a Internet y luego configure los servidores de administración aislados.

Para configurar un Servidor de administración con acceso a Internet, haga lo siguiente:

1. Cree dos carpetas en un disco donde esté instalado el Servidor de administración:

   - Carpeta para obtener la lista de actualizaciones necesarias
   - Carpeta para parches

   Puedes darle el nombre que desee a estas carpetas.

2. Otorgue los derechos de modificación al grupo KL Admins en las carpetas creadas, utilizando las herramientas administrativas estándar del sistema operativo.

3. Utilice la utilidad klscflag para escribir las rutas a las carpetas en las propiedades del Servidor de administración. Introduzca los siguientes comandos en el símbolo del sistema de Windows, usando derechos de administrador:

   - Para establecer la ruta a la carpeta de parches, haga lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<ruta_a_la_carpeta>"`
   - Para configurar la ruta a la carpeta para la lista de actualizaciones requeridas, haga lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<ruta a la carpeta>"`

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\FolderForPatches"`

4. [Opcional] Utilice la utilidad klscflag para especificar la frecuencia con la que el Servidor de administración debe buscar nuevas solicitudes de parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <valor_en_segundos>`

   El valor predeterminado es 120 segundos.

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

5. Reinicie el servicio del Servidor de administración.

Ahora, el Servidor de administración con acceso a Internet está listo para descargar y transmitir actualizaciones a Servidores de administración aislados. Antes de comenzar a corregir vulnerabilidades, configure los Servidores de administración aislados.

Configuración de Servidores de administración aislados para corregir vulnerabilidades en una red aislada

Después de terminar de configurar el Servidor de administración con acceso a Internet, prepare cada Servidor de administración aislado en su red, para que pueda corregir vulnerabilidades e instalar actualizaciones en dispositivos administrados conectados a Servidores de administración aislados.

Para configurar Servidores de administración aislados, realice las siguientes acciones en cada Servidor de administración:

1. Active una clave de licencia para la función Administración de vulnerabilidades y parches (VAPM).

2. Cree dos carpetas en un disco donde esté instalado el Servidor de administración:

   - Carpeta donde aparecerá la lista de actualizaciones necesarias.
   - Carpeta para parches

Puedes darle el nombre que desee a estas carpetas.

3. Otorgue los derechos de *modificación* al grupo KLAdmins en las carpetas creadas, utilizando las herramientas administrativas estándar del sistema operativo.

4. Utilice la utilidad klscflag para escribir las rutas a las carpetas en las propiedades del Servidor de administración. Introduzca los siguientes comandos en el símbolo del sistema de Windows, usando derechos de administrador:

   - Para establecer la ruta a la carpeta de parches, haga lo siguiente:
     `klshcflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<ruta_a_la_carpeta>"`

   - Para configurar la ruta a la carpeta para la lista de actualizaciones requeridas, haga lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<ruta_a_la_carpeta>"`

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\FolderForPatches"`

5. [Opcional] Utilice la utilidad klscflag para especificar la frecuencia con la que el Servidor de administración aislado debe buscar nuevos parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <valor_en_segundos>`

   El valor predeterminado es 120 segundos.

   Ejemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

6. [Opcional] Use la utilidad klscflag para calcular los hashes SHA-256 de los parches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Si introduce ingresa este comando, puede asegurarse de que los parches no se hayan modificado durante su transferencia al Servidor de administración aislado, y que haya recibido los parches correctos que contienen las actualizaciones requeridas.

   De manera predeterminada, Kaspersky Security Center no calcula los hashes SHA-256 de los parches. Si activa esta opción, después de que el Servidor de administración aislado reciba los parches, Kaspersky Security Center calcula sus valores hash y compara los valores adquiridos con los valores hash almacenados en la base de datos del Servidor de administración. Si el hash calculado no coincide con el hash en la base de datos, se produce el error y debe reemplazar los parches incorrectos.

7. Cree la tarea *Buscar vulnerabilidades y actualizaciones requeridas* y establecer la programación de tareas. Ejecute la tarea si desea que se ejecute antes de lo especificado en el programa de tareas.

8. Reinicie el servicio del Servidor de administración.

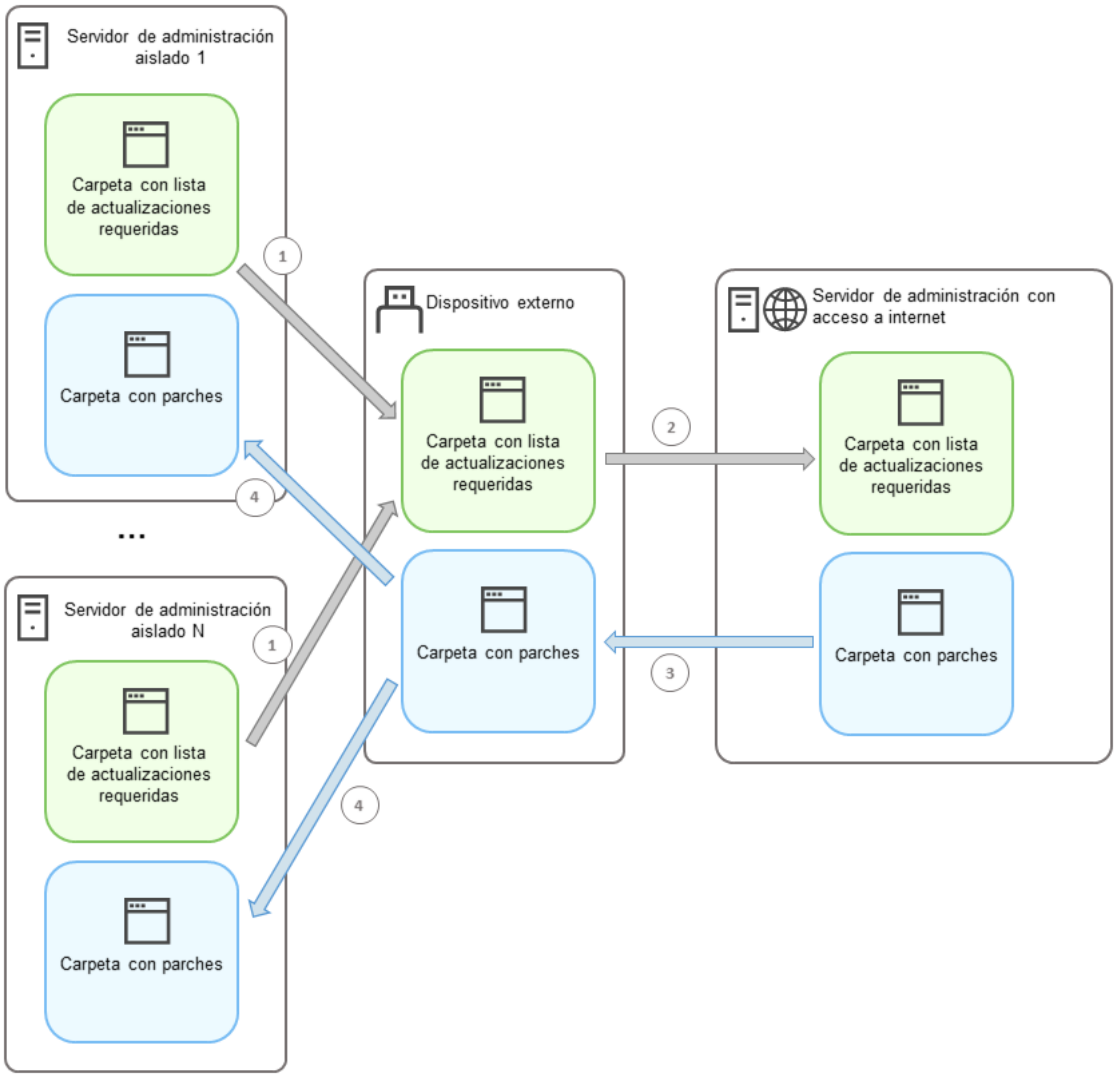
Después de configurar todos los Servidores de administración, puede mover parches y listas de actualizaciones requeridas y reparar vulnerabilidades de software de terceros en dispositivos administrados en la red aislada.

Transmitir parches e instalar actualizaciones en una red aislada

Después de haber terminado la configuración de los Servidores de administración, puede transferir parches que contengan actualizaciones necesarias desde el Servidor de administración con acceso a Internet a los Servidores de administración aislados. Puede transmitir e instalar actualizaciones con la frecuencia que necesite, por ejemplo, una o varias veces al día.

Necesita un dispositivo externo, como una unidad extraíble, para transferir los parches y la lista de actualizaciones requeridas entre los Servidores de administración. Por lo tanto, asegúrese de que el dispositivo externo tenga suficiente espacio en disco para descargar y almacenar parches.

El proceso de transmisión de parches y la lista de actualizaciones requeridas se muestran en la imagen y se describen a continuación:



El proceso de transmisión de parches y la lista de actualizaciones requeridas entre el Servidor de administración con acceso a Internet y los Servidores de administración aislados

Para instalar actualizaciones y corregir vulnerabilidades en dispositivos administrados conectados a Servidores de administración aislados, haga lo siguiente:

1. Iniciar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, si aún no se la está ejecutando.
2. Conecte un dispositivo externo a cualquier Servidor de administración aislado.
3. Cree dos carpetas en el dispositivo externo: una para la lista de actualizaciones requeridas y otra para parches. Puedes darle el nombre que desee a estas carpetas.

   Si ha creado estas carpetas anteriormente, bórrelas.
4. Copie la lista de actualizaciones requeridas de cada Servidor de administración aislado y péguela en la carpeta para la lista de actualizaciones requeridas en el dispositivo externo.

Como resultado, une todas las listas adquiridas de todos los Servidores de administración aislados en una carpeta. Esta carpeta contiene archivos binarios con los ID de los parches necesarios para todos los Servidores de administración aislados.

5. Conecte el dispositivo externo al Servidor de administración con acceso a Internet.

6. Copie la lista de actualizaciones requeridas del dispositivo externo y pegue esta lista en la carpeta de la lista de actualizaciones requeridas en el Servidor de administración con acceso a Internet.

   Todos los parches necesarios se descargan automáticamente de Internet a la carpeta de parches del Servidor de administración. Esto puede llevar varias horas.

7. Asegúrese de descargar todos los parches necesarios. Para ello, puede realizar una de las acciones siguientes:

   - Revise la carpeta en busca de parches en el Servidor de administración con acceso a Internet. Todos los parches que se especificaron en la lista de actualizaciones requeridas deben descargarse en una carpeta necesaria. Esto es más conveniente si se requiere una cantidad pequeña de parches.

   - Prepare un script especial, por ejemplo, un script de shell. Si obtiene una gran cantidad de parches, será difícil comprobar por sí mismo que se han descargado todos los parches. En tales casos, es mejor automatizar el control.

8. Copie los parches del Servidor de administración con acceso a Internet y péguelos en la carpeta correspondiente del dispositivo externo.

9. Transfiera los parches a todos los Servidores de administración aislados. Coloque los parches en una carpeta específica para ellos.

Como resultado, cada Servidor de administración aislado crea una lista real de actualizaciones, que son necesarias para los dispositivos administrados conectados al Servidor de administración actual. Después de que el Servidor de administración con acceso a Internet reciba la lista de actualizaciones requeridas, el Servidor de administración descarga parches de Internet. Cuando estos parches aparecen en Servidores de administración aislados, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* gestiona los parches. Por lo tanto, las actualizaciones se instalan en los dispositivos administrados y se corrigen las vulnerabilidades del software de terceros.

Cuando la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se está ejecutando, no reinicie el dispositivo del Servidor de administración y no ejecute la tarea *Copia de seguridad de los datos del Servidor de administración* (porque también provocará un reinicio). En este caso, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se interrumpe y las actualizaciones no se instalan. En este caso, debe reiniciar la tarea manualmente o esperar a que la tarea se inicie de acuerdo con el cronograma configurado.

Desactivar la opción de transmitir parches e instalar actualizaciones en una red aislada

Puede desactivar la transmisión de parches en los Servidores de administración aislados, por ejemplo, si decide sacar uno o más Servidores de administración de una red aislada. De esta forma, puede reducir la cantidad de parches y el tiempo para descargarlos.

Para desactivar la opción de transmitir parches en Servidores de administración aislados, haga lo siguiente:

1. Si desea eliminar el aislamiento de todos los Servidores de administración, en las propiedades del Servidor de administración con acceso a Internet, elimine las rutas a las carpetas de parches y la lista de las actualizaciones necesarias. Si desea mantener algunos Servidores de administración en una red aislada, omita este paso.

   Introduzca los siguientes comandos en el símbolo del sistema de Windows, usando derechos de administrador:

- Para eliminar la ruta a la carpeta de parches, haga lo siguiente:
  `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""`

- Para eliminar la ruta a la carpeta para una lista de actualizaciones necesarias, haga lo siguiente:
  `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""`

2. Reinicie el servicio del Servidor de administración si eliminó las rutas a las carpetas en este Servidor de administración.

3. En las propiedades de cada Servidor de administración que desee sacar del aislamiento, elimine las rutas a las carpetas de parches y la lista de actualizaciones necesarias.

   Introduzca los siguientes comandos en el símbolo del sistema de Windows, usando derechos de administrador:

   - Para eliminar la ruta a la carpeta de parches, haga lo siguiente:
     `klshcflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""`

   - Para eliminar la ruta a la carpeta para una lista de actualizaciones necesarias, haga lo siguiente:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""`

4. Reinicie el servicio de cada Servidor de administración donde haya eliminado las rutas a las carpetas.

Como resultado, si reconfiguró el Servidor de administración con acceso a Internet, ya no recibirá parches a través de Kaspersky Security Center. Si reconfiguró solo algunos Servidores de administración aislados, por ejemplo, si sacó algunos de ellos de la red aislada, obtendrá parches solo para los Servidores de administración aislados restantes.

Si desea comenzar a corregir vulnerabilidades en Servidores de administración aislados desactivados en el futuro, debe configurar estos Servidores de administración y el Servidores de administración con acceso a Internet una vez más.

Ignorar las vulnerabilidades de software

Puede ignorar las vulnerabilidades de software que se corregirán. Las razones para ignorar las vulnerabilidades de software pueden ser, por ejemplo, las siguientes:

- No considera que la vulnerabilidad de software sea crítica para su organización.

- Comprende que la reparación de la vulnerabilidad de software puede dañar los datos relacionados con el software que causaron la reparación de la vulnerabilidad.

- Está seguro de que la vulnerabilidad de software no es peligrosa para la red de su organización porque utiliza otras medidas para proteger sus dispositivos administrados.

Puede ignorar una vulnerabilidad de software en todos los dispositivos administrados o solo en determinados dispositivos administrados.

Para ignorar una vulnerabilidad de software en todos los dispositivos administrados:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Vulnerabilidades de software**.

   El espacio de trabajo de la carpeta muestra una lista de las vulnerabilidades que detecta el Agente de red en aplicaciones instaladas en dispositivos cliente.

2. Seleccione la vulnerabilidad que desee ignorar.

3. Seleccione **Propiedades** en el menú contextual de la vulnerabilidad.

   Se abrirá la ventana de propiedades de la vulnerabilidad.

4. En la sección **General**, seleccione la opción **Ignorar vulnerabilidad**.

5. Haga clic en **Aceptar**.

   La ventana de propiedades de vulnerabilidad de software está cerrada.

La vulnerabilidad de software se ignora en todos los dispositivos administrados.

Para ignorar una vulnerabilidad de software en los dispositivos administrados seleccionados:

1. Abra la ventana de propiedades del dispositivo administrado seleccionado y seleccione la sección **Vulnerabilidades de software**.

2. Seleccione una vulnerabilidad de software.

3. Ignore la vulnerabilidad seleccionada.

La vulnerabilidad de software se ignora en el dispositivo seleccionado.

La vulnerabilidad de software ignorada no se reparará una vez que se hayan completado las tareas *Reparar vulnerabilidades* o *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Puede excluir vulnerabilidades de software ignoradas de la lista de vulnerabilidades mediante el filtro.

Selección de soluciones de usuario para vulnerabilidades en software de terceros

Para usar la tarea *Reparar vulnerabilidades*, debe especificar manualmente las actualizaciones de software para reparar las vulnerabilidades en el software de terceros que se enumera en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza correcciones recomendadas para el software de Microsoft y correcciones de usuario para otro software de terceros. Las *correcciones de usuario* son actualizaciones de software para reparar vulnerabilidades que el administrador especifica manualmente para la instalación.

Para seleccionar las soluciones de usuario para vulnerabilidades en software de terceros:

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Vulnerabilidades de software**.

   El espacio de trabajo de la carpeta muestra una lista de las vulnerabilidades que detecta el Agente de red en aplicaciones instaladas en dispositivos cliente.

2. Seleccione la vulnerabilidad para la que desea añadir una solución de usuario.

3. Seleccione **Propiedades** en el menú contextual de la vulnerabilidad.

   Se abrirá la ventana de propiedades de la vulnerabilidad.

4. En la sección **Reparaciones del usuario u otras reparaciones**, haga clic en el botón **Agregar**.

   Se muestra una lista disponible de paquetes de instalación. La lista de paquetes de instalación mostrados corresponde a la lista **Instalación remota → Paquetes de instalación**. Si no ha creado un paquete de instalación que contenga la reparación del usuario para la vulnerabilidad seleccionada, ahora puede crear el paquete iniciando el Asistente de nuevo paquete.

5. Seleccione uno o más paquetes de instalación que contengan una o más reparaciones del usuario para la vulnerabilidad en el software de terceros.

6. Haga clic en **Aceptar**.

Se especifican los paquetes de instalación que contienen reparaciones de usuario para la vulnerabilidad de software. Cuando se inicie la tarea *Reparar vulnerabilidades*, se instalará el paquete de instalación y se reparará la vulnerabilidad de software.

Reglas para instalar la actualizaciones

Al corregir vulnerabilidades en aplicaciones, debe especificar reglas para la instalación de actualizaciones. Estas reglas determinan actualizaciones para instalar y vulnerabilidades para reparar.

La configuración exacta depende de si crea una regla para las actualizaciones de las aplicaciones de Microsoft, para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) o para todas las aplicaciones. Al crear una regla para aplicaciones de Microsoft o aplicaciones de terceros, puede seleccionar aplicaciones específicas y versiones de aplicaciones para las que desee instalar actualizaciones. Al crear una regla para todas las aplicaciones, puede seleccionar las actualizaciones específicas que desee instalar y las vulnerabilidades que desee corregir mediante la instalación de actualizaciones.

Para crear una nueva regla para las actualizaciones de todas las aplicaciones:

1. En la página **Configuración** del Asistente para añadir tareas, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance a través del Asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página de **Criterios generales**, use las listas desplegables para especificar las siguientes configuraciones:

   - **Conjunto de actualizaciones para instalar**

     Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:

     - **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

   - **Reparar vulnerabilidades con un nivel de gravedad igual o mayor que**

A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

Esta opción está desactivada de forma predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones para instalar:

- **Instalar todas las actualizaciones pertinentes**

  Instalar todas las actualizaciones de software que cumplan con los criterios especificados en la página de **Criterios generales** del Asistente. Seleccionado de forma predeterminada.

- **Instalar solo las actualizaciones de la lista**

  Instalar solo actualizaciones de software que seleccione manualmente desde la lista. Esta lista contiene todas las actualizaciones de software disponibles.

  Por ejemplo, puede desear seleccionar actualizaciones específicas en los casos siguientes: comprobar su instalación en un entorno de prueba, actualizar solo aplicaciones críticas o actualizar solo aplicaciones específicas.

  - **Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas**

    Mantenga esta opción activada si está de acuerdo con la instalación de versiones de aplicaciones provisionales cuando sea necesario para instalar las actualizaciones seleccionadas.

    Si esta opción está desactivada, solo se instalarán las versiones seleccionadas de las aplicaciones. Desactive esta opción si desea actualizar las aplicaciones de una manera directa, sin intentar instalar versiones sucesivas de forma progresiva. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

    Por ejemplo, tiene la versión 3 de una aplicación instalada en un dispositivo y desea actualizarla a la versión 5, pero la versión 5 de esta aplicación solo se puede instalar sobre la versión 4. Si esta opción está activada, el software instala primero la versión 4 y luego la versión 5. Si esta opción está desactivada, el software no actualiza la aplicación.

    Esta opción está activada de forma predeterminada.

5. En la página de **Vulnerabilidades**, seleccione las vulnerabilidades que se corregirán al instalar las actualizaciones seleccionadas:

- **Reparar todas las vulnerabilidades que coinciden con otros criterios**

  Reparar todas las vulnerabilidades que cumplan con los criterios especificados en la página de **Criterios generales** del Asistente. Seleccionado de forma predeterminada.

- **Reparar solo las vulnerabilidades de la lista**

Solucione solo las vulnerabilidades que seleccione manualmente de la lista. Esta lista contiene todas las vulnerabilidades detectadas.

Por ejemplo, es posible que desee seleccionar vulnerabilidades específicas en los siguientes casos: para verificar su corrección en un entorno de prueba, para corregir vulnerabilidades solo en aplicaciones críticas o para corregir vulnerabilidades solo en aplicaciones específicas.

6. En la página **Nombre**, especifique el nombre de la regla que está creando. Más tarde, puede cambiar este nombre en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se crea y se muestra en el campo **Especificar reglas para instalar actualizaciones** del Asistente para añadir tareas.

Para crear una nueva regla para las actualizaciones de las aplicaciones de Microsoft:

1. En la página **Configuración** del Asistente para añadir tareas, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance a través del Asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página **Criterios generales**, especifique la siguiente configuración:

- Conjunto de actualizaciones para instalar

  Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:

  - **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
  - **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
  - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

- Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

  A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

  Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

  Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

  Esta opción está desactivada de forma predeterminada.

- Reparar vulnerabilidades con un nivel de gravedad MSRC igual o mayor que

A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

Si esta opción está activada, las actualizaciones solucionan solo aquellas vulnerabilidades para las cuales el nivel de gravedad establecido por el Centro de respuesta de seguridad de Microsoft (MSRC) es igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

Esta opción está desactivada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desea instalar actualizaciones. De forma predeterminada, todas las aplicaciones están seleccionadas.

5. En la página **Categorías de actualizaciones**, seleccione las actualizaciones para instalar. Estas categorías están igual que en Microsoft Update Catalog. De forma predeterminada, todas las categorías están seleccionadas.

6. En la página **Nombre**, especifique el nombre de la regla que está creando. Más tarde, puede cambiar este nombre en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Después de que el Asistente finaliza su operación, la nueva regla se crea y se muestra en el campo **Especificar reglas para instalar actualizaciones** del Asistente para añadir tareas.

Para crear una nueva regla para las actualizaciones de aplicaciones de terceros:

1. En la página **Configuración** del Asistente para añadir tareas, haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance a través del Asistente utilizando el botón **Siguiente**.

2. En la página **Tipo de regla**, seleccione **Regla para actualizaciones de terceros**.

3. En la página **Criterios generales**, especifique la siguiente configuración:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:

     - **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

   - Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

Esta opción está desactivada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desea instalar actualizaciones. De forma predeterminada, todas las aplicaciones están seleccionadas.

5. En la página **Nombre**, especifique el nombre de la regla que está creando. Más tarde, puede cambiar este nombre en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Después de que el Asistente finaliza su operación, la nueva regla se crea y se muestra en el campo **Especificar reglas para instalar actualizaciones** del Asistente para añadir tareas.

Grupos de aplicaciones

Esta sección describe cómo administrar grupos de aplicaciones instaladas en dispositivos.

Creación de categorías de aplicaciones

Kaspersky Security Center permite crear categorías de aplicaciones instaladas en equipos cliente.

Las categorías de aplicaciones se pueden crear de una de estas formas:

- El administrador especifica una carpeta en la que los archivos ejecutables se han incluido en la categoría seleccionada.
- El administrador especifica un dispositivo cuyos archivos ejecutables se incluirán en la categoría seleccionada.
- El administrador establece los criterios que se deben utilizar para incluir aplicaciones en la categoría seleccionada.

Cuando se crea una categoría de aplicaciones, el administrador puede establecer reglas para dicha categoría. Las reglas definen el comportamiento de las aplicaciones incluidas en la categoría especificada. Por ejemplo, puede bloquear o permitir la ejecución de las aplicaciones incluidas en la categoría.

Administrar la ejecución de aplicaciones en los dispositivos

Kaspersky Security Center le permite administrar ejecuciones de aplicaciones en dispositivos en el modo Lista de admitidos. Para obtener más información, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows. Mientras está activado el modo Lista de admitidos, en los dispositivos seleccionados solo se pueden ejecutar las aplicaciones pertenecientes a las categorías especificadas. El administrador puede visualizar los resultados del análisis estático de las reglas de ejecución de aplicaciones en los dispositivos de cada usuario.

Inventario del software instalado en dispositivos

Kaspersky Security Center le permite realizar un inventario de software en dispositivos que ejecutan Windows. El Agente de red recopila información acerca de todas las aplicaciones instaladas en los dispositivos. La información recuperada durante el inventario se muestra en el espacio de trabajo de la carpeta **Registro de aplicaciones**. El administrador puede ver información detallada sobre cualquier aplicación, como su versión y fabricante.

El número de archivos ejecutables recibidos de un solo dispositivo no puede ser superior a 150 000. Habiendo alcanzado este límite, Kaspersky Security Center no podrá recibir ningún nuevo archivo.

Administración del grupo de aplicaciones con licencia

Kaspersky Security Center permite crear grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia incluye las aplicaciones que cumplen los criterios establecidos por el administrador. El administrador puede especificar los siguientes criterios para grupos de aplicaciones con licencia:

- Nombre de la aplicación
- Versión de la aplicación
- Fabricante
- Etiqueta de la aplicación

Las aplicaciones que cumplan uno o varios criterios se incluyen automáticamente en un grupo. Para crear un grupo de aplicaciones con licencia, debe establecer al menos un criterio de inclusión de aplicaciones en dicho grupo.

Cada grupo de aplicaciones con licencia dispone de una clave de licencia propia. La clave de licencia de un grupo de aplicaciones con licencia define el número máximo de instalaciones permitidas para las aplicaciones incluidas en este grupo. Si el número de instalaciones supera el límite que establece la clave de licencia, se registra un evento de información en el Servidor de administración. El administrador puede especificar una fecha de caducidad para la clave de licencia. Cuando llega dicha fecha, se registra un evento de información en el Servidor de administración.

Visualización de la información acerca de los archivos ejecutables

Kaspersky Security Center recupera toda la información sobre los archivos ejecutables que se han ejecutado en los dispositivos desde que se instaló en ellos el sistema operativo. La información sobre los archivos ejecutables se muestra en la ventana principal de la aplicación, en el espacio de trabajo de la carpeta **Archivos ejecutables**.

Escenario: administración de aplicaciones

Puede administrar el inicio de aplicaciones en dispositivos de usuario. Puede permitir o bloquear aplicaciones para que se ejecuten en dispositivos administrados. Esta funcionalidad se ejecuta mediante el componente Control de aplicaciones. Solo puede administrar aplicaciones instaladas en dispositivos Windows.

Requisitos previos

- Kaspersky Security Center se ha implementado en su organización.

- Entre los dispositivos administrados en su organización hay dispositivos que ejecutan Windows.
- Se crea la directiva Kaspersky Endpoint Security para Windows y se activa.

Etapas

El escenario de uso de Control de aplicaciones procede en etapas:

1. **Formar y ver la lista de aplicaciones en dispositivos cliente**

   Esta etapa le ayuda a encontrar las aplicaciones que están instaladas en los dispositivos administrados. Puede ver la lista de aplicaciones y decidir las aplicaciones que desea permitir y prohibir, de acuerdo con las directivas de seguridad de su organización. Las restricciones pueden estar relacionadas con las directivas de seguridad de la información en su organización. Puede omitir esta etapa si sabe exactamente las aplicaciones que están instaladas en los dispositivos administrados.

   Instrucciones:

   - Consola de administración: visualización del registro de aplicaciones
   - Kaspersky Security Center 14 Web Console: obtención y visualización de una lista de aplicaciones instaladas en dispositivos cliente

2. **Formar y ver la lista de archivos ejecutables en dispositivos cliente**

   Esta etapa le ayuda a descubrir qué archivos ejecutables se encuentran en los dispositivos administrados. Examine la lista de los archivos ejecutables y compárela con las listas de archivos ejecutables permitidos y prohibidos. Las restricciones sobre el uso de archivos ejecutables pueden estar relacionadas con las directivas de seguridad de la información de su organización. Puede omitir esta etapa si sabe exactamente los archivos ejecutables están instalados en los dispositivos administrados.

   Instrucciones:

   - Consola de administración: inventario de archivos ejecutables
   - Kaspersky Security Center 14 Web Console: obtención y visualización de una lista de archivos ejecutables almacenados en dispositivos cliente

3. **Crear categorías de aplicaciones para las aplicaciones utilizadas en su organización**

   Analizar las listas de aplicaciones y archivos ejecutables almacenados en los dispositivos administrados. Basándose en el análisis, crear categorías de aplicaciones. Se recomienda crear una categoría de «Aplicaciones de trabajo» que cubra el conjunto estándar de aplicaciones que se utilizan en su organización. Si diferentes grupos de usuarios usan diferentes conjuntos de aplicaciones en su trabajo, se puede crear una categoría de aplicación separada para cada grupo de usuarios.

   Según el conjunto de criterios para crear una categoría de aplicación, puede crear categorías de aplicación de tres tipos.

   Instrucciones:

   - Consola de administración: Crear categorías de aplicaciones para las directivas de Kaspersky Endpoint Security para Windows, Crear una categoría de aplicaciones con contenido agregado manualmente, Crear una categoría de aplicaciones con contenido agregado automáticamente
   - Kaspersky Security Center 14 Web Console: Crear categoría de aplicación con contenido agregado manualmente, Crear una categoría de aplicación que incluya archivos ejecutables de dispositivos seleccionados, Crear una categoría de aplicación que incluya archivos ejecutables de la carpeta seleccionada

4. **Configuración del Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows**

Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows utilizando las categorías de aplicaciones que creó en la etapa anterior.

Instrucciones:

- Consola de administración: configuración de administración de inicio de aplicaciones en los dispositivos cliente
- Kaspersky Security Center 14 Web Console: Configuración de Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows

5. **Activación del componente de control de aplicaciones en modo de prueba**

A fin de garantizar que las reglas de Control de aplicaciones no bloqueen las aplicaciones necesarias para el trabajo, se recomienda habilitar la prueba de las reglas de Control de aplicaciones y analizar su funcionamiento después de crear nuevas reglas. Cuando la prueba está activada, Kaspersky Endpoint Security para Windows no bloqueará las aplicaciones cuyo inicio esté prohibido por las reglas de Control de aplicaciones, sino que enviará notificaciones sobre su inicio al Servidor de administración.

Al probar las reglas de Control de aplicaciones, se recomienda realizar las siguientes acciones:

- Determinar el periodo de prueba. El periodo de prueba puede variar de varios días a dos meses.
- Examinar los eventos resultantes de la prueba del funcionamiento del Control de aplicaciones.

Instrucciones para Kaspersky Security Center 14 Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y active la opción **Modo de prueba** en el proceso de configuración.

6. **Cambiar la configuración de categorías de aplicaciones del componente Control de aplicaciones**

Si es necesario, realice cambios en la configuración de Control de aplicaciones. En función de los resultados de la prueba, puede agregar archivos ejecutables relacionados con eventos del componente Control de aplicaciones a una categoría de aplicación con contenido agregado manualmente.

Instrucciones:

- Consola de administración: Añadir archivos ejecutables relacionados con eventos a la categoría de la aplicación
- Kaspersky Security Center 14 Web Console: Agregar archivos ejecutables relacionados con eventos a la categoría de aplicación

7. **Aplicar las reglas de Control de aplicaciones en modo operación**

Después de probar las reglas de Control de aplicaciones y completar la configuración de las categorías de aplicaciones, puede aplicar las reglas de Control de aplicaciones en el modo de operación.

Instrucciones para Kaspersky Security Center 14 Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y desactive la opción **Modo de prueba** en el proceso de configuración.

8. **Verificación de la configuración de Control de aplicaciones**

Asegúrese de haber hecho lo siguiente:

- Creado categorías de aplicaciones.
- Configurado Control de aplicaciones mediante las categorías de aplicaciones.
- Aplicado de las reglas de Control de aplicaciones en modo de operación.

Resultados

Cuando se completa el escenario, se controla el inicio de aplicaciones en dispositivos administrados. Los usuarios solo pueden iniciar las aplicaciones que estén permitidas en su organización y no aquellas que estén prohibidas.

Para obtener información detallada acerca de Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Creación de categorías de aplicaciones para las directivas de Kaspersky Endpoint Security para Windows

Puede crear categorías de aplicaciones para las directivas de Kaspersky Endpoint Security para Windows desde la carpeta **Categorías de aplicaciones** y desde la ventana **Propiedades** de una directiva de Kaspersky Endpoint Security para Windows.

*Para crear una categoría de aplicación para una directiva de Kaspersky Endpoint Security desde la carpeta de **Categorías de aplicaciones**:*

1. En el árbol de consola, seleccione **Avanzado → Administración de aplicaciones → Categorías de aplicaciones**.
2. En el espacio de trabajo de la carpeta **Categorías de aplicaciones**, haga clic en el botón **Categoría nueva**.

   Se inicia el Asistente para crear nueva categoría.
3. En la página **Tipo de categoría**, seleccione el tipo de la categoría del usuario:
   - **Categoría con contenido agregado manualmente**. Especifique los criterios que serán usados para asignar archivos ejecutables a la categoría creada.
   - **Categoría con contenido agregado automáticamente**. Especifique la carpeta desde la cual se asignarán automáticamente los archivos ejecutables a la categoría creada.

     Al crear una categoría con contenido agregado automáticamente, la aplicación de los inventarios en los siguientes formatos de archivo: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, y SCR.
   - **Categoría que incluye archivos ejecutables de dispositivos seleccionados**. Especifique un dispositivo cuyos archivos ejecutables se deban asignar automáticamente a la categoría.
4. Siga las instrucciones del Asistente.

Cuando el Asistente finaliza, se crea una categoría de aplicación personalizada. Puede ver categorías recién creadas utilizando la lista de categorías en el espacio de trabajo de la carpeta **Categorías de aplicaciones**.

También puede crear una categoría de aplicación desde la carpeta **Directivas**.

*Para crear una categoría de aplicación desde la ventana **Propiedades** de una directiva de Kaspersky Endpoint Security para Windows:*

1. En el árbol de consola, seleccione la carpeta **Directivas**.

2. En el espacio de trabajo de la carpeta **Directivas**, seleccione una directiva de Kaspersky Endpoint Security para la que desea crear una categoría.

3. Haga clic derecho y seleccione **Propiedades**.

4. En la ventana **Propiedades** que se abre, en el panel **Secciones** a la izquierda, seleccione **Controles de seguridad → Control de aplicaciones**.

5. En la sección **Control de aplicaciones**, en el **modo Control** y en las listas desplegables **Acción**, realice las selecciones para la lista de admitidos o la lista de rechazados y, a continuación, haga clic en el botón **Añadir**.

   Se abrirá la ventana de la **Regla de control de aplicaciones** que contiene una lista de categorías.

6. Haga clic en el botón **Crear nueva**.

7. Introduzca el nombre de la nueva categoría y haga clic en **Aceptar**.

   Se inicia el Asistente para crear nueva categoría.

8. En la página **Tipo de categoría**, seleccione el tipo de la categoría del usuario:

   - **Categoría con contenido agregado manualmente**. Especifique los criterios que serán usados para asignar archivos ejecutables a la categoría creada.
   - **Categoría con contenido agregado automáticamente**. Especifique la carpeta desde la cual se asignarán automáticamente los archivos ejecutables a la categoría creada.

     Al crear una categoría con contenido agregado automáticamente, la aplicación de los inventarios en los siguientes formatos de archivo: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX, y SCR.

   - **Categoría que incluye archivos ejecutables de dispositivos seleccionados**. Especifique un dispositivo cuyos archivos ejecutables se deban asignar automáticamente a la categoría.

9. Siga las instrucciones del Asistente.

Cuando el Asistente finaliza, se crea una categoría de aplicación personalizada. Puede ver las categorías recién creadas en la lista de categorías.

El componente Control de aplicaciones incluido en Kaspersky Endpoint Security para Windows utiliza las categorías de aplicaciones. El Control de aplicaciones permite que el administrador imponga restricciones al inicio de aplicaciones en dispositivos cliente, por ejemplo, restringiendo los inicios a aplicaciones en una categoría especificada.

Creación de una categoría de aplicaciones con contenido agregado manualmente

Para crear una categoría de aplicaciones con contenido agregado manualmente, haga lo siguiente:

1. En el árbol de consola, en la carpeta **Avanzado → Administración de aplicaciones**, seleccione la subcarpeta **Categorías de aplicaciones**.

2. Haga clic en el botón **Categoría nueva**.

Se inicia el Asistente para crear nueva categoría.

3. En la página del Asistente, seleccione **Categoría con contenido agregado manualmente** como el tipo de categoría del usuario.

4. En la página **Configurar condiciones para incluir aplicaciones en categorías**, haga clic en el botón **Agregar**.

5. En la lista desplegable, especifique la configuración relevante:

   - **Desde la lista de archivos ejecutables**

     Si esta opción está seleccionada, puede usar la lista de archivos ejecutables en el dispositivo cliente para seleccionar aplicaciones y agregarlas a la categoría.

   - **De propiedades del archivo**

     Si se selecciona esta opción, se pueden especificar los datos detallados de los archivos ejecutables que se agregarán a la categoría de aplicaciones personalizada.

   - **Metadatos desde archivos en carpeta**

     Especifique una carpeta en el dispositivo cliente que contenga archivos ejecutables. Los metadatos de los archivos ejecutables incluidos en la carpeta especificada se enviarán al Servidor de administración. Los archivos ejecutables con los mismos metadatos se agregarán a la categoría de aplicaciones personalizada.

   - **Sumas de verificación de los archivos en la carpeta**

     Si se selecciona esta opción, se podrán seleccionar o crear carpetas en un dispositivo cliente. El hash MD5 de los archivos en una carpeta especificada se enviará al Servidor de administración. Las aplicaciones que tengan el mismo hash que los archivos de la carpeta especificada se agregarán a la categoría de aplicación personalizada.

   - **Certificados para los archivos de la carpeta**

     Si esta opción está seleccionada, puede especificar la carpeta en el dispositivo cliente que contiene los archivos ejecutables firmados con certificados. Los certificados de archivos ejecutables se leen y agregan a las condiciones de la categoría. Los archivos ejecutables que se han firmado de acuerdo con los certificados especificados se agregarán a la categoría de usuario.

   - **Metadatos de archivos del programa de instalación MSI**

     Si se selecciona esta opción, puede especificar un archivo de instalación MSI como condición para agregar aplicaciones a la categoría personalizada. Los metadatos del instalador de la aplicación se enviarán al Servidor de administración. Las aplicaciones cuyos metadatos de instalador sean los mismos que los del programa de instalación MSI especificado se agregarán a la categoría de aplicaciones personalizada.

   - **Sumas de comprobación de los archivos del programa de instalación MSI de la aplicación**

Si se selecciona esta opción, puede especificar un archivo de instalación MSI como condición para agregar aplicaciones a la categoría personalizada. El hash del programa de instalación de la aplicación se enviará al Servidor de administración. Las aplicaciones para las cuales el hash de archivos del instalador MSI es idéntico al hash especificado se agregan a la categoría de aplicaciones del usuario.

- **De categoría KL**

  Si se selecciona esta opción, puede especificar una categoría de aplicación de Kaspersky como condición para agregar aplicaciones a la categoría personalizada. Las aplicaciones de la categoría Kaspersky especificada se agregarán a la categoría de aplicación personalizada.

- **Carpeta de la aplicación**

  Si se selecciona esta opción, se puede especificar la ruta a la carpeta del dispositivo cliente que contiene los archivos ejecutables que se agregarán a la categoría de aplicación personalizada.

- **Seleccionar el certificado del repositorio**

  Si esta opción está seleccionada, puede especificar los certificados del almacenamiento. Los archivos ejecutables que se han firmado de acuerdo con los certificados especificados se agregarán a la categoría de usuario.

- **Tipo de unidad**

  Si se selecciona esta opción, se puede especificar el tipo de medio (cualquier unidad o disco extraíble) en el que se ejecutará la aplicación. Las aplicaciones que se hayan ejecutado en el tipo selecciona de unidad de disco se agregarán a la categoría de aplicación personalizada.

6. Siga las instrucciones del Asistente.

Kaspersky Security Center solo gestiona metadatos de archivos firmados digitalmente. No se puede crear ninguna categoría sobre la base de metadatos de archivos que no contengan una firma digital.

Cuando el Asistente finaliza, se crea una categoría de aplicaciones del usuario con contenido agregado manualmente. Puede ver la categoría recién creada utilizando la lista de categorías en el espacio de trabajo de la carpeta **Categorías de aplicaciones**.

Creación de una categoría de aplicaciones con contenido agregado automáticamente

Para crear una categoría de aplicaciones con contenido agregado automáticamente, haga lo siguiente:

1. En el árbol de consola, en la carpeta **Avanzado** → **Administración de aplicaciones**, seleccione la subcarpeta **Categorías de aplicaciones**.

2. Haga clic en el botón **Categoría nueva** para iniciar el Asistente para crear nueva categoría.

En la ventana del Asistente, seleccione **Categoría con contenido agregado automáticamente** como el tipo de categoría del usuario.

3. En la ventana **Carpeta de repositorio**, especifique la siguiente configuración:

- **Ruta a la carpeta para la adición automática de contenido por categoría**

  En este campo, especifique la ruta a la carpeta en la que el Servidor de administración buscará periódicamente los archivos ejecutables. La ruta a esta carpeta se especifica al crear la categoría. La ruta a esta carpeta no puede cambiarse.

- **Incluir bibliotecas de vínculo dinámico (DLL) en esta categoría**

  La categoría de aplicaciones incluye bibliotecas de vínculo dinámico (archivos en el formato de DLL) y el componente Control de aplicaciones registra las acciones de esas bibliotecas que se ejecutan en el sistema. Si se incluyen archivos de DLL en la categoría, el rendimiento de Kaspersky Security Center puede verse afectado.

  De forma predeterminada, esta casilla está en blanco.

- **Incluir datos de script en esta categoría**

  La categoría de aplicaciones incluye datos de scripts y la Protección frente a amenazas web no bloquea los scripts. Si se incluyen datos de script en la categoría, el rendimiento de Kaspersky Security Center puede verse afectado.

  De forma predeterminada, esta casilla está en blanco.

- **Algoritmo de cálculo del valor de hash**

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores de hash calculados se almacena en la base de datos del Servidor de administración. El almacenamiento de valores de hash no aumenta significativamente el tamaño de la base de datos.

SHA-256 es una función hash criptográfica: no se ha encontrado ninguna vulnerabilidad en su algoritmo, y por lo que se la considera como la función criptográfica más fiable hoy en día. Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores admiten el cálculo de SHA-256. El cálculo de la función hash MD5 es compatible con todas las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center para archivos en la categoría:

- Si todas los instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, seleccione la casilla **Calcular SHA-256 para archivos en esta categoría (admitido por Kaspersky Endpoint Security 10 Service Pack 2 for Windows o posterior)**. No es aconsejable agregar categorías creadas según el criterio de hash SHA-256 de un archivo ejecutable para versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows. Esto puede causar fallos en el funcionamiento de la aplicación de seguridad. En ese caso, puede usar la función hash criptográfica MD5 para archivos de la categoría.

- Si alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows está instalada en su red, seleccione **Calcular MD5 para archivos de esta categoría (admitido por Kaspersky Endpoint Security, versiones anteriores a 10 Service Pack 2 para Windows)**. No puede agregar una categoría cuyo criterio de creación sea la suma de comprobación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. En ese caso, puede usar la función hash criptográfica SHA-256 para archivos de la categoría.

Si distintos dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, seleccione la casilla **Calcular SHA-256 para archivos en esta categoría** y la casilla **Calcular MD5 para archivos en esta categoría**.

La casilla **Calcular SHA-256 para archivos en esta categoría (admitido por Kaspersky Endpoint Security 10 Service Pack 2 para Windows o posterior)** está seleccionada de forma predeterminada.

La casilla **Calcular MD5 para archivos de esta categoría (admitido por versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** no aparecerá marcada de forma predeterminada.

- Forzar el análisis de la carpeta en busca de cambios

Si esta opción está activada, la aplicación verifica periódicamente la carpeta de adición de contenido de categoría para ver si hay cambios. Puede especificar la frecuencia de comprobaciones (en horas) en el campo de entrada al lado de la casilla de verificación. De forma predeterminada, el intervalo de tiempo entre las comprobaciones forzadas es de 24 horas.

Si esta opción está desactivada, la aplicación no fuerza ninguna de las verificaciones de la carpeta. El servidor intenta acceder a los archivos si se han modificado, agregado o eliminado.

Esta opción está desactivada de forma predeterminada.

- Forzar el análisis de la carpeta en busca de cambios

En este campo, puede especificar el intervalo de tiempo (en horas) después del cual la aplicación iniciará una comprobación forzada de la carpeta de adición automática de contenido por categoría para detectar cualquier cambio. De forma predeterminada, el intervalo de tiempo entre las comprobaciones forzadas es de 24 horas. Este campo estará disponible si se ha seleccionado la casilla **Forzar el análisis de la carpeta en busca de cambios**.

De forma predeterminada, esta casilla está en blanco.

4. Siga las instrucciones del Asistente.

Cuando el Asistente termina, se crea una categoría de aplicaciones con contenido agregado automáticamente. Puede ver la categoría recién creada utilizando la lista de categorías en el espacio de trabajo de la carpeta **Categorías de aplicaciones**.

Añadir archivos ejecutables relacionados con eventos a la categoría de aplicaciones

Puede agregar archivos ejecutables a los eventos **Inicio de aplicación prohibido** y el **Inicio de aplicación prohibido en modo de prueba** a una categoría de aplicación existente con contenido añadido manualmente o a una nueva categoría de aplicación.

Para agregar archivos ejecutables relacionados con eventos de control de aplicaciones a la categoría de aplicaciones:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. En la ficha **Eventos**, seleccione los eventos requeridos.
4. En el menú contextual de uno de los eventos seleccionados, seleccione **Añadir categoría**.
5. En la ventana **Acción en el archivo ejecutable relacionado con el evento** que se abre, especifique la configuración relevante:

   Seleccione uno de los siguientes:

   - **Agregar a una nueva categoría de aplicaciones**

     Seleccione esta opción si desea crear una nueva categoría de aplicaciones.

     Haga clic en **Aceptar** para ejecutar el Asistente para la creación de categorías de usuario. Cuando el Asistente termina, se crea la categoría con la configuración especificada.

     Esta opción no está seleccionada de forma predeterminada.

   - **Agregar a una categoría de aplicaciones existente**

     Seleccione esta opción si tiene que agregar reglas a una categoría de aplicaciones existente. Seleccione la categoría correspondiente en la lista de categorías de aplicaciones.

     Esta opción está seleccionada de forma predeterminada.

En la sección **Tipo de regla**, seleccione una de las siguientes configuraciones:

- **Agregar a categoría**

  Seleccione esta opción si tiene que agregar reglas a las condiciones de la categoría de aplicaciones.

  Esta opción está seleccionada de forma predeterminada.

- **Reglas para agregar exclusiones**

  Seleccione esta opción si desea añadir reglas a las exclusiones de la categoría de aplicaciones.

En la sección **Tipo de información de archivo**, seleccione una de las siguientes configuraciones:

- **Información del certificado (o hashes SHA-256 para archivos sin certificado)**

  Los archivos pueden estar firmados con un certificado. Se pueden firmar varios archivos con el mismo certificado. Por ejemplo, se pueden firmar diferentes versiones de la misma aplicación con el mismo certificado o se pueden firmar varias aplicaciones diferentes del mismo proveedor con el mismo certificado. Cuando selecciona un certificado, varias versiones de una aplicación o varias aplicaciones del mismo proveedor pueden terminar en la categoría.

  Cada archivo tiene su propia función hash SHA-256 exclusiva. Cuando selecciona una función hash SHA-256, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

  Seleccione esta opción si quiere agregar a las reglas de la categoría los detalles del certificado de un archivo ejecutable (o la función hash SHA-256 para archivos sin certificado).

  Esta opción está seleccionada de forma predeterminada.

- **Información de certificado (los archivos sin un certificado se omitirán)**

  Los archivos pueden estar firmados con un certificado. Se pueden firmar varios archivos con el mismo certificado. Por ejemplo, se pueden firmar diferentes versiones de la misma aplicación con el mismo certificado o se pueden firmar varias aplicaciones diferentes del mismo proveedor con el mismo certificado. Cuando selecciona un certificado, varias versiones de una aplicación o varias aplicaciones del mismo proveedor pueden terminar en la categoría.

  Seleccione esta opción si quiere agregar los detalles del certificado de un archivo ejecutable a las reglas de la categoría. Si el archivo ejecutable no tiene certificados, este archivo se omitirá. No se agregará ninguna información sobre este archivo a la categoría.

- **Solo SHA-256 (Los archivos sin hash serán omitidos)**

  Cada archivo tiene su propia función hash SHA-256 exclusiva. Cuando selecciona una función hash SHA-256, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

  Seleccione esta opción si solo quiere agregar los detalles de la función hash SHA-256 del archivo ejecutable.

- **Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service versión Pack 1)**

Cada archivo tiene su propia función hash MD5 exclusiva. Cuando selecciona una función hash MD5, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

Seleccione esta opción si solo quiere agregar los detalles de la función hash MD5 del archivo ejecutable. El cálculo de la función hash MD5 es compatible con Kaspersky Endpoint Security 10 Service Pack 1 for Windows y las versiones anteriores.

6. Haga clic en **Aceptar**.

Configuración de administración de inicio de aplicaciones en los dispositivos cliente

La clasificación de aplicaciones le permite optimizar la administración de ejecuciones de aplicación en dispositivos. Puede crear una categoría de aplicaciones y configurar Control de aplicaciones para una directiva, de modo que solo se inicien aplicaciones de la categoría especificada en dispositivos a los que concierne esa directiva. Por ejemplo, supongamos que ha creado una categoría que incluye aplicaciones denominadas *Aplicación_1* y *Aplicación_2*. Después de añadir esta categoría a una directiva, solo se permite el inicio de dos aplicaciones en dispositivos a los que concierne esta directiva: la *Aplicación_1* y la *Aplicación_2*. Si un usuario intenta usar una aplicación que no se ha incluido en esa categoría (por ejemplo, *Aplicación_3*), se bloquea el inicio de esa aplicación. Se muestra al usuario una notificación que informa que el inicio de *Application_3* está bloqueado, de acuerdo con una regla de Control de aplicaciones. Puede crear una categoría con contenido añadido automáticamente desde una carpeta específica según varios criterios. En este caso, los archivos se añaden automáticamente a la categoría de la carpeta especificada. Los archivos ejecutables de aplicaciones se copian a la carpeta especificada y se procesan automáticamente. Sus métricas se añaden a la categoría.

Para configurar la administración de ejecución de aplicaciones en los dispositivos cliente:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Categorías de aplicaciones**.

2. En el espacio de trabajo de la carpeta **Categorías de aplicaciones**, cree una categoría de aplicaciones que desee administrar mientras estas se ejecutan.

3. En la carpeta **Dispositivos administrados**, en la ficha **Directivas**, haga clic en el botón **Nueva directiva** para crear una nueva directiva de Kaspersky Endpoint Security para Windows y siga las instrucciones del Asistente.

   Si ya existe esta directiva, puede saltarse este paso. Puede configurar la administración de inicio de aplicaciones en una categoría especificada mediante la configuración de la directiva. La directiva recién creada aparece en la carpeta **Dispositivos administrados**, en la ficha **Directivas**.

4. Seleccione **Propiedades** en el menú contextual de la directiva de Kaspersky Endpoint Security para Windows.

   Se abre la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows.

5. En la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Controles de seguridad** → **Control de aplicaciones**, seleccione la casilla de verificación **Control de aplicaciones**.

6. Haga clic en el botón **Agregar**.

   Se abre la ventana **Regla de control de aplicaciones**.

7. En la ventana **Regla de Control de aplicaciones**, en la lista desplegable **Categoría**, seleccione la categoría de aplicaciones que será cubierta por la regla de ejecución. Configure la regla de inicio para la categoría de

aplicación seleccionada.

Para Kaspersky Endpoint Security 10 Service Pack 2 y posteriores, no se muestran categorías cuyo criterio de creación sea de hash MD5 de un archivo ejecutable.

No es aconsejable añadir categorías creadas según el criterio de hash SHA-256 de un archivo ejecutable para versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2. Esto puede causar fallos de aplicación.

En la Ayuda en línea de Kaspersky Endpoint Security para Windows encontrará instrucciones detalladas sobre la configuración de reglas de control.

8. Haga clic en **Aceptar**.

Las aplicaciones se ejecutarán en los dispositivos incluidos en la categoría especificada, según la regla que haya creado. La regla creada aparece en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Control de aplicaciones**.

Visualización de los resultados del análisis estadístico de reglas de inicio aplicadas a archivos ejecutables

Siga estos pasos para ver información sobre qué archivos ejecutables no pueden ejecutar los usuarios:

1. En la carpeta **Dispositivos administrados** del árbol de consola, seleccione la ficha **Directivas**.
2. Seleccione **Propiedades** en el menú contextual de la directiva de Kaspersky Endpoint Security para Windows.

   Se abre la ventana de propiedades de la directiva de aplicación.
3. En el recuadro **Secciones**, seleccione **Controles de la seguridad** y luego seleccione la subdivisión **Control de aplicaciones**.
4. Haga clic en el botón **Análisis estático**.

   Se abre la ventana **Análisis de la lista de derechos de acceso**. En la parte izquierda de la ventana se muestra una lista de usuarios basada en datos de Active Directory.
5. Seleccione un usuario de la lista.

   La parte derecha de la ventana muestra categorías de aplicaciones asignadas a este usuario.
6. Para ver los archivos ejecutables que el usuario tiene prohibido ejecutar, haga clic en el botón **Ver archivos** de la ventana **Análisis de la lista de derechos de acceso**.

   Se abrirá una ventana que muestra una lista de archivos ejecutables prohibidos.
7. Para ver la lista de archivos ejecutables incluidos en una categoría, seleccione una categoría de aplicaciones y haga clic en el botón **Ver archivos de la categoría**.

   Se abre una ventana que muestra una lista de archivos ejecutables incluidos en la categoría de aplicación.

Visualización del registro de aplicaciones

Kaspersky Security Center realiza un inventario de todo el software instalado en los dispositivos administrados.

El Agente de red elabora una lista de las aplicaciones instaladas en un dispositivo cliente y luego transmite la lista al Servidor de administración. Agente de red recibe automáticamente información acerca de las aplicaciones instaladas desde el registro de Windows.

La recuperación de información sobre las aplicaciones instaladas solo está disponible para dispositivos en los que se ejecuta Microsoft Windows.

Para visualizar el registro de aplicaciones instaladas en los dispositivos cliente,

En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Registro de aplicaciones**.

El espacio de trabajo de la carpeta **Registro de aplicaciones** muestra una lista de aplicaciones instaladas en los dispositivos cliente y el Servidor de administración.

Puede ver los detalles de cualquier aplicación al abrir su menú contextual y al seleccionar **Propiedades**. Se abre una ventana de propiedades de la aplicación en la que se muestran detalles de la aplicación e información sobre sus archivos ejecutables, así como una lista de los dispositivos en los que está instalada la aplicación.

En el menú contextual de cualquier aplicación de la lista puede:

- Añadir esta aplicación a una categoría de aplicación.
- Asignar una etiqueta a la aplicación.
- Exportar la lista de aplicaciones a un archivo CSV o TXT.
- Ver las propiedades de la aplicación, por ejemplo, el nombre del proveedor, número de versión, lista de archivos ejecutables, lista de dispositivos en los que está instalada la aplicación, lista de actualizaciones de software disponibles o la lista de vulnerabilidades de software detectadas.

Para visualizar las aplicaciones que cumplen los criterios especificados, puede utilizar los campos de filtros en el espacio de trabajo de la carpeta **Registro de aplicaciones**.

En la ventana de propiedades del dispositivo seleccionado de la sección **Registro de aplicaciones**, puede ver la lista de aplicaciones instaladas en el dispositivo.

Generación de un informe sobre las aplicaciones instaladas

En el espacio de trabajo **Registro de aplicaciones**, también puede hacer clic en el botón **Ver informe sobre las aplicaciones instaladas** para generar un informe que contenga estadísticas detalladas sobre las aplicaciones instaladas, incluido el número de dispositivos donde está instalada cada aplicación. Este informe, que se abre en la página **Informe sobre aplicaciones instaladas**, contiene información sobre las aplicaciones de Kaspersky y el software de terceros. Si solo desea información sobre las aplicaciones de Kaspersky instaladas en los dispositivos cliente, en la lista **Resumen**, seleccione AO Kaspersky Lab.

La información sobre las aplicaciones de Kaspersky y el software de terceros instalados en los dispositivos conectados a los Servidores de administración secundarios y virtuales también se almacena en el registro de aplicaciones del Servidor de administración principal. Después de añadir datos de los Servidores de administración secundarios y virtuales, haga clic en el botón **Ver informe sobre las aplicaciones instaladas** y en la página **Informe sobre las aplicaciones instaladas** que se abre, puede ver esta información.

Para añadir información de los Servidores de administración secundarios y virtuales al informe sobre las aplicaciones instaladas haga lo siguiente:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. En la pestaña **Informes**, seleccione **Informe sobre las aplicaciones instaladas**.
4. Seleccione **Propiedades** en el menú contextual del informe.

   Se abre la ventana **Propiedades: Informe sobre las aplicaciones instaladas**.
5. En la sección **Jerarquía de Servidores de administración**, seleccione la casilla de verificación **Incluir datos de los Servidores de administración secundarios y virtuales**.
6. Haga clic en **Aceptar**.

La información de los Servidores de administración secundarios y virtuales se incluirá en el **Informe sobre las aplicaciones instaladas**.

Cambiar el tiempo de inicio del inventario de software

Kaspersky Security Center hace un inventario de todo el software instalado en los dispositivos cliente administrados que ejecutan Windows.

El Agente de red elabora una lista de las aplicaciones instaladas en un dispositivo cliente y luego transmite la lista al Servidor de administración. Agente de red recibe automáticamente información acerca de las aplicaciones instaladas desde el registro de Windows.

De manera predeterminada, para ahorrar recursos en el dispositivo cliente, el Agente de red comienza a recibir información acerca de las aplicaciones instaladas 10 minutos después de que se inicia el servicio del Agente de red.

Para modificar el tiempo que transcurre entre que se inicia el servicio del Agente de red y se realiza el inventario de software en un dispositivo:

1. Abra el registro del sistema de un dispositivo cliente en el que está instalado el Agente de red (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).
2. Vaya al siguiente subárbol:

   - Para un sistema de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
   - Para un sistema de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
3. Para la clave KLINV_INV_COLLECTOR_START_DELAY_SEC, configure el valor requerido en segundos.

   El valor predeterminado es 600 segundos.
4. Reinicie el servicio Agente de red.

La hora de inicio del inventario de software, que transcurre después de ejecutarse el servicio Agente de red, se cambiará.

Acerca de la gestión de claves de licencia de aplicaciones de terceros

Kaspersky Security Center le permite realizar un seguimiento del uso de claves de licencias de aplicaciones de terceros instaladas en los dispositivos administrados. La lista de aplicaciones para las que puede realizar un seguimiento del uso de la clave de licencia se obtiene del registro de aplicaciones. Para cada clave de licencia, puede especificar y rastrear las infracciones de las siguientes restricciones:

- Número máximo de dispositivos en los que puede instalarse la aplicación que usa esta clave de licencia.
- Fecha de caducidad de la clave de licencia.

Kaspersky Security Center no comprueba si usted especifica o no una clave de licencia real. Solo puede realizar un seguimiento de las restricciones que especifique. Si se infringe una de las restricciones que ha impuesto a una clave de licencia, el Servidor de administración registra un evento informativo, de advertencia o de fallo operativo.

Las claves de licencia están vinculadas a grupos de aplicaciones. Un grupo de aplicaciones es un grupo de aplicaciones de terceros que usted combina según uno o varios criterios. Puede definir aplicaciones por el nombre de la aplicación, su versión, proveedor y etiqueta. Una aplicación se añade al grupo si se cumple al menos uno de los criterios. Para cada grupo de aplicaciones, puede vincular varias claves de licencia, pero cada clave de licencia puede vincularse a un solo grupo de aplicaciones.

Un instrumento más que puede utilizar para realizar un seguimiento del uso de la clave de licencia es el Informe sobre el estado de los grupos de aplicaciones con licencia. Este informe proporciona información sobre el estado actual de los grupos de aplicaciones con licencia, que incluye:

- El número de instalaciones de claves de licencia en cada grupo de aplicaciones
- El número de claves de licencia en uso y claves de licencia vacantes
- Lista detallada de aplicaciones instaladas en dispositivos administrados

Los instrumentos de gestión de claves de licencia de aplicaciones de terceros se encuentran en la subcarpeta **Uso de licencias de terceros** (**Avanzado → Administración de aplicaciones → Uso de licencias de terceros**). En esta subcarpeta, puede crear grupos de aplicaciones, añadir claves de licencia y generar el Informe sobre los estados de los grupos de aplicaciones con licencia.

Las herramientas para la gestión de claves de licencia de aplicaciones de terceros están disponibles solo si activó la opción Administración de vulnerabilidades y parches en ventana **Configurar interfaz**.

Crear grupos de aplicaciones con licencia

Para crear un grupo de aplicaciones con licencia:

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Uso de licencias de terceros**.
2. Haga clic en el botón **Agregar un grupo de aplicaciones con licencia** para ejecutar Asistente para añadir grupos de programas con licencia.

   Asistente para añadir grupos de programas con licencia se inicia.
3. En el paso **Detalles del grupo de aplicaciones con licencia**, especifique qué aplicaciones desea incluir en el grupo de aplicaciones:

- **Nombre del grupo de aplicaciones con licencia**
- **Realizar el seguimiento de las restricciones incumplidas**

  Si se viola una de las restricciones que haya impuesto a una clave de licencia del grupo de aplicaciones, el Servidor de administración registra un evento informativo, de advertencia o de fallo operativo:

  - Evento informativo: **Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia (ya se ha usado más del 95 %)**
  - Evento de advertencia: **Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia**
  - Evento de fallo operativo: **Se ha superado el límite de instalaciones para uno de los grupos de aplicaciones con licencia**

    Un evento se registra una sola vez, cuando se cumple la condición establecida. La vez siguiente, el mismo evento puede registrarse solo cuando el número de instalaciones regrese a un nivel normal y luego el evento vuelva a ocurrir. Un evento no se puede registrar más de una vez por hora.

- **Criterios para agregar aplicaciones detectadas a este grupo de aplicaciones con licencia**

  Especifique criterios para definir qué aplicaciones desea incluir en el grupo de aplicaciones. Puede definir aplicaciones por el nombre de la aplicación, su versión, proveedor y etiqueta. Debe especificar al menos un criterio. Una aplicación se añade al grupo si se cumple al menos uno de los criterios.

4. En el paso **Introducir datos sobre las claves de licencia existentes**, especifique las claves de licencia que desea rastrear. Seleccione la opción **Controlar si se supera el límite de licencias** y luego agregue las claves de licencia:

   a. Haga clic en el botón **Agregar**.

   b. Seleccione la clave de licencia que desea eliminar y haga clic en el botón **Aceptar**. Si la clave de licencia requerida no aparece en la lista, haga clic en el botón **Agregar** y luego especifique las propiedades de la clave de licencia.

5. En la página **Agregar un grupo de aplicaciones con licencia**, haga clic en el botón **Finalizar**.

Con esto, se habrá creado y se mostrará un grupo de aplicaciones con licencia en la carpeta **Uso de licencias de terceros**.

Administración de claves de licencia para grupos de aplicaciones con licencia

Para crear una clave de licencia para un grupo de aplicaciones con licencia:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Uso de licencias de terceros**.
2. En el espacio de trabajo de la carpeta **Uso de licencias de terceros**, haga clic en el botón **Administrar claves de licencia de aplicaciones con licencia**.

   Se abre la ventana **Administración de claves de licencia en aplicaciones con licencia**.

3. En la ventana **Administración de claves de licencia en aplicaciones con licencia**, haga clic en el botón **Agregar**.

   Se abre la ventana **Clave de licencia**.

4. En la ventana **Clave de licencia**, especifique las propiedades de la clave de licencia y las restricciones que esta impone al grupo de aplicaciones con licencia.

   - **Nombre**. Nombre de la clave de licencia.
   - **Comentario**. Notas en la clave de licencia seleccionada.
   - **Restricción**. Número de dispositivos en los que puede instalarse la aplicación que usa esta clave de licencia.
   - **Caduca el**. Fecha de vencimiento de la clave de licencia.

Las claves de licencia creadas se muestran en la ventana **Administración de claves de licencia en aplicaciones con licencia**.

Para aplicar una clave de licencia a un grupo de aplicaciones con licencia:

1. En la carpeta **Avanzado → Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Uso de licencias de terceros**.
2. En la carpeta **Uso de licencias de terceros**, seleccione el grupo de aplicaciones con licencia al que desee aplicar una clave de licencia.
3. Haga clic en **Propiedades** en el menú contextual del grupo de aplicaciones con licencia.

   Esto abrirá la ventana de propiedades del grupo de aplicaciones con licencia.

4. En la ventana de propiedades del grupo de aplicaciones con licencia, en la sección **Claves de licencia**, seleccione **Controlar si se supera el límite de licencias**.
5. Haga clic en el botón **Agregar**.

   Se abre la ventana **Selección de una clave de licencia**.

6. En la ventana **Selección de una clave de licencia**, seleccione una clave de licencia que desee aplicar a un grupo de aplicaciones con licencia.
7. Haga clic en **Aceptar**.

Las restricciones impuestas a un grupo de aplicaciones autorizado y especificadas en la clave de licencia también se aplicarán al grupo de aplicaciones con licencia seleccionado.

Inventario de archivos ejecutables

Puede utilizar una tarea de inventario para elaborar un inventario de archivos ejecutables en dispositivos cliente. Kaspersky Endpoint Security para Windows proporciona la función de inventario de archivos ejecutables.

El número de archivos ejecutables recibidos de un solo dispositivo no puede ser superior a 150 000. Habiendo alcanzado este límite, Kaspersky Security Center no podrá recibir ningún nuevo archivo.

Antes de comenzar, active las notificaciones sobre el inicio de las aplicaciones en la política de Kaspersky Endpoint Security y la política del Agente de red, de modo que pueda transferir datos al Servidor de administración.

Para habilitar las notificaciones sobre el inicio de aplicaciones:

- Abra la configuración de la política de Kaspersky Endpoint Security y haga lo siguiente:
  1. Vaya a **Configuración general** → **Informes y almacenamiento**.
  2. En la sección **Transferencia de datos al Servidor de administración**, seleccione la casilla **Acerca de las aplicaciones iniciadas**.
  3. Guarde sus cambios.
- Abra la configuración de la política del Agente de red y haga lo siguiente:
  1. Vaya a **Configuración de la aplicación** → **Repositorios**.
  2. Selecciona la casilla de verificación **Detalles de las aplicaciones instaladas**.
  3. Guarde sus cambios.

Para crear una tarea de inventario de archivos ejecutables en dispositivos cliente:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. Haga clic en el botón **Nueva tarea** en el espacio de trabajo de la carpeta **Tareas**.

   Se inicia el Asistente para añadir tareas.
3. En la ventana **Seleccionar el tipo de tarea** del Asistente, seleccione **Kaspersky Endpoint Security** como el tipo de tarea; a continuación, seleccione **Inventario** como subtipo de tarea y haga clic en **Siguiente**.
4. Siga el resto de instrucciones del Asistente.

   Una vez que haya finalizado el Asistente, se crea una tarea de inventario para Kaspersky Endpoint Security. La tarea recién creada se muestra en la lista de tareas en el espacio de trabajo de la carpeta **Tareas**.

En el espacio de trabajo de la carpeta **Archivos ejecutables** se muestra una lista de los archivos ejecutables que se detectaron en los dispositivos durante el inventario.

Durante el inventario, la aplicación detecta archivos ejecutables en los siguientes formatos: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR y archivos HTML.

Visualización de la información acerca de los archivos ejecutables

Realice lo siguiente para ver una lista de todos los archivos ejecutables detectados en dispositivos cliente:

En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Archivos ejecutables**.

El espacio de trabajo de la carpeta **Archivos ejecutables** muestra una lista de archivos ejecutables que se han ejecutado en dispositivos desde la instalación del sistema operativo o que se han detectado mientras se ejecutaba la tarea de inventario de Kaspersky Endpoint Security para Windows.

Puede usar los filtros para ver los datos de los archivos ejecutables que cumplen criterios especificados.

Realice lo siguiente para visualizar las propiedades de un archivo ejecutable:

Seleccione **Propiedades** del menú contextual del archivo.

Se abre una ventana que muestra información sobre el archivo ejecutable y una lista de dispositivos en los que se encuentra el archivo ejecutable.

Supervisión e informes

Esta sección describe las capacidades de supervisión e informes de Kaspersky Security Center. Estas capacidades le brindan una descripción general de su infraestructura, estados de protección y estadísticas.

Después del despliegue de Kaspersky Security Center o durante la operación, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

- **Semáforo**

  La Consola de administración le permite evaluar rápidamente el estado actual de Kaspersky Security Center y los dispositivos administrados al comprobar los semáforos.

- **Estadísticas**

  Las estadísticas sobre el estado del sistema de protección y los dispositivos administrados se muestran en paneles de información que se pueden personalizar.

- **Informes**

  La característica de los informes le permiten obtener información numérica detallada sobre la seguridad de la red de su organización, guardar esta información en un archivo, enviarla por correo electrónico e imprimirla.

- **Eventos**

  Las selecciones de eventos proporcionan una vista en pantalla de los conjuntos de eventos con nombre que se seleccionan desde la base de datos del Servidor de administración. Estos conjuntos de eventos se agrupan según las siguientes categorías:

  - Por nivel de importancia: **Eventos críticos**, **Fallos operativos**, **Advertencias** y **Eventos de información**
  - Por tiempo: **Eventos recientes**
  - Por tipo: **Solicitudes de los usuarios** y **Eventos de auditoría**

Puede crear y ver selecciones de eventos definidos por el usuario según la configuración disponible en la interfaz de Kaspersky Security Center 14 Web Console para configurarlas.

Escenario: seguimiento e informes

Esta sección proporciona un escenario para configurar la función Supervisión e informes en Kaspersky Security Center.

Requisitos previos

Después de desplegar Kaspersky Security Center en la red de una organización, puede comenzar a supervisarlo y generar informes sobre su funcionamiento.

Etapas

El seguimiento y la elaboración de informes en la red de una organización se realizan en etapas:

1. **Configuración del cambio de estado de los dispositivos**

   Conozca los ajustes que definen la asignación de los estados de los dispositivos en función de condiciones específicas. Al cambiar estas configuraciones, puede cambiar la cantidad de eventos con niveles de importancia *Crítica* o *Advertencia*.

   Al configurar el cambio de estado de los dispositivos, asegúrese de que la nueva configuración no entre en conflicto con las directivas de seguridad de la información de su organización y de que pueda reaccionar de manera oportuna a los eventos de seguridad importantes en la red de su organización.

2. **Configuración de notificaciones sobre eventos en dispositivos cliente**

   Configure la notificación (por correo electrónico, SMS o ejecutando un archivo ejecutable) de eventos en dispositivos cliente de acuerdo con las necesidades de su organización.

3. **Cambio de respuesta de su red de seguridad ante el Brote de virus evento**

   Para ajustar la respuesta de la red a los nuevos eventos, puede cambiar los umbrales específicos en las propiedades del Servidor de administración. También puede crear una directiva más estricta que se activará cuando ocurra este evento, o crear una tarea con el mismo fin.

4. **Administrar estadísticas**

   Configurar la visualización de estadísticas de acuerdo con las necesidades de su organización.

5. **Revisión del estado de seguridad de la red de su organización**

   Para revisar el estado de seguridad de la red de su organización, puede realizar cualquiera de las siguientes acciones:

   - En el espacio de trabajo del nodo del **Servidor de administración**, en la pestaña **Estadísticas** abra la pestaña de segundo nivel (página) **Estado de la protección** y revise el panel de información **Estado de protección en tiempo real**
   - Generar y revisar el **Informe del estado de la protección**
   - Generar y revisar el **Informe de errores**

6. **Ubicación de dispositivos cliente que no están protegidos**

   Para localizar dispositivos cliente que no están protegidos, vaya al espacio de trabajo del nodo del **Servidor de administración**, en la pestaña **Estadísticas** abra la pestaña de segundo nivel (página) **Estado de la protección**, y revise el panel de información **Historial de detecciones de dispositivos nuevos en red**. También puede generar y revisar el **Informe del despliegue de la protección**.

7. **Comprobación de protección de dispositivos cliente**

Para comprobar la protección de los dispositivos cliente, vaya al espacio de trabajo del nodo del **Servidor de administración**, en la pestaña **Estadísticas** abra la pestaña de segundo nivel (página) **Despliegue** o **Estadísticas de amenazas** y revise los paneles de información relevantes. También puede iniciar y revisar la selección de eventos **Eventos críticos**.

8. **La evaluación y la limitación del evento se cargan en la base de datos**

   Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se registra en la base de datos del Servidor de administración. Para reducir la carga en el Servidor de administración, evalúe y limite el número máximo de eventos que se pueden almacenar en la base de datos.

   Para evaluar la carga de eventos en la base de datos, calcule el espacio de la base de datos. También puede limitar el número máximo de eventos para evitar el desbordamiento de la base de datos.

9. **Consultar la información de la licencia**

   Para revisar la información de la licencia, vaya al espacio de trabajo del nodo del **Servidor de administración**, en la pestaña **Estadísticas** abra la pestaña de segundo nivel (página) **Despliegue**, y revise el panel de información **Uso de claves de licencia**. También puede generar y revisar el **Informe de uso de claves de licencia**.

Resultados

Al completar el escenario, estará informado sobre la protección de la red de su organización y, por lo tanto, podrá planificar acciones para una mayor protección.

Semáforos en la Consola de administración

La Consola de administración le permite evaluar rápidamente el estado actual de Kaspersky Security Center y los dispositivos administrados al comprobar los semáforos. Los semáforos se muestran en el espacio de trabajo del nodo del **Servidor de administración**, en la ficha **Supervisión**. La ficha proporciona seis paneles de información con semáforos. Un semáforo es una barra vertical de color en el lado izquierdo de un panel. Cada panel con un semáforo equivale a una cobertura funcional específica de Kaspersky Security Center (consulte la tabla a continuación).

Coberturas abarcadas por semáforos en la Consola de administración

Nombre del panel	Cobertura del semáforo
Despliegue	Instalación del Agente de red y aplicaciones de seguridad en dispositivos en una red de la organización
Plan de administración	Estructura de grupos de administración. Análisis de la red. Reglas de movimiento de dispositivos
Configuración de protección	Funcionalidad de la aplicación de seguridad: estado de la protección, análisis antivirus
Actualizar	Actualizaciones y parches
Supervisión	Estado de la protección
Servidor de administración	Funciones y propiedades del Servidor de administración

Cada semáforo puede ser de cualquiera de estos cinco colores (consulte la tabla a continuación). El color del semáforo depende del estado actual de Kaspersky Security Center y de los eventos que se registraron.

Códigos de los colores de los semáforos

Estado	Color del	Significado del color del semáforo

	semáforo	
Informativo	Verde	No se requiere la intervención del administrador.
Advertencia	Amarillo	Se requiere la intervención del administrador.
Crítico	Rojo	Se han detectado graves problemas. Se requiere la intervención del administrador para solucionarlos.
Informativo	Celeste	Se han registrado eventos que no están relacionados con amenazas posibles o reales en la seguridad de dispositivos administrados.
Informativo	Gris	Los detalles de los eventos no están disponibles o todavía no se han recuperado.

El objetivo del administrador es mantener los semáforos en todos los paneles de información en la ficha **Supervisión** en verde.

Trabajo con informes, estadísticas y notificaciones

Esta sección proporciona información acerca de cómo trabajar con informes, estadísticas y selecciones de eventos y dispositivos en Kaspersky Security Center, así como la forma de configurar las notificaciones en el Servidor de administración.

Trabajo con informes

Los informes de Kaspersky Security Center contienen información sobre el estado de los dispositivos administrados. Los informes se generan a partir de la información almacenada en el Servidor de administración. Se pueden generar informes de los siguientes tipos de objetos:

- Para selecciones de dispositivos creadas conforme a una configuración determinada.
- Para grupos de administración.
- Para dispositivos específicos de diferentes grupos de administración.
- Para todos los dispositivos en la red (en el informe de despliegue).

La aplicación tiene una selección de plantillas de informe estándar. También es posible crear plantillas de informe personalizadas. Los informes se muestran en la ventana principal de la aplicación, en la carpeta **Servidor de administración** del árbol de consola.

Crear una plantilla de informes

Para crear una plantilla de informes:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. Haga clic en el botón **Nueva plantilla de informe**.

Se ejecutará el Asistente de nueva plantilla de informe. Siga las instrucciones del Asistente.

Cuando el Asistente finaliza, la plantilla de informe de reciente creación se agregará a la carpeta **Servidor de administración** del árbol de consola. Se puede utilizar esta plantilla para generar y visualizar informes.

Ver y editar las propiedades de la plantilla de informe

Puede ver y editar las propiedades básicas de una plantilla de informe, por ejemplo, el nombre de la plantilla de informe o los campos que se muestran en el informe.

Para ver y editar las propiedades de una plantilla de informe:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. En la lista de plantillas de informe, seleccione la plantilla de informe requerida.
4. Seleccione **Propiedades** del menú contextual de la plantilla del informe seleccionado.

   Como una alternativa, primero puede generar el informe y después hacer clic en el botón **Abrir propiedades de plantillas de informes** o en el botón **Configurar columnas de informe**.
5. En la ventana que se abre, edite las propiedades de la plantilla de informe. Las propiedades de cada informe pueden contener solo algunas de las secciones que se describen a continuación.

   - Sección **General**
     - Nombre de la plantilla de informe
     - **Número máximo de entradas que mostrar**

       Si esta opción está activada, el número de entradas que se muestran en la tabla con datos detallados del informe no excede el valor especificado.

       Las entradas de informe se ordenan primero de acuerdo con las reglas especificadas en la sección **Campos → Campos detallados** de las propiedades de la plantilla de informe y luego solo se conserva la primera de las entradas resultantes. El encabezado de la tabla con datos detallados del informe muestra el número de entradas que se muestra y el número total de entradas disponibles que coinciden con otras configuraciones de la plantilla de informes.

       Si esta opción está desactivada, la tabla con datos detallados del informe muestra todas las entradas disponibles. No le recomendamos que utilice esta opción. La limitación del número de entradas de informe visualizadas reduce la carga en el sistema de administración de bases de datos (DBMS) y reduce el tiempo requerido para generar y exportar el informe. Algunos de los informes contienen demasiadas entradas. Si este es el caso, puede resultarle difícil leerlos y analizarlos todos. Además, su dispositivo puede quedarse sin memoria mientras genera un informe de este tipo, y, por consiguiente, no podrá ver el informe.

       Esta opción está activada de forma predeterminada. El valor predeterminado es 1000.

     - **Versión impresa**

       La salida del informe está optimizada para la impresión: los caracteres de espacio se añaden entre algunos valores para una mejor visibilidad.

       Esta opción está activada de forma predeterminada.

   - Sección **Campos**

Seleccione los campos que se mostrarán en el informe y el orden de estos campos, y configure si cada uno de los campos debe clasificar y filtrar la información en el informe.

- Sección **Intervalo de tiempo**

  Modificar el período del informe. Los valores disponibles son los siguientes:

  - Entre las dos fechas especificadas
  - Desde la fecha especificada hasta la fecha de creación del informe
  - Desde la fecha de creación del informe menos el número especificado de días hasta la fecha de creación del informe

- **Grupo**, sección **Selección de dispositivos** o **Dispositivos**

  Cambie el conjunto de dispositivos cliente para los que se crea el informe. Solo una de estas secciones puede estar presente, dependiendo de la configuración especificada durante la creación de la plantilla del informe.

- Sección **Configuración**

  Cambiar la configuración del informe. El conjunto exacto de ajustes depende del informe específico.

- Sección **Seguridad**

  - Heredar configuración del Servidor de administración

    Si esta opción está activada, la configuración de seguridad del informe se hereda del Servidor de administración.

    Si esta opción está desactivada, puede configurar los ajustes de seguridad para el informe. Puede asignar una función a un usuario o un grupo de usuarios o asignar permisos a un usuario o un grupo de usuarios, según se aplique al informe.

    Esta opción está activada de forma predeterminada.

  La sección **Seguridad** está disponible si se selecciona la casilla de verificación **Mostrar secciones de configuración de seguridad** en la ventana de configuración de la interfaz.

- Sección **Jerarquía de Servidores de administración**

  - Incluir datos de los Servidores de administración secundarios y virtuales

    Si esta opción está activada, el informe incluye la información de los Servidores de administración secundarios y virtuales que están subordinados al Servidor de administración para el cual se crea la plantilla de informe.

    Desactive esta opción si desea ver solo los datos del Servidor de administración actual.

    Esta opción está activada de forma predeterminada.

  - Subir hasta el nivel de anidamiento

El informe incluye datos de los Servidores de administración secundarios y virtuales que se encuentran bajo el Servidor de administración actual en un nivel de anidamiento menor o igual al valor especificado.

El valor predeterminado es 1. Es posible que desee cambiar este valor si tiene que recuperar información de los Servidores de administración secundarios ubicados en los niveles más bajos del árbol.

- Intervalo de espera de datos (min)

  Antes de generar el informe, el Servidor de administración para el que se crea la plantilla de informe espera los datos de los Servidores de administración secundarios durante la cantidad de minutos especificada. Si no se reciben datos de un Servidor de administración secundario al final de este periodo, el informe se ejecuta de todos modos. En lugar de los datos reales, el informe muestra los datos tomados del caché (si la opción **Copiar en caché datos de los Servidores de administración secundarios** está activada) o, por el contrario, **N/A** (no disponible).

  El valor predeterminado es 5 (minutos).

- Copiar en caché datos de los Servidores de administración secundarios

  Los Servidores de administración secundarios transfieren regularmente datos al Servidor de administración para el que se crea la plantilla del informe. Allí, los datos transferidos se almacenan en el caché.

  Si el Servidor de administración actual no puede recibir datos de un Servidor de administración secundario mientras genera el informe, se muestran los datos tomados de la caché en él. También se muestra la fecha en que se transfirieron los datos al caché.

  Habilitar esta opción le permite ver la información de los Servidores de administración secundarios, incluso si no se pueden recuperar los datos actualizados. Sin embargo, los datos mostrados pueden ser obsoletos.

  Esta opción está desactivada de forma predeterminada.

- Frecuencia de actualización de la caché (h)

  Los Servidores de administración secundarios transfieren a intervalos regulares datos al Servidor de administración para el que se crea la plantilla del informe. Puede especificar este periodo en horas. Si especifica 0 horas, los datos se transfieren solo cuando se termina de generar el informe.

  El valor predeterminado es 0.

- Transferir información detallada desde los Servidores de administración secundarios

  En el informe generado, la tabla con datos detallados del informe incluye datos de los Servidores de administración secundarios del Servidor de administración para los cuales se crea la plantilla del informe.

  Habilitar esta opción ralentiza la generación de informes y aumenta el tráfico entre los Servidores de administración. Sin embargo, puede ver todos los datos en un informe.

  En lugar de activar esta opción, es posible que desee analizar datos de informes detallados para detectar un Servidor de administración secundario defectuoso y luego generar el mismo informe solo para ese Servidor de administración defectuoso.

  Esta opción está desactivada de forma predeterminada.

Formato de filtro extendido en plantillas de informes

En Kaspersky Security Center 14, puede aplicar el formato de filtro extendido a una plantilla de informe. El formato de filtro extendido es más flexible que el formato predeterminado. Puede crear condiciones de filtrado complejas mediante un conjunto de filtros, que se aplicarán al informe mediante el operador lógico "O" durante su creación, tal como se muestra a continuación:

Filtro[1](Campo[1] Y Campo[2]... Y Campo[n]) O Filtro[2](Campo[1] Y Campo[2]... Y Campo[n]) O... Filtro[n] (Campo[1] Y Campo[2]... Y Campo[n])

Además, con el formato de filtro extendido, puede establecer un valor para el intervalo de tiempo en un formato de tiempo relativo (por ejemplo, con una condición del tipo "Para los últimos N días") para campos específicos en un filtro. La disponibilidad y los tipos de condiciones de intervalos de tiempo dependen del tipo de plantilla de informe.

Conversión del filtro al formato extendido

El formato de filtro extendido para las plantillas de informes solo es compatible con Kaspersky Security Center 12 y versiones posteriores. Después de convertir el filtro predeterminado al formato extendido, la plantilla de informe deja de ser compatible con los Servidores de administración de su red que tienen instaladas versiones anteriores de Kaspersky Security Center. La información de estos Servidores de administración no se tomará en cuenta para el informe.

Para convertir el filtro predeterminado de la plantilla de informe al formato extendido, haga lo siguiente:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. En la lista de plantillas de informe, seleccione la plantilla de informe requerida.
4. Seleccione **Propiedades** del menú contextual de la plantilla del informe seleccionado.
5. En la ventana de propiedades que se abre, seleccione la sección **Campos**.
6. En la ficha **Campos detallados**, haga clic en el enlace **Convertir filtro**.
7. En la ventana que se abre, haga clic en el botón **Aceptar**.

   La conversión al formato de filtro extendido es irreversible para la plantilla de informe a la que se aplica. Si hizo clic accidentalmente en el enlace **Convertir filtro**, puede hacer clic en el botón **Cancelar** de la ventana de propiedades de la plantilla de informe para cancelar los cambios.

8. Para aplicar los cambios, haga clic en el botón **Aceptar** para cerrar la ventana de propiedades de la plantilla de informe.

   Cuando se abre nuevamente la ventana de propiedades de la plantilla de informe, se muestra la nueva sección de **Filtros** disponibles. En esta sección puede configurar el filtro extendido.

Configuración del filtro extendido

Para configurar el filtro extendido en las propiedades de la plantilla de informe, haga lo siguiente:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. En la lista de plantillas de informes, seleccione la plantilla de informe que se había convertido al formato de filtro extendido.
4. Seleccione **Propiedades** del menú contextual de la plantilla del informe seleccionado.
5. En la ventana de propiedades que se abre, seleccione la sección **Filtros**.

   La sección **Filtros** no se muestra si la plantilla del informe no se ha convertido previamente al formato de filtro extendido.

   En la sección **Filtros** de la ventana de propiedades de la plantilla de informe, puede revisar y modificar la lista de filtros que se aplican al informe. Cada filtro de la lista tiene un nombre único y representa un conjunto de filtros para los campos correspondientes del informe.
6. Abra la ventana de configuración de filtros de alguna de las siguientes formas:
   - Para crear un filtro nuevo, haga clic en el botón **Agregar**.
   - Para modificar el filtro actual, seleccione el filtro requerido y haga clic en el botón **Modificar**.
7. En la ventana que se abre, seleccione y especifique los valores de los campos obligatorios del filtro.
8. Haga clic en el botón **Aceptar** para guardar los cambios y cerrar la ventana.

   Si está creando un filtro nuevo, el nombre del filtro se debe especificar en el campo **Nombre de filtro** antes de hacer clic en el botón **Aceptar**.
9. Para cerrar la ventana de propiedades de la plantilla de informe, haga clic en el botón **Aceptar**.

   El filtro extendido en la plantilla de informe está configurado. Ahora puede crear informes con esta plantilla de informe.

Creación y visualización de un informe

Para crear y visualizar un informe:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. En la lista de plantillas del informe, haga doble clic en la plantilla del informe que necesite.

   Se mostrará un informe para la plantilla seleccionada.

El informe muestra los siguientes datos:

- El nombre y tipo de informe, una descripción breve del mismo y el periodo cubierto, así como información sobre el grupo de dispositivos para el que se generará el informe.
- Gráfico que muestra los datos más representativos del informe.
- Tabla consolidada con indicadores de informe calculados.
- Tabla con datos del informe detallados.

Guardar informe

Para guardar un informe generado:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. En la lista de plantillas del informe, seleccione la plantilla del informe que necesite.
4. Seleccione **Guardar** del menú contextual de la plantilla del informe seleccionado.

   Se iniciará el Asistente para guardar el informe. Siga las instrucciones del Asistente.

Una vez finalizado el Asistente, se abrirá la carpeta en la que ha guardado el archivo de informe.

Crear una tarea de entrega de informes

Los informes se pueden enviar por correo electrónico. La entrega de informes en Kaspersky Security Center se realiza mediante la tarea de entrega del informe.

Para crear una tarea de entrega para un único informe:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Informes**.
3. En la lista de plantillas del informe, seleccione la plantilla del informe que necesite.
4. Seleccione **Entregar informes** del menú contextual de la plantilla del informe seleccionado.

   Se inicia el Asistente para crear tareas de entrega de informes. Siga las instrucciones del Asistente.

Para crear una tarea de entrega para múltiple informes:

1. En el árbol de consola, en el nodo con el nombre del Servidor de administración requerido, seleccione la carpeta **Tareas**.
2. En el espacio de trabajo de la carpeta **Tareas**, haga clic en el botón **Crear una tarea**.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

   La tarea de entrega de informes recién creada se muestra en la carpeta **Tareas** del árbol de consola.

La tarea de entrega del informe se crea automáticamente si los parámetros de correo electrónico se especificaron durante la instalación de Kaspersky Security Center.

Paso 1. Selección del tipo de tarea

En la ventana **Seleccionar el tipo de tarea**, en la lista de tareas seleccione **Entregar informes** como el tipo de tarea.

Haga clic **Siguiente** para ir al paso siguiente.

Paso 2. Selección del tipo del informe

En la ventana **Seleccionar tipo de informe**, en la lista de plantillas de creación de tareas, seleccione el tipo de informe.

Haga clic **Siguiente** para ir al paso siguiente.

Paso 3. Acciones con un informe

En la ventana **Acción para aplicar a los informes**, especifique la siguiente configuración:

- Enviar informes por correo electrónico

  Si esta opción está activada, la aplicación envía los informes generados por correo electrónico.

  Al hacer clic en el enlace **Configuración de notificaciones por correo** se configura el envío del informe por correo electrónico. El enlace está disponible si esta opción está activada.

  Si esta opción está desactivada, la aplicación guarda los informes en la carpeta especificada para almacenarlos.

  Esta opción está desactivada de forma predeterminada.

- Guardar informes en una carpeta compartida

  Si esta opción está activada, la aplicación guarda informes en la carpeta, especificada en el campo que hay debajo de la casilla de verificación. Para guardar informes en una carpeta compartida, especifique la ruta de UNC a la carpeta. En este caso, en la ventana **Seleccionar una cuenta para ejecutar la tarea**, debe especificar la cuenta de usuario y contraseña para acceder a esta carpeta.

  Si esta opción está desactivada, la aplicación no guarda los informes en la carpeta y los envía por correo electrónico.

  Esta opción está desactivada de forma predeterminada.

- Sobrescribir informes antiguos del mismo tipo

  Si esta opción está activada, el nuevo archivo de informe en cada inicio de tarea sobrescribirá el archivo guardado en la carpeta de informes en el inicio de tarea anterior.

  Si esta opción está desactivada, los archivos de informe no se sobrescribirán. Se guarda un nuevo archivo de informe en la carpeta de informes en cada inicio de tarea.

  Esta casilla de verificación está disponible si se ha seleccionado **Guardar informe en una carpeta**.

  Esta opción está desactivada de forma predeterminada.

- Especificar cuenta para el acceso a la carpeta compartida

Si esta opción está activada, puede especificar la cuenta con la que se guardará el informe en la carpeta. Si una ruta de UNC a una carpeta compartida se especifica como configuración **Guardar informe en una carpeta** en la ventana **Acción para aplicar al informe**, debe especificar la cuenta de usuario y la contraseña para acceder a esta carpeta.

Si esta opción está desactivada, el informe se guarda en la carpeta en la cuenta del Servidor de administración.

La casilla de verificación está disponible si se ha seleccionado **Guardar informe en una carpeta**.

Esta opción está desactivada de forma predeterminada.

Haga clic **Siguiente** para ir al paso siguiente.

Paso 4. Selección de una cuenta para iniciar la tarea

En la ventana **Seleccionar una cuenta para ejecutar la tarea**, puede especificar qué cuenta utilizar al ejecutar la tarea. Seleccione una de las siguientes opciones:

- **Cuenta preconfigurada**

  La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

  - **Cuenta**

    Cuenta bajo la que se ejecuta la tarea.

  - **Contraseña**

    La contraseña de la cuenta bajo la cual la tarea se ejecutará.

Haga clic **Siguiente** para ir al paso siguiente.

Paso 5. Configuración de la planificación de una tarea

En la página **Configurar programación de tareas** del Asistente, puede crear una planificación para el inicio de la tarea. Si es necesario, defina la siguiente configuración:

- **Inicio programado:**

  Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

  - **Cada N horas**

La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

- Cada N días

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

- Cada N semanas

  La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

  De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- Cada N minutos

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- Diario (no compatible con horario de verano)

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- Semanalmente

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- Por días de la semana

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- Mensualmente

La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

En los meses que faltan el día especificado, la tarea se ejecuta el último día.

De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Al detectar un foco de virus**

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

Esta opción está activada de forma predeterminada.

- **Usar un retraso aleatorio automático para el inicio de las tareas**

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

Paso 6. Definición del nombre de la tarea

En la ventana **Especifique el nombre de la tarea**, especifique el nombre de la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como `"*<>-_?:\"|`).

Haga clic **Siguiente** para ir al paso siguiente.

Paso 7. Finalización de la creación de la tarea

En la ventana **Finalizar la creación de tareas**, haga clic en el botón **Finalizar** para cerrar el Asistente.

Si desea que la tarea comience tan pronto como finalice Asistente, seleccione la casilla **Ejecutar tarea después de que finalice el Asistente**.

Administrar estadísticas

Las estadísticas sobre el estado del sistema de protección y los dispositivos administrados se muestran en paneles de información que se pueden personalizar. En el espacio de trabajo del nodo **Servidor de administración**, en la ficha **Estadísticas**, se muestran estadísticas. La ficha contiene una serie de fichas de nivel secundario (páginas). Cada página con fichas muestra paneles de información con estadísticas, así como enlaces a noticias corporativas y otros materiales desde Kaspersky. La información estadística se muestra en los paneles de información en forma de tabla o de gráfico (circular o de barras). Los datos en los paneles de información se actualizan mientras se ejecuta la aplicación, y reflejan el estado actual del sistema de protección antivirus.

Se puede modificar el conjunto de fichas de segundo nivel en la ficha **Estadísticas**, el número de paneles de información por página con fichas y el modo de mostrar los datos en los paneles de información.

*Para agregar una ficha de segundo nivel con paneles de información en la ficha **Estadísticas**:*

1. Haga clic en el botón **Personalizar vista** Ver en la esquina superior derecha de la ficha **Estadísticas**.

   Se abre la ventana de propiedades de estadísticas. Dicha ventana contiene una lista de las páginas que se muestran en la ficha **Estadísticas**. En esta ventana, puede cambiar el orden de visualización de las páginas en la ficha, agregar y quitar páginas, y acceder a la configuración de las propiedades de las páginas haciendo clic en el botón **Propiedades**.

2. Haga clic en el botón **Agregar**.

   De esta forma se abre la ventana de propiedades de una página nueva.

3. Configure la página de nueva:

   - En la sección **General**, especifique el nombre de la página.

   - En la sección **Paneles de información**, haga clic en el botón **Agregar** para agregar los paneles de información que se deben mostrar en la página.

     Haga clic en el botón **Propiedades** de la sección **Paneles de información** para configurar las propiedades de los paneles de información que ha agregado: el nombre, el tipo y el aspecto del gráfico en el panel, así como los datos que se utilizan para generar el gráfico.

4. Haga clic en **Aceptar**.

La página con fichas con paneles de información que ha agregado se muestra en la ficha **Estadísticas**. Haga clic en el icono de **Configuración** (⚙) para ir al instante a la configuración de la página o a un panel de información seleccionado en esa página.

Configuración de notificación de eventos

Kaspersky Security Center le permite seleccionar un método para notificar al administrador los eventos que tienen lugar en los dispositivos cliente, así como configurar la notificación:

- Correo electrónico. Cuando se produce un evento, la aplicación envía una notificación a las direcciones de correo electrónico especificadas. Puede editar el texto de la notificación.

- SMS. Cuando se produce un evento, la aplicación envía una notificación a los números de teléfono especificados. Puede configurar las notificaciones por SMS para que se envíen a través de la puerta de enlace

de correo.

- Archivo ejecutable. Cuando se produce un evento en un dispositivo, el archivo ejecutable se inicia en la estación de trabajo del administrador. Mediante el archivo ejecutable, el administrador puede recibir los parámetros de cualquier evento ocurrido.

Para configurar las notificaciones de los eventos sucedidos en los dispositivos cliente:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. Haga clic en el enlace **Configurar las notificaciones y la exportación de eventos** y seleccione el valor **Configurar notificaciones** en la lista desplegable.

   De este modo, se abre la ventana **Propiedades: Eventos**.
4. En la sección **Notificación**, seleccione un método de notificación (por correo electrónico, SMS o un archivo ejecutable) y defina la configuración de la notificación:

   - Correo electrónico

La ficha **Correo electrónico** le permite configurar las notificaciones de correo electrónico para eventos.

En el campo **Destinatarios (correo electrónico)**, especifique las direcciones de correo electrónico a las cuales la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolos con punto y coma. Puede usar los siguientes valores:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

Si activa la opción **Buscar registros MX por DNS**, puede utilizar varios registros MX de las direcciones IP para el mismo nombre DNS del servidor SMTP. El mismo nombre DNS puede tener varios registros MX con diferentes valores de prioridad de recepción de mensajes de correo electrónico. El Servidor de administración intenta enviar notificaciones del correo electrónico al servidor SMTP en orden ascendente de prioridad de registros MX. Esta opción está desactivada de forma predeterminada.

Si activa la opción **Buscar registros MX por DNS** y no activa el uso de la configuración de TLS, le recomendamos que use la configuración de DNSSEC en el dispositivo de su servidor como medida adicional de protección para el envío de notificaciones del correo electrónico.

Haga clic en el enlace **Configuración** para definir ajustes de notificación adicionales:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de autenticación ESMTP

Debe especificar una cuenta para la autenticación en un servidor SMTP si la opción de autenticación ESMTP está activada para el servidor SMTP.

- Configuración de TLS para el servidor SMTP:
  - **Do not use TLS**

    Puede seleccionar esta opción si desea desactivar el cifrado de mensajes de correo electrónico.
  - **Use TLS if supported by SMTP server**

    Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.
  - **Always use TLS, check the server certificate for validity**

    Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse con el servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si elige el valor **Always use TLS, check the server certificate for validity**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

Puede especificar la configuración de TLS para un servidor SMTP:

- Busque un archivo de certificado para el servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo en el Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

- Busque un archivo de certificado para el cliente:

Puede utilizar un certificado que haya recibido de cualquier fuente, por ejemplo, de cualquier autoridad de certificación confiable. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Ambos archivos no dependen el uno del otro y, por ende, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

- Contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y su clave privada. Cuando se cargue el archivo, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

El campo **Mensaje de notificación** contiene el texto estándar con información sobre el evento que la aplicación envía cuando un evento ocurre. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje añadiendo otros parámetros sustitutos con detalles más relevantes del evento. La lista de parámetros sustitutos está disponible haciendo clic en el botón a la derecha del campo.

Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que escribir dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

Haga clic en el enlace **Configurar límite numérico de notificaciones**, para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en el botón **Enviar mensaje de prueba** para verificar si ha configurado las notificaciones correctamente. La aplicación debería enviar una notificación de prueba a las direcciones de correo electrónico que ha especificado.

- SMS

La ficha **SMS** le permite configurar la transmisión de notificaciones por SMS de varios eventos a un teléfono celular. Los mensajes SMS se enviarán a través de una puerta de enlace de correo.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las cuales la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma. Las notificaciones se transmitirán a los números de teléfono asociados con las direcciones de correo electrónico especificadas.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolos con punto y coma. Puede usar los siguientes valores:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

Haga clic en el enlace **Configuración** para definir ajustes de notificación adicionales:

- Nombre del sujeto (nombre del sujeto de un mensaje de correo electrónico)
- Dirección de correo electrónico del remitente
- Configuración de autenticación ESMTP

En caso de ser necesario, puede especificar una cuenta para la autenticación en un servidor SMTP si la opción de autenticación ESMTP está activada para el servidor SMTP.

- Configuración de TLS para un servidor SMTP

Puede desactivar el uso de TLS, usar TLS si el servidor SMTP admite este protocolo o forzar el uso de TLS únicamente. Si elige usar solo TLS, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, si elige usar solo TLS, puede especificar un certificado para la autenticación de clientes en el servidor SMTP.

- Busque un archivo de certificado para el servidor SMTP

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo en Kaspersky Security Center. Kaspersky Security Center verifica si el certificado del servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado del servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

Debe cargar un solo archivo que contenga el certificado y su clave privada. Cuando se cargue el archivo, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede estar vacía si la clave privada no está cifrada. El campo **Mensaje de notificación** contiene el texto estándar con información sobre el evento que la aplicación envía cuando un evento ocurre. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje añadiendo otros parámetros sustitutos con detalles más relevantes del evento. La lista de parámetros sustitutos está disponible haciendo clic en el botón a la derecha del campo.

Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que escribir dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

Haga clic en el enlace **Configurar límite numérico de notificaciones** para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en el botón **Enviar mensaje de prueba** para comprobar si ha configurado correctamente las notificaciones. La aplicación debería enviar una notificación de prueba al destinatario que ha especificado.

- Archivo ejecutable para lanzar

  Si se selecciona este método de notificación, en el campo de entrada puede especificar la aplicación que se iniciará cuando ocurra un evento.

  Al hacer clic en el enlace **Configurar límite numérico de notificaciones**, puede especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

  Al hacer clic en el botón **Enviar mensaje de prueba** le permite verificar si ha configurado las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que ha especificado.

5. En el campo **Mensaje de notificación**, introduzca el texto que la aplicación enviará cuando se produzca un evento.

   Puede usar la lista desplegable a la derecha del campo del texto para agregar los parámetros de sustitución con detalles del evento (por ejemplo, la descripción del evento o la hora en que ocurrió).

   Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que especificar dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

6. Haga clic en el botón **Enviar mensaje de prueba** para comprobar si la notificación se ha configurado correctamente.

   La aplicación envía una notificación de prueba al usuario especificado.

7. Haga clic en **Aceptar** para guardar los cambios.

Los parámetros reajustados de la notificación se aplicarán a todos los eventos que tengan lugar en los dispositivos cliente.

Puede anular la configuración de notificación para ciertos eventos en la sección **Configuración de eventos** de la Configuración del Servidor de administración, de una configuración de directiva o de una configuración de aplicación.

Creación de un certificado para un servidor SMTP

Para crear un certificado para un servidor SMTP:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. Haga clic en el enlace **Configurar las notificaciones y la exportación de eventos** y seleccione el valor **Configurar notificaciones** en la lista desplegable.

   Se abre la ventana Propiedades del evento.

4. En la ficha **Correo electrónico**, haga clic en el enlace **Configuración** para abrir la ventana **Configuración**.
5. En la ventana **Configuración**, haga clic en el enlace **Especificar certificado** para abrir la ventana **Certificado para firmar**.
6. En la ventana **Certificado para firmar**, haga clic en el botón **Examinar**.

Se abre la ventana **Certificado**.

7. En la lista desplegable **Tipo de certificado**, especifique el tipo de certificado (público o privado):

   - Si se ha seleccionado el tipo privado de certificado (**Contenedor PKCS #12**), especifique el archivo de certificado y la contraseña.
   - Si se ha seleccionado el tipo público de certificado (**Certificado X.509**):

     a. Especifique el archivo clave privado (tiene la extensión *.prk o *.pem).

     b. Especifique la contraseña de la clave privada.

     c. Especifique el archivo clave público (tiene la extensión *.cer).

8. Haga clic en **Aceptar**.

Se emite el certificado para el servidor SMTP.

Selecciones de eventos

La información sobre eventos en el funcionamiento de Kaspersky Security Center y las aplicaciones administradas se guarda tanto en el registro del sistema de Microsoft Windows como en la base de datos del Servidor de administración. Puede ver información de la base de datos del Servidor de administración en el espacio de trabajo del nodo **Servidor de administración**, en la ficha **Eventos**.

La información de la ficha **Eventos** se representa como una lista de selecciones de eventos. Cada selección incluye eventos únicamente de un determinado tipo. Por ejemplo, la selección "El estado del dispositivo es crítico" contiene solamente registros sobre los cambios de estados del dispositivo a "Crítico". Después de instalar la aplicación, la ficha **Eventos** contiene unas cuantas selecciones de eventos estándar. Se pueden crear selecciones adicionales (personalizadas) de eventos o exportar la información de los eventos a un archivo.

Visualización una selección de eventos

Para visualizar una selección de eventos:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. En la lista desplegable **Selecciones de eventos**, elija la correspondiente selección de eventos.

   Si desea que los eventos de esta selección se muestren de forma permanente en el espacio de trabajo, haga clic en el botón ☆ junto a la selección.

   El espacio de trabajo mostrará una lista de eventos del tipo seleccionado, almacenados en el Servidor de administración.

Puede clasificar la información en la lista de eventos en orden ascendente o descendente en cualquier columna.

Personalización de una selección de eventos

Para personalizar una selección de eventos:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. Abra la selección de eventos requerida en la ficha **Eventos**.
4. Haga clic en el botón **Propiedades de la selección**.

En la ventana de propiedades de la selección de eventos que se abrirá, puede configurar la selección de eventos.

Creación de una selección de eventos

Para crear una selección de eventos:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. Haga clic en el botón **Crear una selección**.
4. En la ventana **Nueva selección de eventos** que se abrirá, introduzca el nombre de la nueva selección y haga clic en **Aceptar**.

En la lista desplegable **Selecciones de eventos** se crea una selección con el nombre que haya especificado.

De forma predeterminada, cuando se crea una selección de eventos, esta contiene todos los eventos almacenados en el Servidor de administración. Para hacer que una selección solo muestre los eventos que desea, debe personalizar la selección.

Exportación de una selección de eventos a un archivo de texto

Para exportar una selección de eventos a un archivo de texto:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. Haga clic en el botón **Importar/Exportar**.
4. En la lista desplegable, seleccione **Exportar eventos a archivo**.

Se inicia el Asistente de exportación de eventos. Siga las instrucciones del Asistente.

Eliminación de eventos de una selección

Para eliminar eventos de una selección:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración relevante.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. Seleccione los eventos que quiere eliminar con el ratón, la tecla **Mayús** o la tecla **Ctrl**.
4. Elimine los eventos seleccionados por alguno de los medios siguientes:
   - Seleccione **Eliminar** en el menú contextual de cualquiera de los eventos seleccionados.

     Si selecciona en el menú contextual el elemento **Borrar todo**, se quitarán todos los eventos mostrados de la selección, sin tener en cuenta qué eventos seleccionó para eliminar.
   - Haga clic en el enlace **Eliminar evento** si ha seleccionado un único evento o en el enlace **Eliminar eventos** en el cuadro de información de esos eventos.

Los eventos seleccionados se eliminan.

Adición de aplicaciones a exclusiones por solicitud de usuario

Cuando recibe solicitudes de usuarios para desbloquear aplicaciones bloqueadas erróneamente, puede crear una exclusión de las reglas de seguridad adaptativa para estas aplicaciones. En consecuencia, las aplicaciones ya no serán bloqueadas en los dispositivos de los usuarios. Puede hacer un seguimiento del número de solicitudes de usuarios en la ficha **Supervisión** del Servidor de administración.

Para añadir aplicaciones bloqueadas por Kaspersky Endpoint Security a exclusiones por solicitudes de usuarios:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el espacio de trabajo del nodo, abra la ficha **Eventos**.
3. En la lista desplegable **Selecciones de eventos**, seleccione **Solicitudes de los usuarios**.
4. Haga clic con el botón derecho en la solicitud del usuario (o en varias solicitudes del usuario) que contiene las aplicaciones que desea añadir a las exclusiones y luego seleccione **Agregar exclusión**.

   Esto inicia el Asistente para Añadir exclusiones. Siga sus instrucciones.

Las aplicaciones seleccionadas se excluirán de la **Activación de reglas en el estado Aprendizaje inteligente** (en **Repositorios** en el árbol de la consola) después de la próxima sincronización del dispositivo cliente con el Servidor de administración, y ya no aparecerá en la lista.

Selecciones de dispositivos

La información sobre el estado de los dispositivos se muestra en la carpeta **Selecciones de dispositivos** del árbol de consola.

La información en la carpeta **Selecciones de dispositivos** se muestra como una lista de selecciones de dispositivos. Cada selección contiene dispositivos que cumplen condiciones específicas. Por ejemplo, los **Dispositivos con el estado Crítico** solo contiene dispositivos con el estado *Crítico*. Después de instalar la aplicación, la carpeta **Selecciones de dispositivos** contiene unas cuantas selecciones estándar. Se pueden crear selecciones de dispositivos adicionales (personalizadas), exportar los parámetros de selección a un archivo o crear selecciones con parámetros importados desde otro archivo.

Visualización de una selección de dispositivos

Para ver una selección de dispositivos:

1. En el árbol de consola, seleccione la carpeta **Selecciones de dispositivos**.
2. En el espacio de trabajo de la carpeta, en la lista **Dispositivos en esta selección** escoja la selección de dispositivos relevante.
3. Haga clic en el botón **Ejecutar selección**.
4. Haga clic en la pestaña **Resultados de la selección**.

El espacio de trabajo mostrará la lista de dispositivos que cumplen los criterios de selección.

Puede clasificar la información en la lista de dispositivos en orden ascendente o descendente en cualquier columna.

Configuración de una selección de dispositivos

Para configurar una selección de dispositivos:

1. En el árbol de consola, seleccione la carpeta **Selecciones de dispositivos**.
2. En el espacio de trabajo, haga clic en la ficha **Selección** y luego haga clic en la selección de dispositivos relevante en la lista de selecciones de usuarios.
3. Haga clic en el botón **Propiedades de la selección**.
4. En la ventana de propiedades que se abre, especifique la siguiente configuración:
   - Propiedades de selección generales.
   - Las condiciones que se deben cumplir para dispositivos incluidos en esta selección. Puede configurar las condiciones después de seleccionar un nombre de condición y hacer clic en el botón **Propiedades**.
   - Configuración de seguridad.
5. Haga clic en **Aceptar**.

   La configuración se aplica y se guarda.

A continuación, aparecen descripciones de las condiciones para asignar dispositivos a una selección. Las condiciones se combinan con el operador lógico OR. En la selección estarán los dispositivos que cumplan al menos una de las condiciones enumeradas.

General

En la sección **General**, puede cambiar el nombre de una condición de la selección y especificar si esa condición se debería invertir:

Revertir condición de la selección

Si esta opción está activada, la condición de selección especificada se invertirá. La selección incluirá todos los dispositivos que no cumplen la condición.

Esta opción está desactivada de forma predeterminada.

Red

En la sección **Red**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según sus datos de la red:

- **Nombre o dirección IP del dispositivo**

  Nombre del dispositivo en la red Windows (nombre de NetBIOS).

- **Dominio de Windows**

  Muestra todos los dispositivos incluidos en el dominio de Windows especificado.

- **Grupo de administración**

  Muestra los dispositivos incluidos en el grupo de administración especificado.

- **Descripción**

Texto de la ventana de propiedades del dispositivo: en el campo **Descripción** de la sección **General**.

Para describir texto en el campo **Descripción**, se pueden utilizar los siguientes caracteres:

- Dentro de una palabra:
  - *****. Sustituye cualquier cadena con cualquier número de caracteres.

    Ejemplo:

    Para describir las palabras como **Servidor** o **Servidores** puedes escribir **Servidor***.
  - **?.** Sustituye cualquier carácter individual.

    Ejemplo:

    Para describir palabras como **Window** o **Windows**, puedes escribir **Windo?**.

    El asterisco (*****) o signo de interrogación (**?**) no se puede utilizar como el primer carácter de la pregunta.
- Para encontrar varias palabras:
  - Espacio. Muestra todos los dispositivos cuyas descripciones contienen alguna de las palabras de la lista.

    Ejemplo:

    Para buscar una frase que incluya las palabras **secundario** o **virtual**, en la consulta puede incluir la línea **secundario virtual**.
  - **+**. Cuando se introduce el signo más delante de una palabra, todos los resultados de la búsqueda incluirán esa palabra.

    Ejemplo:

    Para encontrar una frase que contenga tanto **secundario** como **virtual**, introduzca la consulta **+secundario+virtual**.
  - **-**. Cuando se introduce el signo menos delante de una palabra, ningún resultado de la búsqueda incluirá esa palabra.

    Ejemplo:

    Para encontrar una frase que tenga la palabra **secundario**, pero no la palabra **virtual**, introduzca la consulta **+secundario-virtual**.
  - **"<algún texto>"**. El texto escrito entre comillas debe formar parte del texto.

    Ejemplo:

    Para encontrar una frase que contenga la combinación de palabras **Servidor secundario**, introduzca **"Servidor secundario"** en la consulta.

- Rango IP

  Si esta opción está activada, se pueden introducir las direcciones IP inicial y final del rango IP en el que se incluirán los dispositivos pertinentes.

  Esta opción está desactivada de forma predeterminada.

Etiquetas

En la sección **Etiquetas**, puede configurar criterios para incluir dispositivos en una selección según palabras clave (etiquetas) que se añadieron anteriormente a las descripciones de dispositivos administrados:

- **Aplicar si coincide al menos una etiqueta especificada**

  Si esta opción está activada, los resultados de las búsquedas mostrarán dispositivos cuyas descripciones contengan al menos una de las etiquetas seleccionadas.

  Si esta opción está desactivada, los resultados de la búsqueda solo mostrarán dispositivos con descripciones que contengan todas las etiquetas seleccionadas.

  Esta opción está desactivada de forma predeterminada.

- **La etiqueta debe incluirse**

  Si se selecciona esta opción, los resultados de búsqueda mostrarán los dispositivos cuyas descripciones contienen la etiqueta seleccionada. Para buscar dispositivos, puede usar el asterisco, que significa cualquier cadena con cualquier número de caracteres.

  Esta opción está seleccionada de forma predeterminada.

- **La etiqueta debe excluirse**

  Si esta opción se selecciona, los resultados de búsqueda mostrarán los dispositivos cuyas descripciones no contienen la etiqueta seleccionada. Para buscar dispositivos, puede usar el asterisco, que significa cualquier cadena con cualquier número de caracteres.

Active Directory

En la sección **Active Directory**, puede configurar criterios para incluir dispositivos en una selección según sus datos de Active Directory:

- **El dispositivo está en una unidad organizativa de Active Directory**

  Si esta opción está activada, la selección incluye dispositivos de la unidad de Active Directory especificada en el campo de entrada.

  Esta opción está desactivada de forma predeterminada.

- **Incluir unidades organizativas secundarias**

  Si esta opción está activada, la selección incluye dispositivos de todas las unidades organizativas (OU) secundarias de la unidad organizativa de Active Directory especificada.

  Esta opción está desactivada de forma predeterminada.

- **Este dispositivo pertenece al grupo de Active Directory**

Si esta opción está activada, la selección incluye dispositivos del grupo de Active Directory especificado en el campo de entrada.

Esta opción está desactivada de forma predeterminada.

Actividad de red

En la sección **Actividad de red**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según su actividad de red:

- Este dispositivo es un punto de distribución

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La selección incluirá dispositivos que funcionan como puntos de distribución.
  - **No**. Los dispositivos que funcionan como puntos de distribución no se incluirán en la selección.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- No desconectar del Servidor de administración

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Activado**. La selección incluirá dispositivos en los que la casilla de verificación **No desconectar del Servidor de administración** está seleccionada.
  - **Desactivado**. La selección incluirá dispositivos en los que la casilla de verificación **No desconectar del Servidor de administración** no está seleccionada.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Perfil de conexión cambiado

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La selección incluirá dispositivos que se conectaron al Servidor de administración después del cambio del perfil de conexión.
  - **No**. La selección no incluirá dispositivos que se conectaron al Servidor de administración después del cambio del perfil de conexión.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Última conexión al Servidor de administración

Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos en función de la hora de la última conexión al Servidor de administración.

Si se activa esta casilla de verificación, en el campo de entrada se puede especificar el intervalo de tiempo (fecha y hora) durante el que se produjo la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá los dispositivos que se encuentren dentro del intervalo especificado.

No se aplica el criterio si esta casilla está vacía.

De forma predeterminada, esta casilla está en blanco.

- **El sondeo de la red ha detectado dispositivos nuevos**

  Busca los nuevos dispositivos que se han detectado mediante el sondeo de la red hace pocos días.

  Si esta opción está activada, la selección incluirá solamente los nuevos dispositivos que se hayan detectado mediante la detección de dispositivos durante el número de días especificados en el campo **Periodo de detección (días)**.

  Si esta opción está desactivada, la selección incluye todos los dispositivos que han sido detectados por detección de dispositivos.

  Esta opción está desactivada de forma predeterminada.

- **El dispositivo es visible**

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La aplicación incluye en la selección los dispositivos actualmente visibles en la red.
  - **No**. La aplicación incluye en la selección los dispositivos actualmente invisibles en la red.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

Aplicación

En la sección **Aplicación**, puede configurar criterios para incluir dispositivos en una selección según la aplicación administrada seleccionada:

- **Nombre de la aplicación**

  En la lista desplegable, puede establecer un criterio para incluir los dispositivos en una selección al realizar búsquedas por el nombre de una aplicación Kaspersky.

  La lista proporciona únicamente los nombres de las aplicaciones con los complementos de administración instalados en la estación de trabajo del administrador.

  No se aplica el criterio si no se selecciona ninguna aplicación.

- **Versión de la aplicación**

  En el campo de entrada, puede establecer un criterio para incluir los dispositivos en una selección al realizar búsquedas por el número de versión de una aplicación Kaspersky.

  No se aplica el criterio si no indica el número de la versión.

- Nombre de la actualización crítica

  En el campo de entrada, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas por el nombre de una aplicación o el número de paquete de una actualización.

  No se aplica el criterio si deja el campo en blanco.

- Última actualización de los módulos

  Puede utilizar esta opción como criterio para realizar búsquedas de dispositivos según la hora de la última actualización de los módulos de las aplicaciones instaladas en esos dispositivos.

  Si se selecciona esta casilla, en los campos de entrada podrá especificar el intervalo de tiempo (fecha y hora) en el que se realizó la última actualización de los módulos de las aplicaciones instaladas en esos dispositivos.

  No se aplica el criterio si esta casilla está vacía.

  De forma predeterminada, esta casilla está en blanco.

- El dispositivo se administra a través de Kaspersky Security Center 14

  En la lista desplegable, puede incluir en la selección los dispositivos administrados mediante Kaspersky Security Center:

  - **Sí**. En la selección los dispositivos administrados mediante Kaspersky Security Center.
  - **No**. La aplicación incluye en la selección dispositivos que no estén administrados por Kaspersky Security Center.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Aplicación de seguridad instalada

  En la lista desplegable, puede incluir en la selección todos los dispositivos con la aplicación de seguridad instalada:

  - **Sí**. La aplicación incluye en la selección todos los dispositivos con la aplicación de seguridad instalada.
  - **No**. La aplicación incluye en la selección todos los dispositivos que no tienen aplicación de seguridad instalada.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

Sistema operativo

En la sección **Sistema operativo**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según su tipo del sistema operativo.

- Versión del sistema operativo

  Si se selecciona esta casilla de verificación, puede seleccionar un sistema operativo de la lista. Los dispositivos que tienen el sistema operativo especificado instalado se incluyen en los resultados de la búsqueda.

- Tamaño de bits del sistema operativo

  En la lista desplegable, puede seleccionar la arquitectura de su sistema operativo, que determinará cómo aplicar la regla de migración a su dispositivo (**Desconocido**, **x86**, **AMD64**, or **IA64**). De forma predeterminada, ninguna opción está seleccionada en la lista de modo que no se define la arquitectura del sistema operativo.

- Versión del Service Pack del sistema operativo

  En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y.*), que determinará cómo aplicar la regla de migración a su dispositivo. De forma predeterminada, no se especifica ningún valor de la versión.

- Compilación del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de Windows.

  El número de compilación del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un número de compilación igual, anterior o posterior. También puede configurar la búsqueda de todos los números de compilación, excepto el especificado.

- ID de versión del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de Windows.

  El identificador de la versión (Id.) del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un Id. de versión igual, anterior o posterior. También puede configurar la búsqueda de todos los números de Id. de versión, excepto el especificado.

Estado del dispositivo

En la sección **Estado del dispositivo**, puede configurar criterios para incluir dispositivos en una selección según la descripción del estado de dispositivos desde una aplicación administrada:

- Estado del dispositivo

  Lista desplegable en la que se puede seleccionar uno de los estados del dispositivo: *Aceptar*, *Crítico* o *Advertencia*.

- Descripción del estado del dispositivo

  En este campo se pueden seleccionar las casillas de verificación que se muestran junto a las condiciones que, si se cumplen, asignarán uno de los siguientes estados al dispositivo: *Aceptar, Crítico* o *Advertencia*.

- Estado del dispositivo definido por la aplicación

Lista desplegable en la que se puede seleccionar el estado de protección en tiempo real. Se incluyen en la selección los dispositivos que tengan el estado de protección en tiempo real especificado.

Componentes de protección

En la sección **Componentes de protección**, puede configurar los criterios para incluir dispositivos en una selección según su estado de protección:

- Bases de datos lanzadas

  Si esta opción está seleccionada, se puede hacer una búsqueda de dispositivos cliente por la fecha de lanzamiento de la base de datos antivirus. En los campos de entrada se puede establecer el intervalo de tiempo con el que se realizará la búsqueda.

  Esta opción está desactivada de forma predeterminada.

- Último análisis

  Si esta casilla está activada, se puede hacer una búsqueda de dispositivos cliente por la fecha de último análisis antivirus. En los campos de entrada puede especificar el período de tiempo en el cual se realizó el último análisis antivirus.

  Esta opción está desactivada de forma predeterminada.

- Número total de amenazas detectadas

  Si esta opción está activada, puede buscar dispositivos cliente por número de virus detectados. En los campos de entrada se pueden establecer los valores máximo y mínimo del número de virus encontrados.

  Esta opción está desactivada de forma predeterminada.

Registro de aplicaciones

En la sección **Registro de aplicaciones**, puede configurar los criterios para buscar dispositivos según aplicaciones instaladas en ellos:

- Nombre de la aplicación

  Lista desplegable en la que se puede seleccionar la aplicación. En la selección se incluirán los dispositivos que tengan instalada la aplicación especificada.

- Versión de la aplicación

  Campo de entrada en el que se puede especificar la versión de la aplicación seleccionada.

- Proveedor

  Lista desplegable en la que se puede seleccionar el fabricante de una aplicación instalada en el dispositivo.

- Estado de la aplicación

  Una lista desplegable en la que se puede seleccionar el estado de una aplicación (*Instalada*, *No instalada*). Los dispositivos en los cuales la aplicación especificada está instalada o no instalada, según el estado seleccionado, se incluirán en la selección.

- Buscar por la actualización

  Si esta opción está activada, la búsqueda se realizará utilizando los detalles de las actualizaciones para las aplicaciones instaladas en los dispositivos relevantes. Después de seleccionar la casilla de verificación, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambian a **Nombre de actualización**, **Versión de actualización** y **Estado** respectivamente.

  Esta opción está desactivada de forma predeterminada.

- Nombre de la aplicación de seguridad incompatible

  Lista desplegable en la que se puede seleccionar aplicaciones de seguridad de terceros. Durante la búsqueda, se incluirán en la selección los dispositivos que tengan instalada la aplicación especificada.

- Etiqueta de la aplicación

  En la lista desplegable se puede seleccionar la etiqueta de la aplicación. Todos los dispositivos que han instalado aplicaciones con la etiqueta seleccionada en la descripción se incluyen en la selección de dispositivos.

- Aplicar a los dispositivos que no tengan etiquetas especificadas

  Si esta opción está activada, el perfil de la directiva incluirá los dispositivos con descripciones que no contengan ninguna de las etiquetas seleccionadas.

  Si esta opción está desactivada, el software no se actualiza.

  Esta opción está desactivada de forma predeterminada.

Registro de hardware

En la sección **Registro de hardware**, puede configurar criterios para incluir dispositivos incluidos en una selección según su hardware instalado:

- Dispositivo

  En la lista desplegable, puede seleccionar el tipo de unidad. Todos los dispositivos con esta unidad se incluyen en los resultados de la búsqueda.

  El campo admite búsqueda de texto completo.

- Proveedor

En la lista desplegable se puede seleccionar el nombre del fabricante de la unidad. Todos los dispositivos con esta unidad se incluyen en los resultados de la búsqueda.

El campo admite búsqueda de texto completo.

- **Nombre del dispositivo**

  Nombre del dispositivo cliente en la red Windows. El dispositivo con el nombre especificado se incluirá en la selección.

- **Descripción**

  Descripción del dispositivo o unidad de hardware. Los dispositivos con la descripción especificada en este campo se incluirán en la selección.

  La descripción de un dispositivo en cualquier formato se puede introducir en la ventana de propiedades de ese dispositivo. El campo admite búsqueda de texto completo.

- **Proveedor del dispositivo**

  Nombre del fabricante del dispositivo. Los dispositivos fabricados por el fabricante especificado en este campo se incluirán en la selección.

  Puede introducir el nombre del fabricante en la ventana de propiedades de un dispositivo.

- **Número de serie**

  Todas las unidades de hardware con el número de serie especificado en este campo se incluirán en la selección.

- **Número de inventario**

  El equipo con el número de inventario especificado en este campo se incluirá en la selección.

- **Usuario**

  Todas las unidades de hardware del usuario especificado en este campo se incluirán en la selección.

- **Ubicación**

  Ubicación de un dispositivo o una unidad de hardware (por ejemplo, en la sede central o en una filial). Los dispositivos u otros dispositivos desplegados en la ubicación especificada en este campo se incluirán en la selección.

  Puede describir la ubicación de un dispositivo en cualquier formato en la ventana de propiedades de ese dispositivo.

- **Frecuencia de la CPU (MHz)**

Intervalo de frecuencia de una CPU. Los dispositivos con las CPU que coincidan con el intervalo de frecuencia especificado en estos campos (valores máximo y mínimo incluidos) se incluirán en la selección.

- Núcleos de CPU virtual

  Intervalo del número de núcleos virtuales en una CPU. Los dispositivos con las CPU que coincidan con el intervalo especificado en estos campos (valores máximo y mínimo incluidos) se incluirán en la selección.

- Volumen del disco duro, en GB

  Intervalo de los valores para el tamaño del disco duro en el dispositivo. Los dispositivos con los discos duros que coincidan con el intervalo especificado en estos campos de entrada (valores máximo y mínimo incluidos) se incluirán en la selección.

- Tamaño de RAM, en MB

  Intervalo de los valores para el tamaño de la RAM de un dispositivo. Los dispositivos con las RAM que coincidan con el intervalo especificado en estos campos de entrada (valores máximo y mínimo incluidos) se incluirán en la selección.

Máquinas virtuales

En la sección **Máquinas virtuales**, puede configurar los criterios para incluir dispositivos en la selección según si estos son máquinas virtuales o parte de la Infraestructura de escritorio virtual (VDI):

- Es una máquina virtual

  En la lista desplegable se pueden seleccionar las siguientes opciones:

  - **No es importante**.
    - **No**. Buscar dispositivos que no son máquinas virtuales.
    - **Sí**. Buscar dispositivos que son máquinas virtuales.

- Tipo de máquina virtual

  En la lista desplegable se puede seleccionar el fabricante de la máquina virtual.

  Esta lista desplegable está disponible si el valor **Sí** o **No es importante** se selecciona en la lista desplegable **Es una máquina virtual**.

- Parte de la infraestructura de escritorio virtual

En la lista desplegable se pueden seleccionar las siguientes opciones:

- **No es importante**.
  - **No**. Buscar dispositivos que no formen parte de la Infraestructura de escritorio virtual.
  - **Sí**. Buscar dispositivos que formen parte de una Infraestructura de escritorio virtual (VDI) de Microsoft.

Vulnerabilidades y actualizaciones

En la sección **Vulnerabilidades y actualizaciones**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según su fuente de Windows Update:

El WUA se ha cambiado al Servidor de administración

Puede seleccionar una de las opciones de búsqueda de la lista desplegable:

- **Sí**. Si se selecciona esta opción, en los resultados de la búsqueda se incluirán los dispositivos que reciben actualizaciones del Servidor de administración a través de Windows Update.
- **No**. Si se selecciona esta opción, en los resultados se incluirán los dispositivos que reciben actualizaciones de otras fuentes a través de Windows Update.

Usuarios

En la sección **Usuarios**, puede configurar los criterios para incluir dispositivos en la selección según las cuentas de usuarios que han iniciado sesión en el sistema operativo.

- Último usuario que inició sesión en el sistema

  Si esta opción está activada, haga clic en el botón **Examinar** para especificar una cuenta de usuario. Los resultados de la búsqueda incluyen los dispositivos en los que un usuario específico ha iniciado sesión por última vez.

- Usuario que inició sesión en el sistema al menos una vez

  Si esta opción está activada, haga clic en el botón **Examinar** para especificar una cuenta de usuario. Los resultados de la búsqueda incluyen los dispositivos en los que el usuario especificado inició sesión en el sistema al menos una vez.

Problemas relacionados con el estado de las aplicaciones administradas

En la sección **Problemas relacionados con el estado de las aplicaciones administradas**, puede especificar los criterios que se utilizarán para incluir dispositivos en la selección de acuerdo con la lista de posibles problemas detectados por una aplicación administrada. Si al menos un problema que selecciona existe en un dispositivo, el dispositivo se incluirá en la selección. Cuando selecciona un problema listado para varias aplicaciones, tiene la opción de seleccionar este problema en todas las listas automáticamente.

[Descripción del estado del dispositivo]

En este campo puede seleccionar las casillas para las descripciones de estados desde la aplicación administrada; al recibir estos estados, los dispositivos se incluirán en la selección. Cuando selecciona un estado listado para varias aplicaciones, tiene la opción de seleccionar este estado en todas las listas automáticamente.

Estados de los componentes en aplicaciones administradas

En la sección **Estados de los componentes en aplicaciones administradas**, puede configurar criterios para incluir dispositivos en una selección según los estados de componentes en aplicaciones administradas:

- [Estado de la prevención contra fugas de datos]

  Buscar dispositivos por el estado de Prevención de fuga de datos (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- [Estado de la protección de los servidores de colaboración]

  Buscar dispositivos por el estado de la protección de colaboración del servidor (*No hay datos del dispositivo*, *Detenido*, *Iniciando, En pausa*, *En ejecución*, *Fallo*).

- [Estado de la protección antivirus de servidores de correo]

  Buscar dispositivos por el estado de protección del servidor de correo (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- [Estado de sensor de Endpoint]

  Buscar dispositivos por el estado del componente del sensor de Endpoint (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

Cifrado

[Algoritmo de cifrado]

Algoritmo de cifrado de bloques simétricos Advanced Encryption Standard (AES). En la lista desplegable, puede seleccionar el tamaño de la clave de cifrado (de 56 bits, de 128 bits, de 192 bits o de 256 bits).

Valores disponibles: *AES56*, *AES128*, *AES192* y *AES256*.

Segmentos de la nube

En la sección **Segmentos de la nube**, puede configurar criterios para incluir dispositivos en una selección según sus segmentos de la nube respectivos:

- [El dispositivo está en un segmento de la nube]

Si esta opción está activada, puede hacer clic en el **Examinar** para especificar qué segmento buscar.

Si la opción **Incluir objetos secundarios** también está activada, la búsqueda se ejecuta en todos los objetos secundarios del segmento especificado.

Los resultados de la búsqueda solo incluyen dispositivos desde el segmento seleccionado.

- Dispositivo descubierto mediante la API

  En la lista desplegable, puede seleccionar si un dispositivo es detectado por herramientas API.

  - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de AWS.
  - **Azure**. El dispositivo se descubre mediante la Azure API, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
  - **Google Cloud.**El dispositivo se descubre mediante la API de Google, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de Google.
  - **No**. El dispositivo no se puede detectar con AWS, Azure o Google API, es decir, o bien está fuera del entorno de nube, o está en el entorno de nube pero no se puede detectar mediante API por algún motivo.
  - Ningún valor. Este criterio no se puede aplicar.

Componentes de la aplicación

Esta sección contiene la lista de componentes de aquellas aplicaciones que tienen complementos de administración correspondientes instalados en la Consola de administración.

En la sección **Componentes de la aplicación**, puede especificar los criterios para incluir dispositivos en una selección de acuerdo con los estados y números de versión de los componentes que se refieren a la aplicación que seleccione:

- Estado

Buscar dispositivos de acuerdo con el estado del componente enviado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *No se reciben datos del dispositivo*, *Detenido*, *Iniciado*, *Pausado*, *En ejecución*, *Mal funcionamiento* o *No instalado*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo se incluye en la selección de dispositivos.

Estados enviados por solicitudes:

- *Iniciando:* El componente está actualmente en el proceso de iniciación.
- *En ejecución:* El componente se activa y funciona correctamente.
- *En pausa:* El componente se suspende, por ejemplo, después de que el usuario ha hecho una pausa la protección en la aplicación administrada.
- *Mal funcionamiento:* Un error ha ocurrido durante la operación del componente.
- *Detenido:* El componente está desactivado y no funciona en este momento.
- *No instalado:* El usuario no seleccionó el componente para la instalación al configurar la instalación personalizada de la aplicación.

A diferencia de otros estados, las aplicaciones *no envían datos del estado del dispositivo*. Esta opción muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Por ejemplo, esto puede suceder cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

- **Versión**

  Buscar dispositivos de acuerdo con el número de versión del componente que seleccione en la lista. Puede escribir un número de versión, por ejemplo `3.4.1.0`, y luego especificar si el componente seleccionado debe tener una versión igual, anterior o posterior. También puede configurar la búsqueda de todas las versiones excepto la especificada.

Exportar a un archivo de texto los parámetros de una selección de dispositivos

Para exportar a un archivo de texto los parámetros de una selección de dispositivos:

1. En el árbol de consola, seleccione la carpeta **Selecciones de dispositivos**.
2. En el espacio de trabajo, en la ficha **Selección** haga clic en la selección de dispositivos relevante en la lista de selecciones de usuarios.

   La configuración solo se puede exportar desde las selecciones de dispositivo creadas por un usuario.

3. Haga clic en el botón **Ejecutar selección**.
4. En la pestaña **Resultados de la selección**, haga clic en el botón **Exportar configuración**.
5. En la ventana **Guardar como** que se abre, especifique un nombre para el archivo de exportación de la configuración de la selección, seleccione una carpeta para guardarla y haga clic en el botón **Guardar**.

La configuración de la selección de dispositivos se guardará en el archivo especificado.

Creación de una selección de dispositivos

Para crear una selección de dispositivos:

1. En el árbol de consola, seleccione la carpeta **Selecciones de dispositivos**.
2. En el espacio de trabajo de la carpeta, haga clic en **Avanzado** y seleccione **Crear una selección** en la lista desplegable.
3. En la ventana **Nueva selección de dispositivos** que se abrirá, introduzca el nombre de la nueva selección y haga clic en **Aceptar**.

En el árbol de consola, en la carpeta **Selecciones de dispositivos**, aparecerá una carpeta nueva con el nombre introducido. De forma predeterminada, la nueva selección de dispositivos contiene todos los dispositivos incluidos en los grupos de administración del Servidor de administración en el que se ha creado la selección. Para que una selección se muestre únicamente en los dispositivos en los que esté especialmente interesado, configúrela haciendo clic en el botón **Propiedades de la selección**.

Creación de una selección de dispositivos mediante parámetros importados

Para crear una selección de dispositivos mediante parámetros importados:

1. En el árbol de consola, seleccione la carpeta **Selecciones de dispositivos**.
2. En el espacio de trabajo de la carpeta, haga clic en el botón **Avanzado** y seleccione **Importar selección desde archivo** en la lista desplegable.
3. En la ventana que se abra, especifique la ruta del archivo desde la que se quiere importar la selección de parámetros. Haga clic en el botón **Abrir**.

Se crea una entrada **Nueva selección** en la carpeta **Selecciones de dispositivos**. Los parámetros de la nueva selección se importarán desde el archivo especificado.

Si ya existe una selección denominada **Nueva selección** en la carpeta **Selecciones de dispositivos**, se agregará un índice con el formato **(<siguiente número secuencial>)** al nombre de la selección creada; por ejemplo: **(1)**, **(2)**.

Eliminación de dispositivos de grupos de administración en una selección

Al trabajar con una selección de dispositivos, se pueden quitar dispositivos de los grupos de administración en esta selección, sin necesidad de cambiar a los grupos de administración donde se encuentren ubicados los dispositivos.

Para quitar dispositivos de los grupos de administración:

1. En el árbol de consola, seleccione la carpeta **Selecciones de dispositivos**.
2. Seleccione los dispositivos que quiera quitar mediante las teclas **Mayús** o **Ctrl**.
3. Quite los dispositivos seleccionados de los grupos de administración de una de estas formas:

- Seleccione **Eliminar** en el menú contextual de cualquiera de los dispositivos seleccionados.
- Haga clic en el botón **Realizar acción** y seleccione **Quitar del grupo** en la lista desplegable.

Los dispositivos seleccionados se quitarán de los grupos de administración correspondientes.

Supervisión de instalación y desinstalación de aplicaciones

Puede supervisar la instalación y desinstalación de aplicaciones específicas en dispositivos administrados (por ejemplo, un navegador específico). Para usar esta función, puede añadir aplicaciones del Registro de aplicaciones a la lista de aplicaciones supervisadas. Cuando se instala o desinstala una aplicación supervisada, el Agente de red publica los eventos respectivos: **La aplicación supervisada se ha instalado** o **La aplicación supervisada se ha desinstalado**. Puede supervisar estos eventos utilizando, por ejemplo, selecciones de eventos o informes.

Puede supervisar estos eventos solo si están almacenados en la base de datos del Servidor de administración.

Para añadir una aplicación a la lista de aplicaciones supervisadas:

1. En la carpeta **Avanzado** → **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Registro de aplicaciones**.
2. Antes de la lista de aplicación que se muestra, haga clic en el botón **Mostrar ventana de propiedades del Registro de aplicaciones**.
3. En la **Aplicaciones supervisadas** ventana que se muestra, haga clic en el botón **Añadir**.
4. En la ventana que se muestra **Seleccione el nombre de la aplicación**, seleccione las aplicaciones del registro de aplicaciones cuya instalación o desinstalación desea supervisar.
5. En la ventana **Seleccione el nombre de la aplicación**, haga clic en el botón **Aceptar**.

Después de configurar la lista de aplicaciones supervisadas y de que una aplicación supervisada se instale o desinstale en los dispositivos administrados en su organización, puede supervisar los eventos respectivos, por ejemplo, utilizando la selección de eventos Eventos recientes.

Tipos de evento

Cada componente de Kaspersky Security Center tiene su propio conjunto de tipos de evento. Esta sección enumera los tipos de eventos que ocurren en el Servidor de administración de Kaspersky Security Center, Agente de red, Servidor de MDM para iOS y Servidor de dispositivos móviles de Exchange. Los tipos de eventos que ocurren en las aplicaciones de Kaspersky no se enumeran en esta sección.

Estructura de datos de descripción de tipo de evento

Para cada tipo de evento, se proporcionan su nombre para mostrar, el identificador (Id.), el código alfabético, la descripción y el plazo de almacenamiento predeterminado.

- **Nombre de visualización del tipo de evento**. Este texto se muestra en Kaspersky Security Center cuando configura los eventos y cuando ocurren.

- **ID del tipo de evento**. Este código numérico se usa cuando procesa eventos utilizando herramientas de terceros para el análisis de eventos.
- **Tipo de evento** (código alfabético). Este código se usa cuando navega y procesa eventos utilizando vistas públicas que se proporcionan en la base de datos de Kaspersky Security Center y cuando los eventos se exportan a un sistema SIEM.
- **Descripción**. Este texto contiene las situaciones en las que ocurre un evento y lo que puede hacer en tal caso.
- **Plazo de almacenamiento predeterminado**. Este es el número de días durante los cuales el evento se almacena en la base de datos del Servidor de administración y se muestra en la lista de eventos en el Servidor de administración. Transcurrido este periodo, se elimina el evento. Si el valor del plazo de almacenamiento de eventos es 0, dichos eventos se detectan pero no se muestran en la lista de eventos en el Servidor de administración. Si se configuró para guardar dichos eventos en el registro de eventos del sistema operativo, puede encontrarlos allí.

  Puede cambiar el plazo de almacenamiento para eventos:

  - Consola de administración: Configuración del plazo de almacenamiento para un evento
  - Kaspersky Security Center 14 Web Console: Configuración del plazo de almacenamiento para un evento

Otros datos pueden incluir los siguientes campos:

- **event_id**: número único del evento en la base de datos, generado y asignado automáticamente. No se debe confundir con el **ID del tipo de evento**.
- **task_id**: el ID de la tarea que causó el evento (si lo hay).
- **gravedad**: uno de los siguientes niveles de gravedad (en orden ascendente de gravedad):

  0) Nivel de gravedad no válido

  1) Info.

  2) Advertencia

  3) Error

  4) Crítico

Eventos del Servidor de administración

Esta sección contiene información sobre los eventos relacionados con el Servidor de administración.

Eventos críticos del Servidor de administración

La siguiente tabla muestra los tipos de eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Crítico**.

Eventos críticos del Servidor de administración

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plaz almacer predete
Se ha superado el límite de	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Una vez al día, Kaspersky Security	180 días

licencias			Center comprueba si se excede una restricción de licencia. Los eventos de este tipo ocurren cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en dispositivos cliente exceden algunos límites de licencia y si el número de unidades de licencia utilizadas actualmente y cubiertas por una sola licencia supera el 110 % del número total de unidades cubiertas por la licencia. Incluso cuando se produce este evento, los dispositivos cliente están protegidos. Puede responder al evento de las siguientes formas: • Mire la lista de dispositivos administrados. Elimine dispositivos que no están en uso. • Proporcione una licencia para más dispositivos (añada un código de activación o un archivo clave válidos al Servidor de administración). Kaspersky Security Center determina las reglas para generar eventos cuando se excede una restricción de licencia.	
Brote de virus	26 (para	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este	180 días

	Protección frente a amenazas en archivos)		tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto periodo de tiempo. Puede responder al evento de las siguientes formas: • Puede configurar el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se activará o cree una tarea que se ejecutará cuando ocurra este evento.	
Brote de virus	27 (para Protección frente a amenazas en el correo)	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto periodo de tiempo. Puede responder al evento de las siguientes formas: • Puede configurar el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se activará o cree una tarea que se ejecutará cuando ocurra este evento.	180 días
Brote de virus	28 (para	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este	180 días

	firewall)		tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto periodo de tiempo. Puede responder al evento de las siguientes formas: • Puede configurar el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se activará o cree una tarea que se ejecutará cuando ocurra este evento.	
Se ha perdido la conexión con el dispositivo	4111	KLSRV_HOST_OUT_CONTROL	Los eventos de este tipo ocurren si un dispositivo administrado es visible en la red pero no se ha conectado al Servidor de administración durante un cierto periodo de tiempo. Averigüe lo que impide el buen funcionamiento del Agente de red en el dispositivo. Las causas posibles incluyen problemas de red y la eliminación de Agente de red del dispositivo.	180 días
El estado del dispositivo es Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Los eventos de este tipo ocurren cuando se le asigna el estado *Crítico* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del	180 días

			dispositivo se cambia a *Crítico*.	
El archivo clave se ha añadido a la lista de rechazados	4124	KLSRV_LICENSE_BLACKLISTED	Los eventos de este tipo ocurren cuando Kaspersky ha añadido a la lista de rechazados el código de activación o el archivo clave que usa en la lista de prohibidos. Póngase en contacto con el Servicio de soporte técnico para obtener más detalles.	180 días
Modo de funcionalidad limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Los eventos de este tipo ocurren cuando Kaspersky Security Center empieza a funcionar con funcionalidad básica, sin la Administración de vulnerabilidades y parches y sin la función Administración de dispositivos móviles. A continuación, se presentan las causas y las respuestas adecuadas al evento: • El periodo de vigencia de la licencia ha caducado. Proporcione una licencia para utilizar el modo de funcionalidad completa de Kaspersky Security Center (añada un código de activación válido o un archivo clave al Servidor de administración). • El Servidor de administración gestiona más dispositivos de los que especifica el límite de licencia.	180 días

			Mueva los dispositivos de los grupos de administración de un Servidor de administración a los de otro Servidor de administración (si el límite de licencia del otro Servidor de administración lo permite).	
La licencia caduca pronto	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Ocurren eventos de este tipo cuando se acerca la fecha de caducidad de la licencia comercial. Una vez al día, Kaspersky Security Center comprueba si se acerca la fecha de caducidad de la licencia. Los eventos de este tipo se publican 30 días, 15 días, cinco días y un día antes de la fecha de caducidad de la licencia. No puede cambiar el número de días. Si el Servidor de administración se apaga el día especificado antes de la fecha de caducidad de la licencia, el evento no se publicará hasta el día siguiente. Cuando caduca la licencia comercial, Kaspersky Security Center presta solo la funcionalidad básica. Puede responder al evento de las siguientes formas: • Asegúrese de añadir una clave de licencia de reserva al Servidor de administración.	180 días

			• Si usa una suscripción, asegúrese de renovarla. Una suscripción ilimitada se renueva automáticamente si se ha pagado previamente al proveedor de servicios en el plazo de vencimiento.	
El certificado ha caducado	4132	KLSRV_CERTIFICATE_EXPIRED	Los eventos de este tipo ocurren cuando caduca el certificado del Servidor de administración para la Administración de dispositivos móviles. Debe actualizar el certificado caducado. Puede configurar actualizaciones automáticas de certificados seleccionando la casilla de verificación **Reemitir el certificado automáticamente siempre que sea posible** en la configuración de emisión del certificado.	180 días
Se han anulado las actualizaciones para los módulos del software Kaspersky	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Los eventos de este tipo ocurren si los especialistas técnicos de Kaspersky han revocado las actualizaciones sin problemas (El estado *revocado* se muestra para estas actualizaciones), por ejemplo, se deben actualizar a una versión más reciente. El evento afecta a los parches de Kaspersky Security Center pero no a los módulos de las	180 días

			aplicaciones de Kaspersky administradas. El evento proporciona el motivo por el que no se instalan las actualizaciones sin problemas.	

Servidor de administración eventos de fallos operativos

La siguiente tabla muestra los tipos de eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Fallo operativo**.

Servidor de administración eventos de fallos operativos

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamie predetermin
Error en tiempo de ejecución	4125	KLSRV_RUNTIME_ERROR	Los eventos de este tipo ocurren debido a problemas desconocidos. La mayoría de las veces, se trata de problemas de DBMS, problemas de red y otros problemas de software y hardware. Los detalles del evento se pueden encontrar en la descripción del evento.	180 días
Se ha superado el límite de instalaciones para uno de los grupos de aplicaciones con licencia	4126	KLSRV_INVLICPROD_EXCEDED	El Servidor de administración genera eventos de este tipo de manera periódica (cada hora). Los eventos de este tipo ocurren si administra claves de licencia de aplicaciones de terceros en Kaspersky Security Center y si el número de instalaciones ha superado el límite establecido por la clave de licencia de la aplicación de terceros.	180 días

			Puede responder al evento de las siguientes formas: • Mire la lista de dispositivos administrados. Elimine la aplicación de terceros de los dispositivos en los cuales la aplicación no está en uso. • Utilice una licencia de terceros para más dispositivos. Puede administrar claves de licencia de terceros utilizando la funcionalidad de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia incluye las aplicaciones de terceros que cumplen los criterios establecidos por usted.	
No se ha podido sondear el segmento de la nube	4143	KLSRV_KLCLOUD_SCAN_ERROR	Los eventos de este tipo ocurren cuando el Servidor de administración no puede sondear un segmento de red en un entorno de nube. Lea los detalles en la descripción del evento y actúe en consecuencia.	No almacena
Error al copiar las actualizaciones en la carpeta especificada	4123	KLSRV_UPD_REPL_FAIL	Los eventos de este tipo ocurren cuando las actualizaciones de software se copian a (una) carpeta(s) compartida(s) adicional(es). Puede responder al evento de las siguientes formas: • Compruebe si la cuenta de usuario que se emplea para obtener	180 días

			acceso a la(s) carpeta(s) tiene permiso de escritura. • Compruebe si cambió un nombre de usuario y / o una contraseña de la carpeta(s). • Compruebe la conexión a Internet, ya que podría ser la causa del evento. Siga las instrucciones para actualizar las bases de datos y los módulos de software.	
No queda espacio libre en el disco	4107	KLSRV_DISK_FULL	Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración se queda sin espacio libre. Liberar espacio en disco en el dispositivo.	180 días
La carpeta compartida no está disponible	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Los eventos de este tipo ocurren si la carpeta compartida del Servidor de administración no está disponible. Puede responder al evento de las siguientes formas: • Compruebe si el Servidor de administración (donde se encuentra la carpeta compartida) está encendido y disponible. • Compruebe si se cambió/cambiaron un nombre de usuario y / o una	180 días

			contraseña de la carpeta. • Compruebe la conexión de red.	
La base de datos de información del Servidor de administración no está disponible	4109	KLSRV_DATABASE_UNAVAILABLE	Los eventos de este tipo ocurren si la base de datos del Servidor de administración no está disponible. Puede responder al evento de las siguientes formas: • Compruebe si está disponible el servidor remoto que instala SQL Server. • Vea los registros de DBMS para descubrir el motivo de la falta de disponibilidad de la base de datos del Servidor de administración. Por ejemplo, un servidor remoto que tiene instalado SQL Server podría no estar disponible debido al mantenimiento preventivo.	180 días
No hay espacio libre en la base de datos del Servidor de administración	4110	KLSRV_DATABASE_FULL	Los eventos de este tipo ocurren cuando no hay espacio libre en la base de datos del Servidor de administración. El Servidor de administración no funciona cuando su base de datos ha alcanzado su capacidad y cuando no es posible seguir guardando en la base de datos.	180 días

					A continuación se describen las causas de este evento, según el DBMS que utiliza, y las respuestas adecuadas al evento: • Usted utiliza el DBMS de SQL Server Express Edition: En la documentación de SQL Server Express, revise el límite del tamaño de la base de datos de la versión que utiliza. Probablemente, la base de datos de su Servidor de administración ha superado el límite del tamaño de la base de datos. Limite el número de eventos para almacenar en la base de datos del Servidor de administración. En la base de datos del Servidor de administración hay demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de la directiva de Kaspersky Endpoint Security para Windows relacionada con el almacenamiento de eventos del Control de aplicaciones en la base de datos del Servidor de administración. • Usted utiliza un DBMS distinto de

			SQL Server Express Edition: No limite el número de eventos para almacenar en la base de datos del Servidor de administración. Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración. Revise la información sobre la selección de DBMS.	

Eventos de advertencia del Servidor de administración

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Advertencia**.

Eventos de advertencia del Servidor de administración

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo almacenar predeterm
Se ha superado el límite de licencias	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una vez al día, Kaspersky Security Center comprueba si se excede una restricción de licencia.	90 días

			Los eventos de este tipo ocurren cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente exceden algunos límites de licencia y si el número de unidades de licencia utilizadas actualmente y cubiertas por una sola licencia constituye del 100 % al 110 % del número total de unidades cubiertas por la licencia. Incluso cuando se produce este evento, los dispositivos cliente están protegidos. Puede responder al evento de las siguientes formas: • Mire la lista de dispositivos administrados. Elimine dispositivos que no están en uso. • Proporcione una licencia para más dispositivos (añada un código de activación o un archivo clave válidos al Servidor de administración). Kaspersky Security Center determina las reglas para generar eventos cuando se excede una restricción de licencia.	
El dispositivo ha permanecido inactivo en la	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Los eventos de este tipo ocurren cuando un dispositivo administrado muestra	90 días

red durante mucho tiempo			inactividad durante algún tiempo. La mayoría de las veces, esto sucede cuando se da de baja un dispositivo administrado. Puede responder al evento de las siguientes formas: • Elimine manualmente el dispositivo de la lista de dispositivos administrados. • Especifique el intervalo de tiempo después del cual se crea el evento **El dispositivo ha permanecido inactivo en la red durante mucho tiempo** mediante el uso de la Consola de administración o Kaspersky Security Center 14 Web Console. • Especifique el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo mediante el uso de la Consola de administración o Kaspersky Security Center 14 Web Console.	
Conflicto de nombres de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Los eventos de este tipo ocurren cuando el Servidor de administración considera que dos o más dispositivos administrados distintos son un solo dispositivo.	90 días

			La mayoría de las veces, esto sucede cuando se ha utilizado un disco duro clonado para el despliegue de software en los dispositivos administrados y sin haber cambiado el Agente de red al modo de clonación de discos específico en un dispositivo de referencia. Para evitar este problema, cambie el Agente de red al modo de clonación de discos en un dispositivo de referencia antes de clonar el disco duro de este dispositivo.	
El estado del dispositivo es Advertencia	4114	KLSRV_HOST_STATUS_WARNING	Los eventos de este tipo ocurren cuando se le asigna el estado de *Advertencia* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del dispositivo se cambia a *Advertencia*.	90 días
Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia	4127	KLSRV_INVLICPROD_FILLED	Los eventos de este tipo ocurren cuando la cantidad de instalaciones de aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del valor máximo permitido que se especifica en las propiedades de la clave de licencia. Puede responder al evento de las siguientes formas: • Si la aplicación de terceros no está en uso en algunos de los dispositivos administrados,	90 días

			elimínela de estos dispositivos. • Si cree que la cantidad de instalaciones de la aplicación de terceros excederá pronto el máximo permitido, le recomendamos que adquiera con anticipación una licencia de terceros para una mayor cantidad de dispositivos. Puede administrar claves de licencia de terceros utilizando la funcionalidad de grupos de aplicaciones con licencia.	
Se ha solicitado el certificado	4133	KLSRV_CERTIFICATE_REQUESTED	Los eventos de este tipo ocurren cuando no se puede volver a emitir automáticamente un certificado para Administración de dispositivos móviles. A continuación se mencionan las probables causas del evento y las respuestas adecuadas a este: • Se ha iniciado la nueva emisión automática de un certificado para el que la opción **Reemitir el certificado automáticamente siempre que sea posible** está desactivada. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se deba volver a emitir el	90 días

			certificado de forma manual. • Si utiliza una integración con una infraestructura de clave pública, la causa podría ser la falta del atributo SAM-Account-Name de la cuenta utilizada para la integración con PKI y para la emisión del certificado. Revise las propiedades de la cuenta.	
El certificado se ha eliminado	4134	KLSRV_CERTIFICATE_REMOVED	Los eventos de este tipo ocurren cuando un administrador elimina algún tipo de certificado (General, Correo, VPN) para Administración de dispositivos móviles. Después de eliminar un certificado, los dispositivos móviles que estén conectados a través de este certificado no podrán conectarse al Servidor de administración. Este evento puede resultar útil a la hora de investigar errores asociados con la administración de dispositivos móviles.	90 días
El certificado de APNs ha caducado	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Los eventos de este tipo ocurren cuando caduca un certificado de APNs. Debe renovar el certificado de APNs manualmente e instalarlo en un servidor de MDM para iOS.	No almace
El certificado de APNs	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Los eventos de este tipo ocurren cuando	No almace

caducará pronto			quedan menos de 14 días para que caduque el certificado de APNs. Cuando el certificado de APNs caduca, debe renovarlo manualmente e instalarlo en un servidor de MDM para iOS. Le recomendamos que programe la renovación del certificado de APNs antes de la fecha de caducidad.	
No se ha podido enviar el mensaje FCM al dispositivo móvil	4138	KLSRV_GCM_DEVICE_ERROR	Los eventos de este tipo ocurren cuando Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectarse a dispositivos móviles administrados con sistema operativo Android y cuando el servidor de FCM no puede manejar algunas de las solicitudes que recibe del Servidor de administración. Significa que algunos de los dispositivos móviles administrados no recibirán una notificación push.	90 días

			Lea el código HTTP en los detalles de la descripción del evento y actúe en consecuencia. Para obtener más información sobre los códigos HTTP que se reciben del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (consulte el capítulo "Códigos de respuesta de errores de mensajes descendentes").	
Se produjo un error de HTTP al enviar el mensaje FCM al servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	Los eventos de este tipo ocurren cuando Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectar dispositivos móviles administrados con sistema operativo Android y cuando el servidor de FCM devuelve un código HTTP distinto de 200 (OK) a la solicitud del Servidor de administración. A continuación se mencionan las probables causas del evento y las respuestas adecuadas a este: • Problemas en el lado del servidor de FCM. Lea el código HTTP en los detalles de la descripción del evento y actúe en consecuencia. Para obtener más información sobre los códigos HTTP que se reciben del servidor de FCM y los errores relacionados,	90 días

			consulte la documentación del servicio Google Firebase (consulte el capítulo "Códigos de respuesta de errores de mensajes descendentes"). • Problemas del servidor proxy (si usa un servidor proxy). Lea el código HTTP en los detalles del evento y actúe en consecuencia.	
No se ha podido enviar el mensaje FCM al servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	Los eventos de este tipo ocurren debido a errores inesperados en el Servidor de administración cuando se trabaja con el protocolo HTTP de Google Firebase Cloud Messaging. Lea los detalles en la descripción del evento y actúe en consecuencia. Si no puede encontrar la solución para un problema por su cuenta, le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky.	90 días
Poco espacio libre en el disco duro	4105	KLSRV_NO_SPACE_ON_VOLUMES	Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración casi se queda sin espacio libre. Liberar espacio en disco en el dispositivo.	90 días
Poco espacio libre en la base	4106	KLSRV_NO_SPACE_IN_DATABASE	Los eventos de este tipo ocurren si el	90 días

de datos del Servidor de administración			espacio en la base de datos del Servidor de administración es demasiado reducido. Si no soluciona la situación, la base de datos del Servidor de administración pronto alcanzará su capacidad y el Servidor de administración no funcionará. A continuación se describen las causas de este evento, según el DBMS que utiliza, y las respuestas adecuadas al evento. Usted utiliza el DBMS de SQL Server Express Edition: • En la documentación de SQL Server Express, revise el límite del tamaño de la base de datos de la versión que utiliza. Probablemente la base de datos de su Servidor de administración esté por alcanzar el límite del tamaño de la base de datos. • Limite el número de eventos para almacenar en la base de datos del Servidor de administración. • En la base de datos del Servidor de administración hay demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de

			la directiva de Kaspersky Endpoint Security para Windows relacionada con el almacenamiento de eventos del Control de aplicaciones en la base de datos del Servidor de administración. Usted utiliza un DBMS distinto de SQL Server Express Edition: • No limite el número de eventos para almacenar en la base de datos del Servidor de administración. • Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración. Revise la información sobre la selección de DBMS.	
Se ha interrumpido la conexión con el Servidor de administración secundario	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Los eventos de este tipo ocurren cuando se interrumpe una conexión con el Servidor de administración secundario. Lea el Registro de eventos de Kaspersky del dispositivo donde está instalado el Servidor de administración secundario y responda en consecuencia.	90 días
Se ha interrumpido la conexión con el Servidor de administración principal	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Los eventos de este tipo ocurren cuando se interrumpe una conexión con el Servidor de	90 días

			administración principal. Lea el Registro de eventos de Kaspersky del dispositivo donde está instalado el Servidor de administración principal y responda en consecuencia.	
Se han registrado las nuevas actualizaciones para los módulos del software Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Los eventos de este tipo ocurren cuando el Servidor de administración registra actualizaciones nuevas para el software de Kaspersky instalado en los dispositivos administrados que usted debe aprobar para su instalación. Apruebe o rechace las actualizaciones con la Consola de administración o con Kaspersky Security Center Web Console.	90 días
Se ha superado el límite del número de eventos en la base de datos, se ha iniciado la eliminación de eventos	4145	KLSRV_EVP_DB_TRUNCATING	Los eventos de este tipo ocurren cuando ha comenzado la eliminación de eventos antiguos de la base de datos del Servidor de administración después de que se alcanzó la capacidad de la base de datos del Servidor de administración. Puede responder al evento de las siguientes formas: • Cambie el número de eventos almacenados en la base de datos del Servidor de administración. • Reduzca la lista de eventos para almacenar en la base de datos del	No almace

			Servidor de administración.	
Se ha superado el límite del número de eventos en la base de datos, los eventos se han eliminado	4146	KLSRV_EVP_DB_TRUNCATED	Los eventos de este tipo ocurren cuando se han eliminado los eventos antiguos de la base de datos del Servidor de administración después de que se alcanzó la capacidad de la base de datos del Servidor de administración. Puede responder al evento de las siguientes formas: • Cambie el número máximo permitido de eventos que se almacenarán en la base de datos del Servidor de administración. • Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración.	No almace

Eventos informativos del Servidor de administración

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Información**.

Eventos informativos del Servidor de administración

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha consumido más del 90 % de la clave de licencia	4097	KLSRV_EV_LICENSE_CHECK_90	30 días
Se ha detectado un nuevo dispositivo	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 días
El dispositivo se ha agregado automáticamente al grupo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 días
El dispositivo se ha eliminado del grupo: inactivo en la red durante mucho tiempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 días

Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia (ya se ha usado más del 95 %)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 días
Se han encontrado archivos para enviar a Kaspersky para su análisis	4131	KLSRV_APS_FILE_APPEARED	30 días
El ID de instancia de FCM ha cambiado en este dispositivo móvil	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 días
Las actualizaciones se han copiado correctamente en la carpeta especificada	4122	KLSRV_UPD_REPL_OK	30 días
La conexión con el Servidor de administración secundario está establecida	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 días
La conexión con el Servidor de administración principal está establecida	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 días
Las bases de datos se han actualizado	4144	KLSRV_UPD_BASES_UPDATED	30 días
Auditoría: Se ha establecido la conexión con el Servidor de administración	4147	KLAUD_EV_SERVERCONNECT	30 días
Auditoría: Se ha modificado el objeto	4148	KLAUD_EV_OBJECTMODIFY	30 días
Auditoría: El estado del objeto ha cambiado	4150	KLAUD_EV_TASK_STATE_CHANGED	30 días
Comprobar: Parámetros de grupo modificados	4149	KLAUD_EV_ADMGROUP_CHANGED	30 días
Auditoría: Se ha finalizado la conexión al Servidor de administración	4151	KLAUD_EV_SERVERDISCONNECT	30 días
Auditoría: Se han modificado las propiedades del objeto	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 días
Auditoría: Se han modificado los permisos de usuario	4153	KLAUD_EV_OBJECTACLMODIFIED	30 días

Eventos del Agente de red

Esta sección contiene información sobre los eventos relacionados con el Agente de red.

Eventos de fallos operativos del Agente de red

La siguiente tabla muestra los tipos de eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Fallo operativo**.

Eventos de fallos operativos del Agente de red

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Error al instalar la actualización	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Los eventos de este tipo ocurren si la actualización automática y los parches para los componentes de Kaspersky Security Center no tuvieron éxito. El evento no concierne actualizaciones de las aplicaciones de Kaspersky administradas. Lea la descripción del evento. Un problema de Windows en un Servidor de administración puede ser una razón para este evento. Si la descripción menciona algún problema de la configuración de Windows, resuelva este problema.	30 días
Error al instalar la actualización de software de terceros	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Los eventos de este tipo ocurren si las funciones de la Administración de vulnerabilidades y parches y la Administración de dispositivos móviles están en el uso, y si la instalación de actualizaciones de software de	30 días

			terceros no tuvo éxito. Compruebe si el enlace al software de terceros es válido. Lea la descripción del evento.	
Error al instalar las actualizaciones de Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Los eventos de este tipo ocurren si las actualizaciones de Windows no tuvieron éxito. Configurar las actualizaciones de Windows en una directiva del Agente de red. Lea la descripción del evento. Busque el error en Microsoft Knowledge Base. Póngase en contacto con el servicio de soporte técnico de Microsoft si no puede resolver el problema usted mismo.	30 días

Eventos de advertencia del Agente de red

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Advertencia**.

Eventos de advertencia del Agente de red

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha devuelto una advertencia durante la instalación de la actualización del módulo de software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 días
La instalación de la actualización de software de	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 días

terceros ha finalizado con una advertencia			
Se ha pospuesto la instalación de la actualización de software de terceros	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 días
Se ha producido un incidente	549	GNRL_EV_APP_INCIDENT_OCCURED	30 días
Se ha iniciado el proxy de KSN. Error en la comprobación de la disponibilidad de KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 días

Eventos informativos de advertencia del Agente de red

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Información**.

Eventos informativos de advertencia del Agente de red

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
La actualización de módulos del software se ha instalado correctamente	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 días
Se ha iniciado la instalación de la actualización del módulo de software	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 días
La aplicación se ha instalado	7703	KLNAG_EV_INV_APP_INSTALLED	30 días
La aplicación se ha desinstalado	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 días
La aplicación supervisada se ha instalado	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 días
La aplicación supervisada se ha desinstalado	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 días
La aplicación de terceros se ha instalado	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 días
Se ha agregado un nuevo dispositivo	7708	KLNAG_EV_DEVICE_ARRIVAL	30 días
El dispositivo se ha eliminado	7709	KLNAG_EV_DEVICE_REMOVE	30 días
Se ha detectado un	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 días

nuevo dispositivo			
El dispositivo se ha autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 días
Uso compartido del escritorio de Windows: se ha leído el archivo	7712	KLUSRLOG_EV_FILE_READ	30 días
Uso compartido del escritorio de Windows: se ha modificado el archivo	7713	KLUSRLOG_EV_FILE_MODIFIED	30 días
Uso compartido del escritorio de Windows: se ha iniciado la aplicación	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 días
Uso compartido del escritorio de Windows: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 días
Uso compartido del escritorio de Windows: detenido	7716	KLUSRLOG_EV_WDS_END	30 días
La actualización de software de terceros se ha instalado correctamente	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 días
Se ha iniciado la instalación de la actualización de software de terceros	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 días
El proxy de KSN se ha iniciado. La comprobación de disponibilidad de KSN se ha completado correctamente	7719	KSNPROXY_STARTED_CON_CHK_OK	30 días
El proxy de KSN se ha detenido	7720	KSNPROXY_STOPPED	30 días

Eventos del Servidor de MDM para iOS

Esta sección contiene información sobre los eventos relacionados con el Servidor de MDM para iOS.

Eventos de fallos operativos del Servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Fallo operativo**.

Eventos de fallos operativos del Servidor de MDM para iOS

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Error al solicitar la lista de perfiles	PROFILELIST_COMMAND_FAILED	30 días
Error al instalar el perfil	INSTALLPROFILE_COMMAND_FAILED	30 días
Error al eliminar el perfil	REMOVEPROFILE_COMMAND_FAILED	30 días
Error al solicitar la lista de perfiles de aprovisionamiento	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 días
Error al instalar perfil de aprovisionamiento	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 días
Error al quitar el perfil de aprovisionamiento	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 días
Error al solicitar la lista de certificados digitales	CERTIFICATELIST_COMMAND_FAILED	30 días
Error al solicitar la lista de aplicaciones instaladas	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 días
Error al solicitar información general sobre el dispositivo móvil	DEVICEINFORMATION_COMMAND_FAILED	30 días
Error al solicitar información sobre la seguridad	SECURITYINFO_COMMAND_FAILED	30 días
Error al bloquear el dispositivo móvil	DEVICELOCK_COMMAND_FAILED	30 días
Error al restablecer la contraseña	CLEARPASSCODE_COMMAND_FAILED	30 días
Error al borrar los datos del dispositivo móvil	ERASEDEVICE_COMMAND_FAILED	30 días
Error al instalar la app	INSTALLAPPLICATION_COMMAND_FAILED	30 días
Error al establecer el código de recuperación de la aplicación	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 días
Error al solicitar la lista de apps administradas	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 días
Error al eliminar la app administrada	REMOVEAPPLICATION_COMMAND_FAILED	30 días
La configuración de itinerancia se ha rechazado	SETROAMINGSETTINGS_COMMAND_FAILED	30 días
Se ha producido un error en el funcionamiento de la aplicación	PRODUCT_FAILURE	30 días
El resultado del comando contiene datos no válidos	MALFORMED_COMMAND	30 días

Error al enviar la notificación de inserción	SEND_PUSH_NOTIFICATION_FAILED	30 días
No se puede enviar el comando	SEND_COMMAND_FAILED	30 días
Dispositivo no encontrado	DEVICE_NOT_FOUND	30 días

Eventos de advertencia del Servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Advertencia**.

Eventos de advertencia del Servidor de MDM para iOS

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha detectado un intento de conectar el dispositivo móvil bloqueado	INACTICE_DEVICE_TRY_CONNECTED	30 días
El perfil se ha eliminado	MDM_PROFILE_WAS_REMOVED	30 días
Se ha detectado un intento de reutilización de un certificado de cliente	CLIENT_CERT_ALREADY_IN_USE	30 días
Se ha detectado un dispositivo inactivo	FOUND_INACTIVE_DEVICE	30 días
Se requiere un código de recuperación	NEED_REDEMPTION_CODE	30 días
El perfil se ha incluido en una directiva eliminada del dispositivo	UMDM_PROFILE_WAS_REMOVED	30 días

Eventos informativos del Servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Información**.

Eventos informativos del Servidor de MDM para iOS

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha conectado el nuevo dispositivo móvil	NEW_DEVICE_CONNECTED	30 días
La lista de perfiles se ha solicitado correctamente	PROFILELIST_COMMAND_SUCCESSFULL	30 días
El perfil se ha instalado correctamente	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 días
El perfil se ha eliminado	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 días

correctamente		
La lista de perfiles de aprovisionamiento se ha solicitado correctamente	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 días
El perfil de aprovisionamiento se ha instalado correctamente	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 días
El perfil de aprovisionamiento se ha eliminado correctamente	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 días
La lista de certificados digitales se ha solicitado correctamente	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 días
La lista de aplicaciones instaladas se ha solicitado correctamente	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 días
Se ha solicitado correctamente la información general sobre el dispositivo móvil	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 días
La información sobre seguridad se ha solicitado correctamente	SECURITYINFO_COMMAND_SUCCESSFULL	30 días
Se ha bloqueado correctamente el dispositivo móvil	DEVICELOCK_COMMAND_SUCCESSFULL	30 días
La contraseña se ha restablecido correctamente	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 días
Los datos se han eliminado del dispositivo móvil	ERASEDEVICE_COMMAND_SUCCESSFULL	30 días
La aplicación se ha instalado correctamente	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 días
El código de recuperación de la aplicación se ha establecido correctamente	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 días
Lista de aplicaciones administradas	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 días

solicitada correctamente		
La aplicación administrada se ha eliminado correctamente	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 días
La configuración de itinerancia se ha aplicado correctamente	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 días

Eventos del Servidor de dispositivos móviles de Exchange

Esta sección contiene información sobre los eventos relacionados con Servidor de dispositivos móviles de Exchange.

Eventos de fallos operativos del servidor de dispositivos móviles de Exchange

La siguiente tabla muestra los eventos del Servidor de dispositivos móviles de Kaspersky Security Center Exchange que tienen el nivel de gravedad **Fallo operativo**.

Eventos de fallos operativos del servidor de dispositivos móviles de Exchange

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Error al borrar los datos del dispositivo móvil	WIPE_FAILED	30 días
No se puede eliminar la información sobre la conexión del dispositivo móvil al buzón	DEVICE_REMOVE_FAILED	30 días
No se puede aplicar la directiva de ActiveSync al buzón de correo	POLICY_APPLY_FAILED	30 días
Error de funcionamiento de la aplicación	PRODUCT_FAILURE	30 días
Error al modificar el estado de la función ActiveSync	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 días

Eventos informativos del Servidor de dispositivos móviles de Exchange

La siguiente tabla muestra los eventos del Servidor de dispositivos móviles de Kaspersky Security Center Exchange que tienen el nivel de gravedad **Información**.

Eventos informativos del Servidor de dispositivos móviles de Exchange

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha conectado el nuevo dispositivo móvil	NEW_DEVICE_CONNECTED	30 días
Los datos se han eliminado del	WIPE_SUCCESSFULL	30 días

dispositivo móvil		

Bloqueo de eventos frecuentes

Esta sección proporciona información sobre cómo administrar el bloqueo de eventos frecuentes, cómo eliminar el bloqueo de eventos frecuentes y cómo exportar la lista de eventos frecuentes a un archivo.

Acerca del bloqueo de eventos frecuentes

Una aplicación administrada, por ejemplo, Kaspersky Endpoint Security para Windows, instalada en uno o varios dispositivos administrados, puede enviar muchos eventos del mismo tipo al Servidor de administración. La recepción de eventos frecuentes puede sobrecargar la base de datos del Servidor de administración y sobrescribir otros eventos. El Servidor de administración comienza a bloquear los eventos más frecuentes cuando el total de eventos recibidos excede el límite especificado para la base de datos.

El Servidor de administración bloquea la recepción automática de eventos frecuentes. No puede bloquear los eventos frecuentes usted, mismo ni elegir qué eventos bloquear.

Si desea saber si un evento está bloqueado, puede comprobar si está presente en la sección **Bloqueo de eventos frecuentes** de las propiedades del Servidor de administración. Si el evento está bloqueado, puede hacer lo siguiente:

- Si desea impedir que se sobrescriba la base de datos, puede continuar bloqueando la recepción de este tipo de eventos.
- Si desea, por ejemplo, encontrar el motivo del envío de los eventos frecuentes al Servidor de administración puede desbloquear los eventos frecuentes y seguir recibiendo los eventos de este tipo de todos modos.
- Si desea seguir recibiendo los eventos frecuentes hasta que se los vuelva a bloquear, puede eliminar el bloqueo de eventos frecuentes.

Gestión del bloqueo de eventos frecuentes

El Servidor de administración bloquea automáticamente la recepción de eventos frecuentes, pero usted puede dejar sin efecto el bloqueo y continuar recibiendo eventos frecuentes. También puede bloquear la recepción de eventos frecuentes que desbloqueó antes.

Para gestionar el bloqueo de eventos frecuentes:

1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, vaya al panel **Secciones** y luego seleccione **Bloqueo de eventos frecuentes**.
3. En la sección **Bloqueo de eventos frecuentes**:

- Seleccione las opciones de **Tipo de evento** de los eventos que desea bloquear para no recibirlos.
- Anule la selección de las opciones de **Tipo de evento** de los eventos que desea seguir recibiendo.

4. Haga clic en el botón **Aplicar**.
5. Haga clic en el botón **Aceptar**.

El Servidor de administración recibe los eventos frecuentes para los que seleccionó la opción **Tipo de evento** y bloquea la recepción de los eventos frecuentes para los que seleccionó la opción **Tipo de evento**.

Eliminación del bloqueo de eventos frecuentes

Puede eliminar el bloqueo de los eventos frecuentes y comenzar a recibirlos hasta que el Servidor de administración vuelva a bloquear este tipo de eventos frecuentes.

Para eliminar el bloqueo de eventos frecuentes:

1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, vaya al panel **Secciones** y luego seleccione **Bloqueo de eventos frecuentes**.
3. En la sección **Bloqueo de eventos frecuentes**, haga clic en la fila del evento frecuente cuyo bloqueo desea eliminar.
4. Haga clic en el botón **Eliminar**.

El evento frecuente se elimina de la lista de eventos frecuentes. El Servidor de administración recibirá eventos de este tipo.

Exportación de una lista de eventos frecuentes a un archivo

Para exportar la lista de eventos frecuentes a un archivo, haga lo siguiente:

1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, vaya al panel **Secciones** y luego seleccione **Bloqueo de eventos frecuentes**.
3. Haga clic en el botón **Exportar a archivo**.
4. En la ventana **Guardar como** que se abre, especifique la ruta del archivo donde quiere guardar la lista.
5. Haga clic en el botón **Guardar**.

Todos los registros de la lista de eventos frecuentes se exportan a un archivo.

Controlar los cambios en el estado de las máquinas virtuales

El Servidor de administración almacena información sobre el estado de los dispositivos administrados, como el registro de hardware y la lista de las aplicaciones instaladas, así como la configuración de las aplicaciones administradas, las tareas y las directivas. Si una máquina virtual funciona como un dispositivo administrado, el usuario puede restaurar su estado en cualquier momento mediante una instantánea (creada anteriormente) de la máquina virtual. La información sobre el estado de la máquina virtual en el Servidor de administración podría quedar desfasada.

Por ejemplo, el administrador había creado una política de protección en el Servidor de administración a las 00:00 h., que comenzó a ejecutarse en la máquina virtual VM_1 a las 00:01 h. A las 00:30 h, el usuario de la máquina virtual VM_1 cambió el estado de la misma restableciéndola a partir de una instantánea realizada a las 11:00 h. La política de protección deja de ejecutarse en la máquina virtual. Sin embargo, la información desfasada guardada en el Servidor de administración indica que la directiva de protección de la máquina virtual VM_1 sigue en ejecución.

Kaspersky Security Center le permite supervisar cambios de estado de máquinas virtuales.

Después de cada sincronización con un dispositivo, el Servidor de administración genera un identificador exclusivo que se guarda en el dispositivo y en el Servidor de administración. Antes de que comience la siguiente sincronización, el Servidor de administración compara los valores de los identificadores en ambos extremos. Si los valores de los identificadores no coinciden, el Servidor de administración reconoce la máquina virtual como restaurada a partir de una instantánea. El Servidor de administración restablece todos los parámetros de las directivas y las tareas que están activas para la máquina virtual, y envía a esa máquina las directivas actualizadas y la lista de tareas de grupo.

Supervisión del estado de la protección antivirus mediante información del registro del sistema

Para supervisar el estado de protección antivirus en un dispositivo cliente mediante la información registrada por el Agente de red, según el sistema operativo del dispositivo, realice lo siguiente:

- En dispositivos con Windows:

  1. Abra el registro del sistema de un dispositivo cliente (por ejemplo, localmente, mediante el comando regedit del menú **Iniciar** → **Ejecutar**).

  2. Vaya al siguiente subárbol:

     - Sistemas de 32 bits:

       ```
       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVSt
       ```

     - Sistemas de 64 bits:

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

     El registro del sistema mostrará información sobre el estado de protección antivirus del dispositivo cliente.

- En dispositivos con Linux:

  - La información se adjunta en archivos de texto separados, uno para cada tipo de datos, que se encuentran en /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- En dispositivos con macOS:
  - La información se adjunta en archivos de texto separados, uno para cada tipo de datos, que se encuentran en /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

El estado de protección antivirus se corresponde con los valores de las claves descritos en la tabla inferior.

Claves de registro y sus valores posibles

Clave (tipo de datos)	Valor	Descripción
`Protection_LastConnected (REG_SZ)`	MM/DD/AAAA HH-MM-SS	Fecha y hora (en formato UTC) de la última conexión con el Servidor de administración
`Protection_AdmServer (REG_SZ)`	IP, nombre DNS o nombre NetBIOS	Nombre del Servidor de administración virtual que administra el dispositivo
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	Número de compilación del Agente de red instalado en el dispositivo
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (parche1; parche2; ...; parcheN)	Número completo de la versión del Agente de red (con parches) instalada en el dispositivo
`Protection_HostId (REG_SZ)`	ID del dispositivo	ID del dispositivo
`Protection_DynamicVM (REG_DWORD)`	0 — no 1 — sí	El Agente de red se instala en el modo dinámico para VDI
`Protection_AvInstalled (REG_DWORD)`	0 — no 1 — sí	Una aplicación de seguridad se instala en el dispositivo móvil
`Protection_AvRunning (REG_DWORD)`	0 — no 1 — sí	La protección en tiempo real está activa en el dispositivo
`Protection_HasRtp (REG_DWORD)`	0 — no 1 — sí	Un componente de protección en tiempo real está instalado
`Protection_RtpState (REG_DWORD)`	Estado de protección en tiempo real:	
	0	Desconocido
	1	Desactivado
	2	En pausa
	3	Iniciando
	4	Activado
	5	Activado con el nivel de protección alto (protección máxima)
	6	Activado con el nivel de protección bajo (velocidad máxima)
	7	Activado con la configuración predeterminada (recomendada)
	8	Activado con la configuración personalizada
	9	Fallo de funcionamiento
`Protection_LastFscan (REG_SZ)`	MM/DD/AAAA HH-MM-SS	Fecha y hora (en formato UTC) del último análisis completo

`Protection_BasesDate (REG_SZ)`	MM/DD/AAAA HH-MM-SS	Fecha y hora (en formato UTC) de la publicación de las bases de datos de la aplicación

Ver y configurar las acciones cuando los dispositivos muestran inactividad

Si los dispositivos cliente dentro de un grupo están inactivos, puede recibir notificaciones al respecto. También puede eliminar automáticamente dichos dispositivos.

Para ver o configurar las acciones cuando los dispositivos del grupo muestran inactividad:

1. En el árbol de la consola, haga clic con el botón derecho en el nombre del grupo de administración requerido.
2. En el menú contextual, seleccione **Propiedades**.

   Esto abre la ventana de propiedades del grupo de administración.
3. En la ventana **Propiedades**, vaya a la sección **Dispositivos**.
4. De ser necesario, active o desactive las opciones siguientes:

   - Notificar al administrador si el dispositivo ha estado inactivo durante más de (días)

     Si esta opción está activada, el administrador recibe notificaciones sobre dispositivos inactivos. Puede especificar el intervalo de tiempo después del cual se crea el **dispositivo inactivo en la red en un evento de larga duración**. De forma predeterminada, el intervalo de tiempo es 7 día.

     Esta opción está activada de forma predeterminada.

   - Quitar el dispositivo del grupo si ha estado inactivo durante más de (días)

     Si esta opción está activada, puede especificar el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo. De forma predeterminada, el intervalo de tiempo es 60 día.

     Esta opción está activada de forma predeterminada.

   - Heredar del grupo primario

     La configuración en esta sección se heredará del grupo primario en el que se incluye el dispositivo cliente. Si esta opción está activada, la configuración de **Actividad de los dispositivos en la red** se bloquea de cualquier cambio.

     Esta opción está disponible solo si el grupo de administración tiene un grupo primario.

     Esta opción está activada de forma predeterminada.

   - Forzar herencia en grupos secundarios

     Los valores de configuración se distribuirán a grupos secundarios, pero en las propiedades de los grupos secundarios estas configuraciones están bloqueadas.

     Esta opción está desactivada de forma predeterminada.

5. Haga clic en **Aceptar**.

Sus cambios están guardados y aplicados.

Desactivación de anuncios de Kaspersky

En Kaspersky Security Center 14 Web Console, la sección Anuncios de Kaspersky (**SUPERVISIÓN E INFORMES** → **Anuncios de Kaspersky**) le mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas que están instaladas en los dispositivos administrados. Si no desea recibir anuncios de Kaspersky, puede desactivar esta función.

Los anuncios de Kaspersky incluyen dos tipos de información: anuncios relacionados con seguridad y anuncios de marketing. Puede desactivar los anuncios de cada tipo por separado.

Para desactivar los anuncios relacionados con seguridad:

1. En el árbol de la consola, seleccione el Servidor de administración para el que desea desactivar los anuncios relacionados con la seguridad.
2. Haga clic derecho y en el menú contextual que aparece, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración que se abre, en la sección **Anuncios de Kaspersky**, desactive la opción **Habilitar la visualización de anuncios de Kaspersky en Kaspersky Security Center 14 Web Console**.
4. Haga clic en **Aceptar**.

Los anuncios de Kaspersky están desactivados.

Los anuncios de marketing están deshabilitados de forma predeterminada. Solo recibirá anuncios de marketing si habilitó Kaspersky Security Network (KSN). Puede desactivar KSN para desactivar este tipo de anuncios.

Ajuste de puntos de distribución y puertas de enlace de conexión

Una estructura de grupos de administración en Kaspersky Security Center realiza las funciones siguientes:

- Configura la cobertura de las directivas

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de *perfiles de directiva*. En este caso, define la cobertura de directivas mediante etiquetas, ubicaciones del dispositivo en unidades organizativas de Active Directory o pertenencia a grupos de seguridad de Active Directory.

- Configura la cobertura de las tareas de grupo

  Existe un enfoque para definir la cobertura de las tareas de grupo que no se basan en una jerarquía de los grupos de administración: el uso de tareas para selecciones de dispositivos y tareas para dispositivos específicos.

- Configura los derechos de acceso a dispositivos, Servidores de administración virtuales y Servidores de administración secundarios

- Asigna puntos de distribución

Al construir la estructura de los grupos de administración, debe tener en cuenta la topología de la red de la organización para la asignación óptima de puntos de distribución. La distribución óptima de los puntos de distribución le permite ahorrar tráfico de la red de la organización.

Según el organigrama y la topología de red de la organización, se pueden aplicar las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única
- Varias oficinas remotas pequeñas

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Configuración estándar de puntos de distribución: oficina única

En una configuración de "oficina única" estándar, todos los dispositivos están dentro de la red de la organización. La red de la organización puede consistir en unas partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

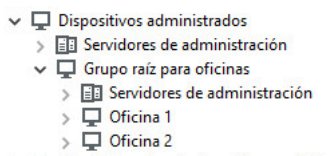
Los métodos siguientes de crear la estructura de grupos de administración son posibles:

- Crear la estructura de grupos de administración tomando en consideración la topología de red. La estructura de grupos de administración puede no reflejar la topología de red con precisión absoluta. Una coincidencia entre las partes independientes de la red y ciertos grupos de administración sería suficiente. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.
- La creación de la estructura de grupos de administración, sin tomar la topología de red en cuenta. En este caso, debe desactivar la asignación automática de puntos de distribución y luego asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración de raíz en cada una de las partes independientes de la red, por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán al mismo nivel y presentarán la misma cobertura que abarca a todos los dispositivos en la red de la organización. En este caso, cada Agente de red en la versión 10 Service Pack 1 o posterior se conectará con el punto de distribución que tenga la ruta más corta. La ruta a un punto de distribución se puede rastrear con la herramienta tracert.

Configuración estándar de los puntos de distribución: varias oficinas remotas pequeñas

Esta configuración estándar sirve para varias pequeñas oficinas remotas, que se pueden comunicar con la oficina central mediante Internet. Cada oficina remota está ubicada detrás de la NAT, es decir, la conexión de una oficina remota a otra no es posible porque las oficinas están aisladas la una de la otra.

La configuración se debe reflejar en la estructura de los grupos de administración: se debe crear un grupo de administración independiente para cada oficina remota (grupos **Oficina 1** y **Oficina 2** en la imagen a continuación).



Las oficinas remotas se incluyen en la estructura del grupo de administración

Se deben asignar uno o varios puntos de distribución a cada grupo de administración que corresponda a una oficina. Los puntos de distribución deben ser dispositivos en la oficina remota que tienen una cantidad suficiente de espacio libre en disco. Los dispositivos desplegados en el grupo **Oficina 1**, por ejemplo, accederán a los puntos de distribución asignados al grupo de administración de **Oficina 1**.

Si algunos usuarios se mueven entre oficinas físicamente con sus equipos portátiles, debe seleccionar dos o más dispositivos (además de los puntos de distribución existentes) en cada oficina remota y asignarlos para que funcionen como puntos de distribución para un grupo de administración de alto nivel (**Grupo raíz para oficinas** en la imagen anterior).

Ejemplo: Un equipo portátil se despliega en el grupo de administración de la **Oficina 1** y luego se mueve físicamente a la oficina que corresponde al grupo de administración de la **Oficina 2**. Después de que se mueve el equipo portátil, el Agente de red intenta acceder a los puntos de distribución asignados al grupo de la **Oficina 1**, pero esos puntos de distribución no están disponibles. Entonces, el Agente de red empieza a intentar acceder a los puntos de distribución que se han asignado al **Grupo raíz para oficinas**. Como las oficinas remotas están aisladas la una de la otra, los intentos de acceder a los puntos de distribución asignados al grupo de administración del **Grupo raíz para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución en el grupo de la **Oficina 2**. Es decir, el equipo portátil permanecerá en el grupo de administración que corresponde a la oficina inicial, pero el equipo portátil usará el punto de distribución de la oficina donde físicamente se ubica en este momento.

Asignación de un dispositivo administrado para actuar como punto de distribución

Puede asignar manualmente un dispositivo para que actúe como punto de distribución de un grupo de administración y configurarlo como puerta de enlace de conexión de la Consola de administración.

Para asignar un dispositivo como punto de distribución de un grupo de administración:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Puntos de distribución**.
4. En la parte derecha de la ventana, seleccione la opción **Asignar manualmente puntos de distribución**.
5. Haga clic en el botón **Agregar**.

   De este modo, se abre la ventana **Agregar un punto de distribución**.
6. En la ventana **Agregar un punto de distribución**, realice las siguientes acciones:

   a. En **Dispositivo que actuará como punto de distribución**, haga clic en la flecha hacia abajo en el botón de división **Seleccionar** y seleccione la opción **Agregar dispositivo del grupo**.

   b. En la ventana **Seleccionar dispositivos** que se abre, seleccione el dispositivo que actuará como punto de distribución.

   c. En **Alcance del punto de distribución**, haga clic en la flecha hacia abajo en el botón de división **Seleccionar**.

   d. Indique los dispositivos específicos a los que el punto de distribución distribuirá actualizaciones. Puede especificar un grupo de administración o una descripción de ubicación de red.

e. Haga clic **Aceptar** para cerrar la ventana **Agregar un punto de distribución**.

El punto de distribución que ha añadido se mostrará en la lista de puntos de distribución, en la sección **Puntos de distribución**.

El primer dispositivo con Agente de red instalado que se conecta al Servidor de administración virtual se asignará automáticamente para que actúe como punto de distribución y se configure como puerta de enlace de conexión.

Conexión de un nuevo segmento de red mediante dispositivos Linux

Puede conectar un nuevo segmento de red en un dispositivo Linux. Necesita al menos dos dispositivos diferentes. Puede configurar un dispositivo como puerta de enlace de conexión en la DMZ; y el otro, como punto de distribución.

Siga el procedimiento descrito en esta sección solo después de haber completado el escenario de instalación principal.

Para conectar un nuevo segmento de red en un dispositivo Linux:

1. Conecte un dispositivo Linux como puerta de enlace en la DMZ.
2. Conecte un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión.

Se configura la conexión de un nuevo segmento de red en un dispositivo Linux.

Conexión de un dispositivo Linux como puerta de enlace en la zona desmilitarizada

Para conectar un dispositivo Linux como puerta de enlace en la zona desmilitarizada (DMZ):

1. Descargue e instale el Agente de red en el dispositivo Linux.
2. Ejecute el script posterior a la instalación y siga el Asistente para configurar el entorno local. En el símbolo del sistema, ejecute el siguiente comando:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```
3. En el paso que solicita el modo Agente de red, elija la opción **Usar como puerta de enlace de conexión**.
4. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Puntos de distribución**.
5. En la ventana **Puntos de distribución** que se abre, en la parte derecha de la ventana:
   a. Seleccione la opción **Asignar manualmente puntos de distribución**.
   b. Haga clic en el botón **Agregar**.

   De este modo, se abre la ventana **Agregar un punto de distribución**.

6. En la ventana **Agregar un punto de distribución**, realice las siguientes acciones:

   a. En **Dispositivo que actuará como punto de distribución**, haga clic en la flecha hacia abajo en el botón de división **Seleccionar** y después seleccione la opción **Añadir puerta de enlace de conexión en DMZ por dirección**.

   b. En **Alcance del punto de distribución**, haga clic en la flecha hacia abajo en el botón de división **Seleccionar**.

   c. Indique los dispositivos específicos a los que el punto de distribución distribuirá actualizaciones. Puede especificar un grupo de administración.

   d. Haga clic **Aceptar** para cerrar la ventana **Agregar un punto de distribución**.

7. El punto de distribución que ha añadido se mostrará en la lista de puntos de distribución, en la sección **Puntos de distribución**.

8. Ejecute la utilidad klnagchk para comprobar si la conexión a Kaspersky Security Center se ha configurado correctamente. En el símbolo del sistema, ejecute:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

9. En la ventana principal de la aplicación, vaya a Kaspersky Security Center y descubra el dispositivo.

10. En la ventana que se abre, haga clic en el <Nombre del dispositivo>.

11. En la lista desplegable, seleccione el enlace **Mover al grupo**.

12. En la ventana **Seleccionar grupo** que se abre, haga clic en el enlace **Puntos de distribución**.

13. Haga clic en **Aceptar**.

14. Reinicie el servicio del Agente de red en el cliente Linux. Para hacerlo, ejecute el siguiente comando en el símbolo del sistema:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

Queda lista la conexión del dispositivo Linux como puerta de enlace en DMZ.

Conexión de un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión

Para conectar un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión, realice las siguientes acciones en este dispositivo:

1. Descargue e instale el Agente de red en el dispositivo Linux.

2. Ejecute el script posterior a la instalación del Agente de red. Para hacerlo, ejecute el siguiente comando en el símbolo del sistema:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. En el paso que pregunta el modo de Agente de red, elija la opción **Conectar al servidor usando la puerta de enlace de conexión** y escriba la dirección de la puerta de conexión.

4. Verifique la conexión con Kaspersky Security Center y la puerta de enlace de conexión, mediante el siguiente comando en el símbolo del sistema:

```
$ sudo /opt/kaspersky/klnagent64/bin/klnagchk
```

La dirección de la puerta de enlace de conexión se muestra en la salida.

La conexión de un dispositivo Linux al Servidor de administración a través de una puerta de enlace de conexión estará completa. Puede usar este dispositivo para actualizar la distribución, para la instalación remota de aplicaciones y para recuperar información sobre dispositivos en red.

Adición de una puerta de enlace de conexión en la DMZ como punto de distribución

Una puerta de enlace de conexión espera las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración. Por lo tanto, justo después de instalar una puerta de enlace de conexión en un dispositivo en la DMZ, el Servidor de administración no enumera el dispositivo entre los dispositivos administrados. Por lo tanto, necesita un procedimiento especial para asegurarse de que el Servidor de administración inicie una conexión con la puerta de enlace de conexión.

Para añadir un dispositivo con una puerta de enlace de conexión como punto de distribución:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Puntos de distribución**.
4. En la parte derecha de la ventana, seleccione la opción **Asignar manualmente puntos de distribución**.
5. Haga clic en el botón **Agregar**.

   De este modo, se abre la ventana **Agregar un punto de distribución**.
6. En la ventana **Agregar un punto de distribución**, realice las siguientes acciones:

   a. En **Dispositivo que actuará como punto de distribución**, haga clic en la flecha hacia abajo en el botón de división **Seleccionar** y después seleccione la opción **Agregar puerta de enlace de conexión en DMZ por dirección**.

   b. En la ventana **Escriba la dirección de la puerta de enlace de conexión** que se abre, introduzca la dirección IP de la pasarela de conexión (o introduzca el nombre si se puede acceder a la puerta de enlace de conexión por su nombre).

   c. En **Alcance del punto de distribución**, haga clic en la flecha hacia abajo en el botón de división **Seleccionar**.

   d. Indique los dispositivos específicos a los que el punto de distribución distribuirá actualizaciones. Puede especificar un grupo de administración o una descripción de ubicación de red.

      Le recomendamos que tenga un grupo separado para los dispositivos administrados externos.

Después de realizar estas acciones, la lista de puntos de distribución contiene una nueva entrada denominada **Entrada temporal para puerta de enlace de conexión**.

Casi de inmediato, el Servidor de administración intenta conectarse a la puerta de enlace de conexión en la dirección que ha especificado. Si tiene éxito, el nombre de la entrada cambia al nombre del dispositivo de puerta de enlace de conexión. Este proceso tarda hasta 5 minutos.

Mientras que la entrada temporal para la puerta de enlace de conexión se convierte en una entrada con nombre, la puerta de enlace de conexión también aparece en el grupo **Dispositivos no asignados**.

Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. Kaspersky Security Center seleccionará por sí mismo a qué dispositivos se les deben asignar puntos de distribución.

Para asignar puntos de distribución automáticamente:

1. Abra la ventana principal de la aplicación.
2. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración para el que desea asignar puntos de distribución automáticamente.
3. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
4. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Puntos de distribución**.
5. En la parte derecha de la ventana, seleccione la opción **Asignar automáticamente puntos de distribución**.

   Si la asignación automática de dispositivos para que actúen como puntos de distribución está activada, no se pueden configurar los puntos de distribución manualmente ni editar la lista de puntos de distribución.

6. Haga clic en **Aceptar**.

El Servidor de administración asigna y configura puntos de distribución automáticamente.

Acerca de la instalación local del Agente de red en un dispositivo seleccionado como punto de distribución

Para permitir que el dispositivo seleccionado como punto de distribución se comunique directamente con el Servidor de administración virtual para actuar como puerta de enlace de conexión, el Agente de red debe estar instalado localmente en ese dispositivo.

El procedimiento de instalación local del Agente de red en el dispositivo definido como punto de distribución es igual a la instalación local del Agente de red en cualquier dispositivo de red.

Un dispositivo seleccionado como punto de distribución debe cumplir las siguientes condiciones:

- Durante la instalación local del Agente de red, en el campo **Dirección del servidor** de la ventana **Servidor de administración** del Asistente de instalación, especifique la dirección del Servidor de administración virtual que administra el dispositivo. Puede utilizar tanto la dirección IP del dispositivo como el nombre del dispositivo en la red de Windows.

  Se utiliza el siguiente formato para la dirección del Servidor de administración virtual: <Dirección completa del Servidor de administración físico al que se subordina el servidor virtual>/<Nombre del Servidor de administración virtual>.

- Para que pueda servir de pasarela de conexión, abra todos los puertos del dispositivo que sean necesarios para la comunicación con el Servidor de administración.

Después de haber instalado en el dispositivo el Agente de red con la configuración especificada, Kaspersky Security Center realiza las siguientes acciones de forma automática:

- Incluye este dispositivo en el grupo **Dispositivos administrados** del Servidor de administración virtual.
- Designa este dispositivo como punto de distribución del grupo **Dispositivos administrados** del Servidor de administración virtual.

Es necesario y suficiente instalar localmente el Agente de red en el dispositivo designado como punto de distribución para el grupo **Dispositivos administrados** en la red corporativa. Puede instalar el Agente de red de forma remota en los dispositivos que actúan como puntos de distribución en los grupos de administración anidados. Para ello, use el punto de distribución del grupo **Dispositivos administrados** como puerta de enlace de conexión.

Acerca del uso de un punto de distribución como puerta de enlace de conexión

Si el Servidor de administración se encuentra fuera de la zona desmilitarizada (DMZ), los Agentes de red de esta zona no se podrán conectar al Servidor de administración.

Al conectar al Servidor de administración con los Agentes de red, puede utilizar un punto de distribución como puerta de enlace de conexión. El punto de distribución abre un puerto al Servidor de administración para establecer la conexión. Cuando se inicia el Servidor de administración, se conecta a dicho punto de distribución y permanece conectado durante toda la sesión.

Al recibir una señal del Servidor de administración, el punto de distribución envía una señal UDP a los Agentes de red para permitir la conexión al Servidor de administración. Cuando los agentes de red reciben esa señal, se conectan al punto de distribución, que transfiere información entre los Agentes de red y el Servidor de administración. El intercambio de información se puede producir a través de una red IPv4 o IPv6.

Recomendamos que use un dispositivo especialmente asignado como la puerta de enlace de conexión y cubra un máximo de 10.000 dispositivos cliente (incluidos los dispositivos móviles) con esta puerta de enlace de conexión.

Añadir rangos IP a la lista de rangos analizados de un punto de distribución

Puede añadir rangos IP a la lista de rangos explorados de un punto de distribución.

Para añadir un rango de IP a la lista de rangos analizados:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. En el menú contextual del nodo, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Puntos de distribución**.
4. En la lista, seleccione el punto de distribución necesario y haga clic en **Propiedades**.

5. En la ventana de propiedades del punto de distribución que se abre, en el panel izquierdo **Secciones**, seleccione **Detección de dispositivos → Rangos IP**.

6. Selecciona la casilla de verificación **Activar sondeo del rango**.

7. Haga clic en el botón **Agregar**.

   El botón **Agregar** está activo solo si selecciona la casilla de verificación **Activar sondeo del rango**.

   Se abre la ventana **Rango IP**.

8. En la ventana de **Rango IP**, introduzca el nombre del nuevo rango de IP (el nombre predeterminado es Nuevo rango).

9. Haga clic en el botón **Agregar**.

10. Realice una de las siguientes acciones:

    - Especifique el rango de IP utilizando las direcciones IP de iniciales y finales.
    - Especifique el rango de IP utilizando la dirección y la máscara de subred.
    - Haga clic en **Examinar** y añada una subred de la lista global de subredes.

11. Haga clic en **Aceptar**.

12. Haga clic en **Aceptar** para añadir el nuevo rango con el nombre especificado.

El nuevo rango aparecerá en la lista de rangos analizados.

Uso de un punto de distribución como servidor push

En Kaspersky Security Center, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y los dispositivos gestionados por Agente de red. Por ejemplo, se debe activar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se activa el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede activar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

Un servidor push soporta la carga de hasta 50 000 conexiones simultáneas.

Se recomienda utilizar puntos de distribución como servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Se necesita conectividad continua para algunas operaciones, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Si utiliza un punto de distribución como servidor push, no es necesario utilizar la opción **No desconectar del Servidor de administración** en dispositivos administrados o enviar paquetes al puerto UDP del Agente de red.

Para usar un punto de distribución como servidor push:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.

2. En el menú contextual del nodo, seleccione **Propiedades**.

3. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Puntos de distribución**.
4. En la lista, seleccione el punto de distribución necesario y, luego, haga clic en **Propiedades**.
5. En la ventana de propiedades del punto de distribución que se abre, en la sección **General** del panel izquierdo **Secciones**, seleccione la opción **Use este punto de distribución como servidor push**.
6. Especifique el número de puerto del servidor push, es decir, el puerto del punto de distribución que los dispositivos cliente utilizarán para conectarse.

   De forma predeterminada, se utiliza el puerto 13295.
7. Haga clic en el botón **Puntos de distribución** para salir de la ventana de propiedades del punto de distribución.
8. Abra la ventana de configuración de la directiva del Agente de red.
9. En la sección **Conectividad**, vaya a la subsección **Red**.
10. En la subsección **Red**, seleccione la opción **Utilice el punto de distribución para forzar la conexión con el Servidor de administración**.
11. Haga clic en el botón **Aceptar** para salir de la ventana.

El punto de distribución funcionará como servidor push. Ya puede enviar notificaciones push a los dispositivos cliente.

Si administra dispositivos con KasperskyOS instalado, o tiene pensado hacerlo, debe utilizar un punto de distribución como servidor push. También puede utilizar un punto de distribución como servidor push si desea enviar notificaciones push a los dispositivos cliente.

Otro trabajo de rutina

Esta sección proporciona recomendaciones sobre el trabajo rutinario con Kaspersky Security Center.

Gestión de los Servidores de administración

Esta sección proporciona información sobre la forma de configurar y trabajar con los Servidores de administración.

Creación de una jerarquía de Servidores de administración: adición de un Servidor de administración secundario

Puede añadir un Servidor de administración como Servidor de administración secundario, y establecer así una jerarquía "principal/secundario". Es posible añadir un Servidor de administración secundario independientemente de si el Servidor de administración que tiene la intención de usar como secundario está disponible para conectarlo mediante la Consola de administración.

Cuando combine dos Servidores de administración en una jerarquía, asegúrese de que el puerto 13291 esté accesible en ambos Servidores de administración. Se requiere el puerto 13291 para recibir conexiones de la Consola de administración al Servidor de administración.

Conexión de un Servidor de administración como secundario vinculado al Servidor de administración principal

Puede añadir un Servidor de administración secundario conectándolo al Servidor de administración principal a través del puerto 13000. Necesitará un dispositivo que tenga la Consola de administración instalada desde la cual se pueda acceder a los puertos TCP 13291 en ambos Servidores de administración: Servidor de administración principal supuesto y Servidor de administración secundario supuesto.

Para añadir un Servidor de administración secundario que se pueda conectar mediante la Consola de administración:

1. Asegúrese de que el puerto 13000 del supuesto Servidor de administración principal esté disponible para la recepción de conexiones desde los Servidores de administración secundarios.
2. Use la Consola de administración para conectarse al supuesto Servidor de administración principal.
3. Seleccione el grupo de administración al que desea añadir el Servidor de administración secundario.
4. En el espacio de trabajo del nodo **Servidores de administración** del grupo seleccionado, haga clic en el enlace **Agregar Servidor de administración secundario**.

   Inicia el Asistente para agregar un Servidor de administración secundario.
5. En el primer paso del Asistente (introduciendo la dirección del Servidor de administración que se añade al grupo), introduzca el nombre de la red del Servidor de administración secundario supuesto.
6. Siga las instrucciones del Asistente.

Se construye la jerarquía "principal/secundario". El Servidor de administración principal recibirá la conexión del Servidor de administración secundario.

Si no tiene un dispositivo que tenga la Consola de administración instalada desde la que acceder a los puertos TCP 13291 en ambos Servidores de administración (si, por ejemplo, el Servidor de administración secundario supuesto se encuentra en una oficina remota y el administrador del sistema de esa oficina no puede abrir el acceso a Internet al puerto 13291 por razones de seguridad), todavía podrá añadir un Servidor de administración secundario.

Para añadir como secundario un Servidor de administración que no se pueda conectar mediante la Consola de administración:

1. Asegúrese de que el puerto 13000 del Servidor de administración principal supuesto esté disponible para conectarse desde los Servidores de administración secundarios.
2. Escriba el archivo de certificado del supuesto Servidor de administración principal en un dispositivo externo, como una unidad flash o envíelo al administrador del sistema de la oficina remota donde se encuentra el Servidor de administración.

   El archivo del certificado del Servidor de administración está en el mismo Servidor de administración, en %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.
3. Escriba el archivo del certificado del Servidor de administración secundario supuesto y guárdelo en un dispositivo externo, como una unidad flash. Si el Servidor de administración secundario supuesto se encuentra en una oficina remota, comuníquese con el administrador del sistema de esa oficina para solicitar que le envíe el certificado.

El archivo del certificado del Servidor de administración está en el mismo Servidor de administración, en %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Use la Consola de administración para conectarse al supuesto Servidor de administración principal.

5. Seleccione el grupo de administración al que desea añadir el Servidor de administración secundario.

6. En el espacio de trabajo del nodo **Servidores de administración**, haga clic en el botón **Agregar Servidor de administración secundario**.

   Inicia el Asistente para agregar un Servidor de administración secundario.

7. En el primer paso del Asistente (introducir la dirección), deje el campo **Dirección del Servidor de administración secundario (opcional)** en blanco.

8. En la ventana **Archivo del certificado del Servidor de administración secundario**, haga clic en el botón **Examinar** y seleccione el archivo del certificado del Servidor de administración secundario que guardó.

9. Cuando el Asistente se haya completado, use una instancia diferente de la Consola de administración para conectar al Servidor de administración secundario supuesto. Si este Servidor de administración se encuentra en una oficina remota, comuníquese con el administrador del sistema de esa oficina para solicitar que se conecte al Servidor de administración secundario supuesto y avance con los pasos.

10. En el menú contextual del nodo **Servidor de administración**, seleccione **Propiedades**.

11. En las propiedades del Servidor de administración, vaya a la sección **Avanzado** y, a continuación, a la subsección **Jerarquía de Servidores de administración**.

12. Selecciona la casilla de verificación **Este Servidor de administración es secundario en la jerarquía**.

    Los campos de entrada están disponibles para la introducción y edición de datos.

13. En el campo **Dirección del Servidor de administración principal**, introduzca el nombre de la red del Servidor de administración principal supuesto.

14. Seleccione el archivo previamente guardado con el certificado del Servidor de administración principal supuesto haciendo clic en el botón **Examinar**.

15. Haga clic en **Aceptar**.

Se construye la jerarquía "principal/secundario". Puede conectarse al Servidor de administración secundario mediante la Consola de administración. El Servidor de administración principal recibirá la conexión del Servidor de administración secundario.

Conexión del Servidor de administración principal a un Servidor de administración secundario

Puede añadir un nuevo Servidor de administración secundario para que el Servidor de administración principal se conecte al Servidor de administración secundario a través del puerto 13000. Esto es recomendable si, por ejemplo, coloca un Servidor de administración secundario en una DMZ.

Necesitará un dispositivo que tenga la Consola de administración instalada desde la cual se pueda acceder a los puertos TCP 13291 en ambos Servidores de administración: Servidor de administración principal supuesto y Servidor de administración secundario supuesto.

Para añadir un nuevo Servidor de administración secundario y conectar el Servidor de administración principal a través del puerto 13000:

1. Asegúrese de que el puerto 13000 del Servidor de administración secundario supuesto esté disponible para la recepción de conexiones desde el Servidor de administración principal.

2. Use la Consola de administración para conectarse al supuesto Servidor de administración principal.

3. Seleccione el grupo de administración al que desea añadir el Servidor de administración secundario.

4. En el espacio de trabajo del nodo **Servidores de administración** del grupo de administración relevante, haga clic en el enlace **Agregar Servidor de administración secundario**.

   Inicia el Asistente para agregar un Servidor de administración secundario.

5. En el primer paso del Asistente (introduciendo la dirección del Servidor de administración que se añade al grupo), introduzca el nombre de la red del Servidor de administración secundario y seleccione la casilla de verificación **Conectar Servidor de administración principal a Servidor de administración secundario en DMZ**.

6. Si se conecta al Servidor de administración secundario supuesto usando un servidor proxy, en el primer paso del Asistente, marque la casilla **Usar servidor proxy** y especifique la configuración de la conexión.

7. Siga las instrucciones del Asistente.

Se crea la jerarquía de Servidores de administración. El Servidor de administración secundario recibirá la conexión del Servidor de administración principal.

Conexión a un Servidor de administración y cambio entre Servidores de administración

Después de iniciar Kaspersky Security Center, este intenta conectarse a un Servidor de administración. Si hay varios Servidores de administración disponibles en la red, la aplicación solicita el servidor al que se había conectado durante la sesión anterior de Kaspersky Security Center.

> Cuando la aplicación se inicia por primera vez después de su instalación, intenta conectarse al Servidor de administración especificado durante la instalación de Kaspersky Security Center.

Una vez establecida una conexión al Servidor de administración, el árbol de carpetas del Servidor se mostrará en el árbol de consola.

Si se han agregado varios Servidores de administración al árbol de consola, puede alternar entre ellos.

La Consola de administración es necesaria para trabajar con cada Servidor de administración. Antes de la primera conexión a un nuevo Servidor de administración, asegúrese de que el puerto 13291, que recibe conexiones desde la Consola de administración, esté abierto, así como todos los puertos restantes necesarios para la comunicación entre el Servidor de administración y otros componentes de Kaspersky Security Center.

Para conectarse a otro Servidor de administración, realice lo siguiente:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.

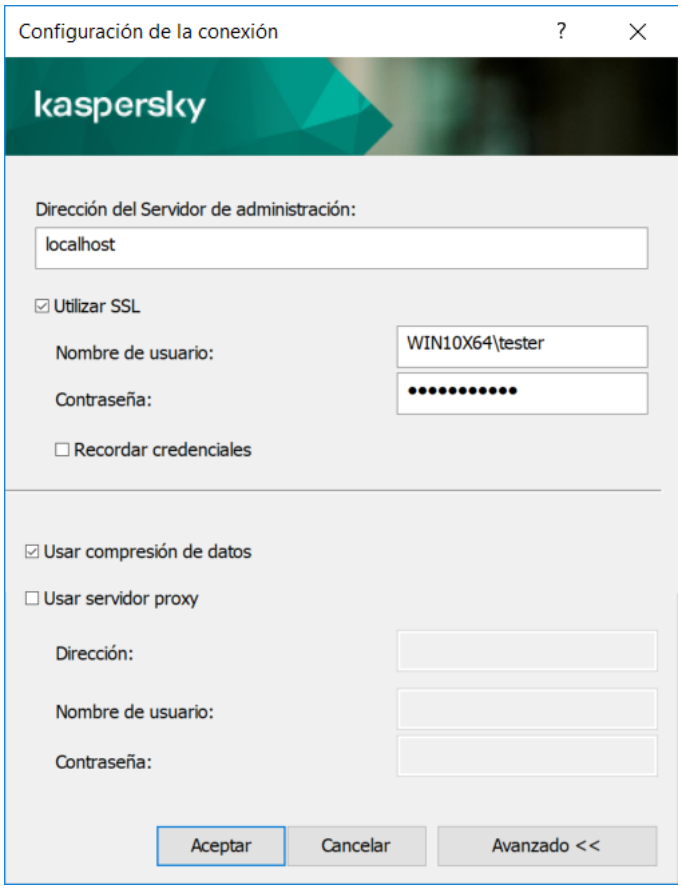
2. En el menú contextual del nodo, seleccione **Conectar al Servidor de administración**.

3. En la ventana **Configuración de la conexión** que se abrirá, en el campo **Dirección del Servidor de administración**, especifique el nombre del Servidor de administración al que quiera conectarse. En una red

Windows, se puede especificar una dirección IP o el nombre de un dispositivo como nombre del Servidor de administración. Puede hacer clic en el botón **Avanzado** para configurar la conexión al Servidor de administración (consulte la figura siguiente).

Para conectarse al Servidor de administración a través de un puerto que no sea el predeterminado, introduzca un valor en el campo **Dirección del Servidor de administración** con el formato <nombre del Servidor de administración>: <puerto>.

Los usuarios que no tengan derechos de **Leer** no tendrán acceso al Servidor de administración.



Conectando al Servidor de administración

4. Haga clic en **Aceptar** para completar el cambio entre los Servidores.

Después de conectar el Servidor de administración, se actualizará el árbol de carpetas del nodo correspondiente en el árbol de consola.

Derechos de acceso al Servidor de administración y sus objetos

Los grupos **KLAdmins** y **KLOperators** se crean automáticamente durante la instalación de Kaspersky Security Center. A estos grupos se les otorgan los permisos para conectarse al Servidor de administración y para trabajar con los objetos de este.

En función del tipo de cuenta que se utilice para la instalación de Kaspersky Security Center, los grupos **KLAdmins** y **KLOperators** se crean de la siguiente manera:

- Si se instala la aplicación con una cuenta de usuario incluida en un dominio, los grupos se crean en el Servidor de administración y en el dominio que incluye el Servidor de administración.

- Si se instala la aplicación en una cuenta del sistema, los grupos se crean únicamente en el Servidor de administración.

Mediante las herramientas administrativas estándar del sistema operativo, se pueden ver los grupos **KLAdmins** y **KLOperators** y modificar los privilegios de acceso de los usuarios que pertenecen a los grupos **KLAdmins** y **KLOperators**.

El grupo **KLAdmins** tiene todos los derechos de acceso y el grupo **KLOperators** solo tiene los derechos Leer y Ejecutar. Los derechos concedidos al grupo **KLAdmins** están bloqueados.

Los usuarios que pertenecen al grupo **KLAdmins** son *administradores de Kaspersky Security Center*; los usuarios del grupo **KLOperators** son *operadores de Kaspersky Security Center*.

Además de los usuarios incluidos en el grupo **KLAdmins**, también se otorgan derechos de administrador de Kaspersky Security Center a los administradores locales de los dispositivos en los que se haya instalado el Servidor de administración.

Se pueden excluir los administradores locales de la lista de usuarios con derechos de administrador de Kaspersky Security Center.

Todas las operaciones que inicien los administradores de Kaspersky Security Center se realizan usando los permisos de la cuenta del Servidor de administración.

Un grupo **KLAdmins** individual se puede crear para cada Servidor de administración de la red; el grupo tendrá los permisos necesarios solo para ese Servidor de administración.

Si dispositivos que pertenecen al mismo dominio están incluidos dentro de grupos de administración de diferentes Servidores de administración, entonces el administrador del dominio será el administrador de Kaspersky Security Center para todos los grupos. El grupo **KLAdmins** es común para estos grupos de administración; se crea durante la instalación del primer Servidor de administración. Todas las operaciones iniciadas por el administrador de Kaspersky Security Center se realizan con los derechos de cuenta del Servidor de administración para los que se han iniciado estas operaciones.

Después de instalar la aplicación, un administrador de Kaspersky Security Center puede hacer lo siguiente:

- Modificar los permisos concedidos a los grupos **KLOperators**.
- Otorgar derechos para acceder a la funcionalidad de Kaspersky Security Center a otros grupos de usuarios y a usuarios individuales registrados en la estación de trabajo del administrador.
- Asignar derechos de acceso a usuarios de cada grupo de administración.

El administrador de Kaspersky Security Center puede asignar derechos de acceso a cada grupo de administración o a otros objetos del Servidor de administración en la sección **Seguridad**, en la ventana de propiedades del objeto seleccionado.

Se puede rastrear la actividad de un usuario con los registros de los eventos en la operación del Servidor de administración. Los registros de eventos se muestran en el nodo **Servidor de administración** de la ficha **Eventos**. Estos eventos tienen el nivel de importancia **Eventos de información**; y los tipos de evento comienzan con "**Auditoría**".

Condiciones de conexión a un Servidor de administración a través de Internet

Si un Servidor de administración está ubicado remotamente fuera de una red corporativa, los dispositivos cliente se conectarán a este a través de Internet.

Para que los dispositivos se conecten a un Servidor de administración a través de Internet, se deben cumplir los siguientes requisitos:

- El Servidor de administración remoto deberá disponer de una dirección IP externa y el puerto de entrada 13000 deberá permanecer abierto (para la conexión de Agentes de red). Le recomendamos que también abra el puerto UDP 13000 (para recibir notificaciones cuando se apaguen los dispositivos).
- Primero deben instalarse los Agentes de red en los dispositivos.
- Al instalar el Agente de red en dispositivos, debe especificar la dirección IP externa del Servidor de administración remoto. Si se utiliza un paquete de instalación, especifique manualmente la dirección IP externa en las propiedades del paquete de instalación en la sección **Configuración**.
- Para usar el Servidor de administración remoto con el fin de administrar las aplicaciones y tareas de un dispositivo, en la ventana de propiedades de ese dispositivo, en la sección **General**, elija la casilla **No desconectar del Servidor de administración**. Una vez que la casilla está seleccionada, espere a que el Servidor de administración esté sincronizado con el dispositivo cliente remoto. El número de dispositivos cliente que mantienen una conexión continua con un Servidor de administración remoto no puede superar los 300.

Para aumentar el rendimiento de las tareas generadas por un Servidor de administración remoto, puede abrir el puerto 15000 en el dispositivo. En este caso, para ejecutar una tarea, el Servidor de administración envía un paquete especial al Agente de red a través del puerto 15000 sin esperar a que se complete la sincronización con el dispositivo.

Conexión cifrada con un Servidor de administración

El intercambio de datos entre los dispositivos cliente y el Servidor de administración, así como la conexión de la Consola de administración al Servidor de administración puede realizarse mediante el protocolo TLS (Transport Layer Security). El protocolo TLS puede identificar las partes integrantes, cifrar los datos que se transfieren y proteger estos contra cualquier modificación durante la transferencia. El protocolo TLS utiliza claves públicas para autenticar las partes integrantes y cifrar los datos.

Autenticación del Servidor de administración al conectarse un dispositivo

Cuando un dispositivo cliente se conecta al Servidor de administración por primera vez, el Agente de red del dispositivo cliente descarga una copia del certificado del Servidor de administración y la almacena localmente.

> Si instala el Agente de red localmente en un dispositivo, podrá seleccionar el certificado del Servidor de administración de forma manual.

La copia descargada del certificado se utiliza para verificar los permisos del Servidor de administración durante las siguientes conexiones.

En sesiones futuras, el Agente de red solicita el certificado del Servidor de administración en cada conexión del dispositivo al Servidor de administración y lo compara con la copia local. Si las copias no coinciden, el dispositivo no recibe permiso para acceder al Servidor de administración.

Autenticación del Servidor de administración durante la conexión de la Consola de administración

Durante la primera conexión al Servidor de administración, la Consola de administración solicita el certificado del Servidor de administración y lo guarda localmente en la estación de trabajo del administrador. Después, cada vez que la Consola de administración intente conectarse al Servidor de administración, este se identificará con la copia del certificado.

Si el certificado del Servidor de administración no coincide con la copia almacenada en la estación de trabajo del administrador, la Consola de administración le solicita confirmar la conexión con el Servidor de administración con el nombre especificado y descargar un certificado nuevo. Después de establecerse la conexión, la Consola de administración guarda una copia del nuevo certificado del Servidor de administración, que se utilizará para identificar el Servidor de administración en el futuro.

Configuración de una lista de admitidos de direcciones IP para conectarse al Servidor de administración

De manera predeterminada, los usuarios pueden iniciar sesión en Kaspersky Security Center desde cualquier dispositivo en el que puedan abrir Kaspersky Security Center 14 Web Console (en adelante, Web Console) o la Consola de administración basada en MMC. Sin embargo, puede configurar el Servidor de administración para que los usuarios puedan conectarse a él solo desde dispositivos con las direcciones IP permitidas. En este caso, incluso si un intruso roba una cuenta de Kaspersky Security Center, no podrá iniciar sesión en Kaspersky Security Center porque la dirección IP del dispositivo del intruso no está en la lista de permitidos.

La dirección IP se verifica cuando un usuario inicia sesión en Kaspersky Security Center o ejecuta una aplicación que interactúa con el Servidor de administración a través de Kaspersky Security Center OpenAPI. En este momento, el dispositivo de un usuario intenta establecer una conexión con el Servidor de administración. Si la dirección IP del dispositivo no está en la lista de admitidos, se produce un error de autenticación y el evento KLAUD_EV_SERVERCONNECT notifica que no se ha establecido una conexión con el Servidor de administración.

Requisitos para una lista de direcciones IP permitidas

Las direcciones IP se verifican solo cuando las siguientes aplicaciones intentan conectarse al Servidor de administración:

- Servidor de Web Console

  Si inicia sesión en Web Console en un dispositivo y el servidor de Web Console está instalado en otro dispositivo, puede configurar un cortafuegos en el dispositivo donde está instalado el servidor de Web Console utilizando los medios estándar del sistema operativo. Luego, si alguien intenta iniciar sesión en Web Console, un cortafuegos ayuda a evitar que los intrusos interfieran.

- Consola de administración

- Aplicaciones que interactúan con el Servidor de administración a través de objetos de automatización klakaut

- Aplicaciones que interactúan con el Servidor de administración a través de OpenAPI, como Kaspersky Anti Targeted Attack Platform o Kaspersky Security for Virtualization

Por lo tanto, especifique las direcciones de los dispositivos en los que están instaladas las aplicaciones enumeradas anteriormente.

Puede establecer direcciones IPv4 e IPv6. No puede especificar rangos de direcciones IP.

Cómo establecer una lista de direcciones IP permitidas

Si no ha establecido una lista de direcciones permitidas antes, siga las instrucciones a continuación.

Para establecer la lista de direcciones IP permitidas para iniciar sesión en Kaspersky Security Center, haga lo siguiente:

1. En el dispositivo del Servidor de administración, ejecute el símbolo del sistema con una cuenta con derechos de administrador.

2. Cambie su directorio actual a la carpeta de instalación de Kaspersky Security Center (generalmente, <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Ingrese el siguiente comando, usando derechos de administrador:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<direcciones IP>" -t s`

   Especifique direcciones IP que cumplan con los requisitos enumerados anteriormente. Las direcciones IP deben estar separadas por un punto y coma.

   Ejemplo de cómo permitir que solo un dispositivo se conecte al Servidor de administración:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Ejemplo de cómo permitir que varios dispositivos se conecten al Servidor de administración:

   `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" -t s`

4. Reinicie el servicio del Servidor de administración.

Puede averiguar si configuró correctamente la lista de direcciones IP permitidas en el Registro de eventos de Kaspersky en el Servidor de administración.

Cómo cambiar una lista de direcciones IP permitidas

Puede cambiar una lista de direcciones permitidas tal como lo hizo cuando la estableció por primera vez. Para ello, ejecute el mismo comando y especifique una nueva lista de permitidas:

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

Si desea eliminar algunas direcciones IP de la lista de admitidos, debe reescribirla. Por ejemplo, su lista de admitidos incluye las siguientes direcciones IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. Desea eliminar la dirección IP 198.51.100.0. Para hacer esto, introduzca el siguiente comando en el símbolo del sistema:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

No olvide reiniciar el servicio del Servidor de administración.

Cómo restablecer una lista de direcciones IP permitidas ya configurada

Para restablecer una lista de direcciones IP permitidas ya configurada:

1. Introduzca el siguiente comando en el símbolo del sistema, usando derechos de administrador:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Reinicie el servicio del Servidor de administración.

Después de hacerlo, las direcciones IP dejan de verificarse.

Uso de la utilidad klscflag para cerrar el puerto 13291

El puerto 13291 del Servidor de administración se usa para recibir conexiones desde las Consolas de administración. Este puerto está abierto de forma predeterminada. Si no desea utilizar la Consola de administración basada en MMC o la utilidad klakaut, puede cerrar este puerto mediante la utilidad klscflag. Esta utilidad cambia el valor del parámetro KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Para cerrar el puerto 13291:

1. Ejecute el siguiente comando en la línea de comandos:
   `klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`

2. Reinicie el servicio del Servidor de administración de Kaspersky Security Center.

   El puerto 13291 está cerrado.

Para comprobar si el puerto 13291 se ha cerrado correctamente:

Ejecute el siguiente comando en la línea de comandos:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Este comando devuelve el siguiente resultado:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

El valor `false` significa que el puerto está cerrado. De lo contrario, aparece el valor `true`.

Desconectar del Servidor de administración

Para desconectar del Servidor de administración:

1. En el árbol de consola, seleccione el nodo correspondiente al Servidor de administración del que se quiera desconectar.

2. En el menú contextual del nodo, seleccione **Desconectar del Servidor de administración**.

Adición de un Servidor de administración al árbol de consola

Para agregar un Servidor de administración al árbol de consola, realice lo siguiente:

1. En la ventana principal de Kaspersky Security Center, en el árbol de la consola, seleccione el nodo de **Kaspersky Security Center 14**.
2. En el menú contextual del nodo, seleccione **Nuevo** → **Servidor de administración**.

Se creará un nodo con el nombre **Servidor de administración-<nombre del dispositivo> (No conectado)** en el árbol de consola; desde ahí se podrá conectar a cualquier Servidor de administración de la red.

Eliminación de un Servidor de administración del árbol de consola

Para quitar un Servidor de administración del árbol de consola, realice lo siguiente:

1. En el árbol de consola, seleccione el nodo correspondiente al Servidor de administración que quiera quitar.
2. En el menú contextual del nodo, seleccione **Quitar**.

Adición de un Servidor de administración virtual al árbol de consola

Para agregar un Servidor de administración virtual al árbol de consola, realice lo siguiente:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración para el que necesita crear un Servidor de administración virtual.
2. En el nodo del Servidor de administración, seleccione la carpeta **Servidores de administración**.
3. En el espacio de trabajo de la carpeta **Servidores de administración**, haga clic en el enlace **Agregar Servidor de administración virtual**.

   Se ejecuta el Asistente para crear nuevo Servidor de administración virtual.
4. En la ventana **Nombre del Servidor de administración virtual**, especifique el nombre del Servidor de administración virtual que se creará.

   El nombre del Servidor de administración virtual no puede contener más de 255 caracteres de largo y no puede incluir ningún carácter especial (como "*<>-_?:\"|).
5. En la ventana **Introducir dirección para la conexión del dispositivo con el Servidor de administración virtual**, especifique la dirección de conexión del dispositivo.

   La dirección de conexión de un Servidor de administración virtual es la dirección de red mediante la cual los dispositivos se conectarán a ese Servidor. La dirección de conexión tiene dos partes: la dirección de red de un Servidor de administración físico y el nombre de un Servidor de administración virtual, separado con una barra. El nombre del Servidor de administración virtual se substituirá automáticamente. La dirección especificada se utilizará en el Servidor de administración virtual como dirección predeterminada en los paquetes de instalación del Agente de red.
6. En la ventana **Creación de la cuenta de administrador del Servidor de administración virtual**, designe a un usuario de la lista para que funcione como el administrador del Servidor virtual o agregue una nueva cuenta de administrador haciendo clic en el botón **Crear**.

   Puede especificar varias cuentas.

Se crea un nodo denominado **Servidor de administración <Nombre del Servidor de administración virtual>** en el árbol de la consola.

Cambio de una cuenta de servicio del Servidor de administración. Herramienta de utilidad klsrvswch

Si necesita cambiar la cuenta de servicio del Servidor de administración que se estableció al instalar Kaspersky Security Center, puede usar la utilidad denominada klsrvswch que está diseñada para cambiar la cuenta del Servidor de administración.

Cuando Kaspersky Security Center esté instalado, la utilidad se copia automáticamente en la carpeta de instalación de la aplicación.

El número de lanzamientos de la utilidad es esencialmente ilimitado.

La utilidad klsrvswch le permite cambiar el tipo de cuenta. Por ejemplo, si usa una cuenta local, puede cambiarla a una cuenta de dominio o a una cuenta de servicio administrado (y viceversa). La utilidad klsrvswch no le permite cambiar el tipo de cuenta a cuenta de servicio administrada por grupo (gMSA).

Windows Vista y las versiones posteriores de Windows no permiten el uso de una cuenta de LocalSystem para el Servidor de administración. En estas versiones de Windows, la opción de cuenta **LocalSystem** está inactiva.

Para cambiar una cuenta de servicio del Servidor de administración a una cuenta de dominio:

1. Inicie la utilidad klsrvswch desde la carpeta de instalación de Kaspersky Security Center.

   Así se inicia también el Asistente para cambiar la cuenta de servicio del Servidor de administración. Siga las instrucciones del Asistente.

2. En la ventana de la **cuenta del servicio del Servidor de administración**, seleccione **Cuenta LocalSystem**.

   Cuando el Asistente termina, la cuenta del Servidor de administración cambia. El servicio del Servidor de administración se iniciará en la *Cuenta de LocalSystem* con sus credenciales.

El correcto funcionamiento de Kaspersky Security Center requiere que la cuenta utilizada para iniciar el servicio del Servidor de administración tenga los derechos de administrador del recurso donde esté alojada la base de datos del Servidor de administración.

Para cambiar una cuenta de servicio del Servidor de administración a una cuenta de usuario o una cuenta de servicio administrada:

1. Inicie la utilidad klsrvswch desde la carpeta de instalación de Kaspersky Security Center.

   Así se inicia también el Asistente para cambiar la cuenta de servicio del Servidor de administración. Siga las instrucciones del Asistente.

2. En la ventana de la **cuenta del servicio del Servidor de administración**, seleccione **Cuenta personalizada**.

3. Haga clic en el botón **Buscar ahora**.

   Se abre la ventana **Seleccionar un usuario**.

4. En la ventana **Seleccionar usuario**, haga clic en el botón **Tipos de objetos**.

5. En la lista de tipos de objetos, seleccione **Usuarios** (si desea una cuenta de usuario) o **Cuentas de servicio** (si desea una cuenta de servicio administrada) y haga clic en **Aceptar**.

6. En el campo del nombre del objeto, introduzca el nombre de la cuenta o una parte del nombre, y haga clic en **Comprobar nombres**.

7. En la lista de nombres coincidentes, seleccione el nombre necesario y luego haga clic en **Aceptar**.

8. Si seleccionó **Cuentas de servicio**, en la ventana **Contraseña de la cuenta**, deje en blanco los campos **Contraseña** y **Confirmar contraseña**. Si seleccionó **Usuarios**, introduzca una nueva contraseña para el usuario y confírmela.

La cuenta de servicio del Servidor de administración se cambiará a la cuenta que seleccionó.

Cuando se utiliza Microsoft SQL Server de forma que suponga autenticar las cuentas de usuario con las herramientas de Windows, se concederá el acceso a la base de datos. La cuenta de usuario debe tener el estado de propietario para la base de datos de Kaspersky Security Center. De forma predeterminada, se utiliza el esquema dbo.

Cambiar las credenciales de DBMS

A veces, es posible que deba cambiar las credenciales de DBMS, por ejemplo, para realizar una rotación de credenciales por motivos de seguridad.

Para cambiar las credenciales de DBMS en un entorno de Windows mediante klsrvswch.exe:

1. Inicie la utilidad klsrvswch que se encuentra en la carpeta de instalación de Kaspersky Security Center.

2. Haga clic en el botón **Siguiente** del Asistente hasta que llegue al paso **Cambiar las credenciales de acceso DBMS**.

3. En el paso del Asistente **Cambiar las credenciales de acceso DBMS**, haga lo siguiente:

   - Seleccione la opción **Aplicar nuevas credenciales**.
   - Especifique un nuevo nombre de cuenta en el campo **Cuenta**.
   - Especifique una nueva contraseña para una cuenta en el campo **Contraseña**.
   - Especifique la nueva contraseña en el campo **Confirmar contraseña**.

   Debe especificar las credenciales de una cuenta que existe en el DBMS.

4. Haga clic en el botón **Siguiente**.

Una vez finalizado el Asistente, se cambiarán las credenciales de DBMS.

Resolver problemas con nodos del Servidor de administración

El árbol de la consola en el panel izquierdo de la Consola de administración contiene nodos de Servidores de administración. Puede añadir al árbol de la consola todos los Servidores de administración que necesite.

La lista de nodos del Servidor de administración en el árbol de la consola se almacena en una copia paralela de un archivo .msc por medio de la Consola de administración de Microsoft. La copia paralela de este archivo se encuentra en la carpeta %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ del dispositivo en que está instalada la Consola de administración. Para cada nodo del Servidor de administración, el archivo contiene esta información:

- Dirección de Servidor de administración
- Número de puerto
- Si se utiliza TLS

  Este parámetro depende del número de puerto utilizado para conectar la Consola de administración al Servidor de administración.
- Nombre de usuario
- Certificado del Servidor de administración

Solución de problemas

Cuando la Consola de administración se conecta al Servidor de administración, el certificado almacenado localmente se compara con el Certificado del Servidor de administración. Si los certificados no coinciden, la Consola de administración genera un error. Por ejemplo, podría haber una discrepancia de certificados al reemplazar el Certificado del Servidor de administración. En ese caso, vuelva a crear el nodo del Servidor de administración en la consola.

Para volver a crear un nodo de Servidor de administración:

1. Cierre la ventana de la Consola de administración de Kaspersky Security Center.
2. Elimine el archivo de Kaspersky Security Center 14 en %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Ejecute la Consola de administración de Kaspersky Security Center.

   Se le pedirá que se conecte al Servidor de administración y acepte el certificado existente.
4. Realice una de las siguientes acciones:

   - Acepte el certificado existente haciendo clic en el botón **Sí**.
   - Para especificar su certificado, haga clic en el botón **No** y luego vaya al archivo del certificado que usar para autenticar el Servidor de administración.

El problema de certificado queda resuelto. Puede utilizar la Consola de administración para conectar con el Servidor de administración.

Visualización y modificación de los parámetros de un Servidor de administración

Se pueden ajustar los parámetros de un Servidor de administración en la ventana de propiedades del servidor.

Para abrir la ventana Propiedades: Servidor de administración,

Seleccione **Propiedades** en el menú contextual del nodo del Servidor de administración en el árbol de consola.

Ajuste de los parámetros generales de un Servidor de administración

Se puede ajustar la configuración general de un Servidor de administración en las secciones **General**, **Configuración de la conexión del Servidor de administración**, **Repositorio de eventos** y **Seguridad** de la ventana de propiedades del Servidor de administración.

Es posible que la sección **Seguridad** no se muestre en la ventana de propiedades del Servidor de administración si la visualización se ha desactivado en la interfaz de la Consola de administración.

*Para activar la visualización de la sección **Seguridad** en la Consola de administración:*

1. En el árbol de consola, seleccione el Servidor de administración que quiera.
2. En el menú **Ver** de la ventana principal de la aplicación, seleccione **Configuración de la interfaz**.
3. En la ventana que se abre **Configuración de la interfaz**, seleccione la casilla de verificación **Mostrar secciones de configuración de seguridad** y haga clic **Aceptar**.
4. En la ventana con el mensaje de la aplicación, haga clic en **Aceptar**.

La sección **Seguridad** se mostrará en la ventana de propiedades del Servidor de administración.

Configuración de la interfaz de la Consola de administración

Puede ajustar la configuración de la interfaz de la Consola de administración para mostrar u ocultar los controles de la interfaz de usuario relacionados con las siguientes funciones:

- Administración de vulnerabilidades y parches
- Protección y cifrado de datos
- Configuración de Control de Endpoint
- Administración de dispositivos móviles
- Servidores de administración secundarios
- Secciones de configuración de seguridad

Para ajustar la configuración de la interfaz de la Consola de administración, realice lo siguiente:

1. En el árbol de consola, seleccione el Servidor de administración que quiera.
2. En el menú **Ver** de la ventana principal de la aplicación, seleccione **Configuración de la interfaz**.
3. En la ventana que se abre **Configuración de la interfaz**, seleccione las casillas de verificación junto a las funciones que desea mostrar y haga clic en **Aceptar**.
4. En la ventana con el mensaje de la aplicación, haga clic en **Aceptar**.

Las funciones seleccionadas se mostrarán en la interfaz de la Consola de administración.

Procesamiento y almacenamiento de eventos en el Servidor de administración

La información sobre eventos de la operación de la aplicación y los dispositivos administrados se guarda en la base de datos del Servidor de administración. Cada evento se atribuye a un determinado tipo y nivel de gravedad (*Evento crítico*, *Fallo operativo*, *Advertencia* o *Información*). Según las condiciones en que tengan lugar los eventos, la aplicación puede asignar diferentes niveles de gravedad a eventos del mismo tipo.

Puede ver los tipos y niveles de gravedad asignados a eventos en la sección **Configuración de eventos** de la ventana de propiedades del Servidor de administración. Asimismo, en la sección **Configuración de eventos**, puede configurar el procesamiento de cada evento por parte del Servidor de administración:

- Registro de eventos en el Servidor de administración y en los registros de eventos del sistema operativo en un dispositivo y en el Servidor de administración.
- El método que se utiliza para notificar un evento al administrador (por ejemplo, por mensaje de correo electrónico o de texto).

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede editar la configuración del almacenamiento de eventos en la base de datos del Servidor de administración limitando el número de registros de eventos o el tiempo de almacenamiento de los registros. Cuando especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede usar este cálculo aproximado para evaluar si tiene suficiente espacio libre en el disco para evitar el desbordamiento de la base de datos. La capacidad predeterminada de la base de datos del Servidor de administración es de 400.000 eventos. La capacidad máxima recomendada de la base de datos es 45 millones de eventos.

Si el número de eventos en la base de datos llega al valor máximo especificado por el administrador, la aplicación elimina los eventos más antiguos sobrescribiéndolos con los nuevos. Cuando el Servidor de administración elimina eventos antiguos, no puede guardar eventos nuevos en la base de datos. Durante este período de tiempo, la información sobre los eventos que fueron rechazados se escribe en el Registro de eventos de Kaspersky. Los nuevos eventos se ponen en cola y luego se guardan en la base de datos una vez que se completa la operación de eliminación.

Visualización del registro de conexiones con el Servidor de administración

El historial de conexiones e intentos de conexión con el Servidor de administración durante su funcionamiento se puede guardar en un archivo de registro. La información en el archivo no solo le permite rastrear las conexiones en la infraestructura de red, sino también los intentos no autorizados de acceder al Servidor de administración.

Para registrar los eventos de conexión al Servidor de administración:

1. En el árbol de la consola, seleccione el Servidor de administración para el que necesita activar el registro de eventos de conexión.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades que se abre, en la sección **Configuración de la conexión del Servidor de administración** seleccione la subsección **Puertos de conexión**.
4. Active la opción **Registrar eventos de conexión del Servidor de administración**.
5. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

Todos los eventos adicionales de la conexión con el Servidor de administración, los resultados de autenticación y los errores de SSL se guardarán en el archivo %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Control de brotes de virus

Kaspersky Security Center le permite responder con rapidez a las nuevas amenazas de los focos de virus. Los riesgos de los focos de virus se evalúan mediante la monitorización de la actividad del virus en los dispositivos.

Puede configurar las reglas de valoración de las amenazas de los focos de virus y las acciones que llevar a cabo en caso de que se desarrollen. Para ello, vaya a la sección **Brote de virus** de la ventana de propiedades del Servidor de administración.

Puede especificar el procedimiento de notificación del evento *Brote de virus* en la sección **Configuración de eventos** de la ventana de propiedades del Servidor de administración, en la ventana de propiedades del evento *Brote de virus*.

El evento *Brote de virus* se genera si se detectan eventos *Objeto malicioso detectado* durante la utilización de aplicaciones de seguridad. Por lo tanto, debe guardar la información sobre todos los eventos *Objeto malicioso detectado* en el Servidor de administración para reconocer focos de virus.

Puede determinar la configuración del almacenamiento de la información sobre cualquier evento *Objeto malicioso detectado* en las directivas de las aplicaciones de seguridad.

Al contar los eventos *Objeto malicioso detectado*, solamente se tomará en cuenta la información de los dispositivos del Servidor de administración principal. La información de los Servidores de administración secundarios no se tiene en cuenta. Los parámetros del evento *Brote de virus* se configuran individualmente para cada servidor secundario.

Limitación del tráfico

La aplicación proporciona la opción de limitar la velocidad de transferencia de datos a un Servidor de administración desde rangos IP y subredes IP especificados, para reducir los volúmenes de tráfico de la red.

Se pueden crear y configurar reglas de limitación del tráfico en la sección **Tráfico** de la ventana de propiedades del Servidor de administración.

Para crear una regla restrictiva de tráfico:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración para el que desea crear una regla restrictiva de tráfico.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Tráfico**.
4. Haga clic en el botón **Agregar**.
5. En la ventana **Nueva regla**, especifique la siguiente configuración:

   En la sección **Rango IP para limitar el tráfico**, seleccione el método que se utilizará con el fin de definir la subred o rango para el cual la tasa de transferencia de datos será limitada y, entonces, introduzca los valores de los parámetros del método seleccionado. Seleccione uno de los siguientes métodos:

- **Especificar el rango mediante el uso de máscara de dirección y de red**

  El tráfico se limita según la configuración de la subred. Especifique la dirección y la máscara de la subred para determinar el rango en el que se limitará el tráfico.

  También puede clic **Navegar** para añadir subredes de la lista global de subredes.

- **Especificar el rango mediante el uso de la dirección inicial y final**

  El tráfico se limita basándose en un rango de direcciones IP. Especifique el rango de direcciones IP en los campos de entrada **Inicial** y **Final**.

  Esta opción está seleccionada de forma predeterminada.

En la sección **Límite de tráfico** puede ajustar los siguientes parámetros de restricción para la tasa de transferencia de datos:

- **Intervalo de tiempo**

  Intervalo de tiempo durante el cual la restricción del tráfico estará en vigor. Puede especificar los límites del intervalo de tiempo en los campos de entrada.

- **Límite (KB/s)**

  Velocidad máxima de la transferencia total de datos entrantes y salientes del Servidor de administración. La restricción de tráfico solo será efectiva dentro del intervalo especificado en el campo **Intervalo de tiempo**.

- **Limitar el tráfico durante el resto del tiempo (KB/s)**

  Si se selecciona esta casilla, el tráfico no se limitará únicamente durante el intervalo de tiempo especificado en el campo **Intervalo de tiempo**, sino también el resto del tiempo.

  De forma predeterminada, esta casilla está en blanco. El valor de este campo podría no coincidir con el valor del campo **Límite (kB/s)**.

Principalmente, las reglas de limitación de tráfico afectan a la transferencia de archivos. Estas reglas no se aplican al tráfico generado por la sincronización entre el Servidor de administración y el Agente de red, o entre los Servidores de administración principales y secundarios.

Configuración de servidor web

El Servidor web está diseñado para publicar paquetes de instalación independientes, perfiles de MDM para iOS y archivos de una carpeta compartida.

Puede definir la configuración para la conexión del Servidor Web al Servidor de administración y especificar un certificado de Servidor Web en la sección **Servidor web** de la ventana de propiedades del Servidor de administración.

Trabajo con usuarios internos

Las cuentas de los *usuarios internos* se utilizan para trabajar con Servidores de administración virtuales. Kaspersky Security Center otorga los derechos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo en Kaspersky Security Center. No se transfiere ningún dato de los usuarios internos al sistema operativo. Kaspersky Security Center autentifica los usuarios internos.

Puede ver los datos de los usuarios internos en la carpeta **Cuentas de usuario**, en el árbol de consola.

Creación de copias de seguridad y restauración de la configuración del Servidor de administración

La copia de seguridad de la configuración del Servidor de administración y su base de datos se realiza a través de la tarea de copia de seguridad y la utilidad klbackup. Una copia de seguridad incluye toda la configuración principal y los objetos que pertenecen al Servidor de administración, por ejemplo, certificados, claves principales para el cifrado de unidades en dispositivos administrados, claves para varias licencias, la estructura de los grupos de administración con todo su contenido, tareas, directivas, etc. Con una copia de seguridad puede recuperar el funcionamiento de un Servidor de administración en el menor tiempo posible, entre una docena de minutos y un par de horas.

Si no hay ninguna copia de seguridad disponible, un fallo puede provocar una pérdida irrevocable de certificados y toda la configuración del Servidor de administración. Esto requerirá configurar nuevamente Kaspersky Security Center desde el principio y realizar el despliegue inicial del Agente de red en la red de la organización otra vez. Todas las claves principales para el cifrado de unidades en dispositivos administrados también se perderán, arriesgando la pérdida irrevocable de datos cifrados en dispositivos con Kaspersky Endpoint Security. Por tanto, no debe dejar de crear, a intervalos regulares, copias de seguridad del Servidor de administración mediante la tarea de copia de seguridad estándar.

El Asistente de inicio rápido crea la tarea de copia de seguridad para la configuración del Servidor de administración y la configura para que se ejecute diariamente a las 4:00 A.M. Las copias de seguridad se guardan de forma predeterminada en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskySC.

Si se utiliza una instancia de Microsoft SQL Server instalada en otro dispositivo como DBMS, debe modificar la tarea de copia de seguridad al especificar una ruta de UNC, que está disponible para escritura tanto del servicio del Servidor de administración como del servicio de SQL Server, como la carpeta para almacenar copias de seguridad. Este requisito, que no es obvio, deriva de una función especial de copia de seguridad en DBMS de Microsoft SQL Server.

Si se utiliza una instancia local de Microsoft SQL Server como DBMS, también recomendamos guardar copias de seguridad en un medio dedicado a fin de protegerlas contra el daño junto con el Servidor de administración.

Como una copia de seguridad contiene datos importantes, la tarea de copia de seguridad y la utilidad klbackup proporcionan la protección con contraseña de las copias de seguridad. De forma predeterminada, la tarea de creación de copia de seguridad se crea con una contraseña en blanco. Debe configurar una contraseña en las propiedades de la tarea de creación de copia de seguridad. Descuidar este requisito causa una situación donde todas las claves de los certificados del Servidor de administración, las claves para licencias y las claves principales para el cifrado de unidades de disco en los dispositivos administrados permanecen sin cifrar.

Además de la copia de seguridad habitual, también debe crear una copia de seguridad antes de cada cambio significativo, incluida la instalación de actualizaciones y parches del Servidor de administración.

Para minimizar el tamaño de las copias de seguridad, active la opción **Comprimir copia de seguridad** en la configuración de SQL Server.

La restauración desde una copia de seguridad se realiza con la utilidad klbackup en una instancia operable del Servidor de administración que se acaba de instalar y tiene la misma versión (o posterior) para la cual se creó la copia de seguridad.

La instancia del Servidor de administración en el cual se debe realizar la restauración debe utilizar un DBMS del mismo tipo (mismo SQL Server, MySQL o MariaDB) y la misma versión (o una posterior). La versión del Servidor de administración puede ser la misma (con un parche idéntico o posterior) o posterior.

Esta sección describe las situaciones estándares para restaurar la configuración y los objetos del Servidor de administración.

Uso de una instantánea del sistema de archivos para reducir la duración de la copia de seguridad

En Kaspersky Security Center 14, el tiempo de inactividad del Servidor de administración durante la copia de seguridad se ha reducido en comparación con las versiones anteriores. Además, se ha añadido la función **Usar instantánea del sistema de archivos para la de copia de seguridad de datos** a la configuración de la tarea. Esta función reduce aún más el tiempo de inactividad mediante la utilidad klbackup, que crea una copia paralela del disco durante la copia de seguridad (tarda unos segundos) y simultáneamente copia la base de datos (tarda unos minutos, como mucho). Cuando klbackup crea una copia paralela del disco y una copia de la base de datos, la herramienta permite que el Servidor de administración se pueda volver a conectar.

Puede utilizar la función de captura de instantáneas del sistema de archivos solo si se cumplen estas dos condiciones:

- La carpeta compartida del Servidor de administración y la carpeta %ALLUSERSPROFILE%\KasperskyLab están localizadas en el mismo disco lógico y son locales en referencia al Servidor de administración.
- La carpeta %ALLUSERSPROFILE%\KasperskyLab no contiene ningún enlace simbólico que se haya creado manualmente.

No utilice esta función si no se puede cumplir alguna de estas dos condiciones. En este caso, la aplicación devolverá un mensaje de error en respuesta a cualquier intento de crear una instantánea del sistema de archivos.

Para usar la función, debe tener una cuenta a la que se le haya otorgado el permiso para crear instantáneas del disco lógico que almacena la carpeta %ALLUSERSPROFILE%. Recuerde que la cuenta de servicio del Servidor de administración no tiene tal permiso.

Para usar la función de captura de instantáneas del sistema de archivos para reducir la duración de la copia de seguridad:

1. En la sección **Tareas**, seleccione la tarea de copia de seguridad.
2. En el menú contextual, seleccione **Propiedades**.
3. En la ventana de propiedades de la tarea que se abre, seleccione la sección **Configuración**.
4. Seleccione la casilla **Usar instantánea del sistema de archivos para la copia de seguridad de datos**.
5. En los campos **Nombre de usuario** y **Contraseña**, indique el nombre y la contraseña de una cuenta que tenga permiso para crear instantáneas del disco lógico que almacena la carpeta %ALLUSERSPROFILE%.
6. Haga clic en **Aplicar**.

Si más adelante se inicia la tarea de copia de seguridad, la utilidad klbackup creará instantáneas del sistema de archivos reduciendo así el tiempo de inactividad del Servidor de administración durante la ejecución de la tarea.

Un dispositivo con el Servidor de administración es inoperable

Si un dispositivo con el Servidor de administración es inoperable debido a una omisión, se recomienda realizar las acciones siguientes:

- Se debe asignar la misma dirección al nuevo Servidor de administración: el nombre NetBIOS, FQDN o IP estática (según cuál de estas opciones se configuró cuando se desplegaron los Agentes de red).
- Instale el Servidor de administración usando un DBMS del mismo tipo, de la misma versión (o posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la configuración inicial a través del Asistente.
- En el menú **Iniciar**, ejecute la utilidad klbackup y realice la restauración.

La configuración del Servidor de administración o la base de datos están dañadas

Si el Servidor de administración es inoperable debido a parámetros o base de datos dañados (por ej., después de una sobretensión), se recomienda usar la situación de restauración siguiente:

1. Analice el sistema de archivos en el dispositivo dañado.
2. Desinstale la versión inoperable del Servidor de administración.
3. Instale nuevamente el Servidor de administración usando un DBMS del mismo tipo y de la misma versión (o posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la configuración inicial a través del Asistente.
4. En el menú **Iniciar**, ejecute la utilidad klbackup y realice la restauración.

Se prohíbe restaurar el Servidor de administración si no es a través de la utilidad klbackup.

Cualquier intento de restaurar el Servidor de administración mediante software de terceros bloqueará la sincronización de los datos en los nodos de la aplicación distribuida Kaspersky Security Center y, por consiguiente, afectará al funcionamiento correcto de la aplicación.

Creación de copias de seguridad y restauración de los datos del Servidor de administración

La copia de seguridad de datos permite trasladar un Servidor de administración de un dispositivo a otro sin perder los datos. Mediante la copia de seguridad, puede restaurar datos cuando traslada la base de datos de un Servidor de administración a otro dispositivo o cuando se pasa a una nueva versión de Kaspersky Security Center.

Puede crear una copia de seguridad de los datos del Servidor de administración mediante uno de los siguientes métodos:

- Creando y ejecutando una tarea de creación de copias de seguridad de datos mediante la Consola de administración.

- Ejecutando la utilidad klbackup en el dispositivo que tenga instalado el Servidor de administración. La utilidad se incluye en el kit de distribución de Kaspersky Security Center. Después de la instalación del Servidor de administración, la utilidad se ubica en la raíz de la carpeta de destino especificada durante la instalación de la aplicación.

Los siguientes datos se guardan en la copia de seguridad del Servidor de administración:

- Base de datos del Servidor de administración (directivas, tareas, parámetros de la aplicación, eventos guardados en el Servidor de administración).
- Información de configuración de la estructura de los grupos de administración y los dispositivos cliente.
- Repositorio de paquetes de distribución de aplicaciones para la instalación remota.
- Certificado del Servidor de administración.

La recuperación de datos del Servidor de administración solo es posible mediante la utilidad klbackup.

Creación de una tarea de copia de seguridad

Las tareas de creación de copias de seguridad son tareas del Servidor de administración creadas por el Asistente de inicio rápido. Si se ha eliminado una tarea de creación de copias de seguridad creada por el Asistente de inicio rápido, puede crear una manualmente.

Para crear una tarea de creación de copias de seguridad de los datos del Servidor de administración:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. Inicie la creación de la tarea por alguno de los siguientes medios:
   - Seleccione **Nuevo** → **Tarea** en el menú contextual de la carpeta **Tareas** en el árbol de la consola.
   - Al hacer clic en el botón **Crear una tarea** en el espacio de trabajo.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente. En la ventana **Seleccionar el tipo de tarea** del Asistente, seleccione el tipo de tarea llamada **Copia de seguridad de los datos del Servidor de administración**.

La tarea **Copia de seguridad de los datos del Servidor de administración** solo puede crearse en una copia individual. Si la tarea de creación de copias de seguridad de los datos del Servidor de administración ya se ha creado, no aparecerá en la ventana de selección de tipo de tarea del Asistente para crear tareas de copia de seguridad.

Utilidad de creación de copias de seguridad y recuperación de datos (klbackup)

Puede hacer copias de seguridad de los datos del Servidor de administración para su almacenamiento y futura recuperación mediante la utilidad klbackup, que es parte del kit de distribución de Kaspersky Security Center.

La utilidad klbackup puede ejecutarse en cualquiera de los dos modos siguientes:

- Interactivo
- No interactivo

Creación de copias de seguridad y recuperación de datos en modo interactivo

Para crear una copia de seguridad de los datos del Servidor de administración en el modo interactivo:

1. Ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center.

   Se inicia el Asistente de copias de seguridad y restauración.

2. En la primera ventana del Asistente, seleccione **Hacer copia de seguridad de los datos del Servidor de administración**.

   Si marca la opción **Restaurar o crear copia de seguridad solamente del certificado del Servidor de administración**, solo se guardará una copia de seguridad del certificado del Servidor de administración.

   Haga clic en **Siguiente**.

3. En la siguiente ventana del Asistente, especifique las siguientes opciones:

   - **La carpeta de destino de la copia de seguridad**
   - **Migrar al formato MySQL/MariaDB**

     Habilite esta opción si está usando SQL Server como DBMS para el Servidor de administración y desea migrar los datos de SQL Server a MySQL o MariaDB DBMS. Kaspersky Security Center creará una copia de seguridad compatible con MySQL y MariaDB. Después de eso, puede restaurar los datos de la copia de seguridad en MySQL o MariaDB.

   - **Migrar al formato de Azure**

     Habilite esta opción si está usando SQL Server como DBMS para el Servidor de administración y desea migrar los datos de SQL Server a Azure SQL DBMS. Kaspersky Security Center creará una copia de seguridad compatible con Azure SQL. Después, puede restaurar los datos de la copia de seguridad en Azure SQL.

   - **Incluir la fecha y la hora actuales en el nombre de la carpeta de destino de la copia de seguridad**
   - **Contraseña de la copia de seguridad**

4. Haga clic en el botón **Siguiente** para iniciar la creación de copias de seguridad.

5. Si está trabajando con una base de datos en un entorno de nube como Amazon Web Services (AWS) o Microsoft Azure, en la ventana **Iniciar sesión en el almacenamiento en línea**, complete los siguientes campos:

   - Para AWS:
     - **Nombre del bucket S3**

       El nombre del bucket S3 que creó para la copia de seguridad.

- **Id. de clave de acceso**

  Recibió el Id. de clave (secuencia de caracteres alfanuméricos) cuando creó la cuenta de usuario de IAM para trabajar con la instancia de almacenamiento de bucket S3.

  El campo está disponible Si ha seleccionado la base de datos de RDS en un bucket S3.

- **Clave secreta**

  La clave secreta que recibió con el Id. de clave de acceso cuando creó la cuenta de usuario de IAM.

  Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a introducir la clave secreta, aparecerá el botón **Mostrar**. Haga clic y mantenga pulsado este botón durante la cantidad de tiempo necesaria para ver los caracteres que introdujo.

  El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

- Para Microsoft Azure:

  - **Nombre de la cuenta de almacenamiento de Azure**

    Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  - **Id. de suscripción de Azure**

    Usted creó la suscripción en el portal de Azure.

  - **Contraseña de Azure**

    Recibió la contraseña del Id. de la aplicación cuando creó el Id. de la aplicación.

    Los caracteres de la contraseña se muestran como asteriscos. Después de empezar a introducir la contraseña, el botón **Mostrar** estará disponible. Haga clic y mantenga presionado este botón para ver los caracteres que introdujo.

  - **Id. de la aplicación en Azure**

    Usted creó este Id. de la aplicación en el portal de Azure.

    Solo puede proporcionar un Id. de la aplicación en Azure para sondeos y otros fines. Si desea sondear otro segmento de Azure, primero debe eliminar la conexión de Azure existente.

  - **Nombre del servidor SQL de Azure**

    El nombre y el grupo de recursos están disponibles en sus propiedades de Azure SQL Server.

  - **Grupo de recursos del servidor SQL de Azure**

    El nombre y el grupo de recursos están disponibles en sus propiedades de Azure SQL Server.

- Clave de acceso al almacenamiento de Azure

  Disponible en las propiedades de su cuenta de almacenamiento, en la sección Claves de acceso. Puede utilizar cualquiera de las claves (clave1 o clave2).

Para recuperar datos del Servidor de administración en modo interactivo:

1. Ejecute la utilidad klbackup ubicada en la carpeta de instalación de Kaspersky Security Center. Inicie la utilidad con la misma cuenta con la que instaló el Servidor de administración.

   Se inicia el Asistente de copias de seguridad y restauración.

2. En la primera ventana del Asistente, seleccione **Restaurar datos del Servidor de administración**.

   Si selecciona la opción **Restaurar o crear copia de seguridad solamente del certificado del Servidor de administración**, el Servidor de administración solo se recuperará.

   Haga clic en **Siguiente**.

3. En la ventana **Restaurar la configuración** del Asistente:

   - Especifique la carpeta que contiene una copia de seguridad de los datos del Servidor de administración. Debe asegurarse de que el archivo se denomine backup.zip. Si está trabajando en un entorno de nube como AWS o Azure, especifique la dirección del almacenamiento.

   - Especifique la contraseña introducida durante la creación de copias de seguridad de los datos.

     Al restaurar datos, debe indicar la misma contraseña que se introdujo durante la creación de copias de seguridad. Si la ruta de una carpeta compartida cambió tras realizar la copia de seguridad, compruebe el funcionamiento de las tareas que utilizan datos restaurados (tareas de restablecimiento y tareas de instalación remota). Si fuera necesario, edite la configuración de estas tareas. Mientras los datos se están restaurando desde una copia de seguridad, nadie debe acceder a la carpeta compartida del Servidor de administración. La cuenta con la que se inicia la utilidad klbackup debe tener total acceso a la carpeta compartida.

4. Haga clic en el botón **Siguiente** para restaurar los datos.

Creación de copias de seguridad y recuperación de datos en modo no interactivo

Para crear una copia de seguridad o recuperar los datos del Servidor de administración en modo no interactivo,

Ejecute la utilidad klbackup con el conjunto de claves requeridas desde la línea de comandos del dispositivo en el que esté instalado el Servidor de administración.

Sintaxis de línea de comandos de la utilidad:

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

Si no hay ninguna contraseña especificada en la línea de comandos de la utilidad klbackup, la utilidad le solicitará introducir la contraseña de forma interactiva.

Descripciones de las claves:

- `-path BACKUP_PATH`: Guardar información en la carpeta BACKUP_PATH o utilizar datos de la carpeta BACKUP_PATH para la recuperación (parámetro obligatorio).

- `-logfile LOGFILE`: Guardar un informe sobre la creación de copias de seguridad y recuperación de los datos del Servidor de administración.

  Se concederá acceso a la cuenta del servidor de bases de datos y a la utilidad klbackup para la modificación de datos en la carpeta BACKUP_PATH.

- `-use_ts`: Al guardar datos, copiar información en la carpeta BACKUP_PATH, en la subcarpeta con un nombre que contenga la hora de funcionamiento y fecha del sistema actual en formato `klbackup AAAA-MM-DD # HH-MM-SS`. Si no se ha especificado ninguna clave, la información se guarda en la raíz de la carpeta BACKUP_PATH.

  Cuando se intenta guardar información en una carpeta que ya tiene almacenada una copia de seguridad, aparece un mensaje de error. No se actualizará ninguna información.

  La disponibilidad de la clave `-use_ts` permite conservar un archivo de datos del Servidor de administración. Por ejemplo, si la clave `-path` indica la carpeta `C:\KLBackups`, entonces la carpeta `klbackup 2022/6/19 # 11-30-18` almacena información sobre el estado del Servidor de administración con fecha de 19 de junio de 2022, a las 11:30:18 h.

- `-restore`: Recupera datos del Servidor de administración. La recuperación de datos se realiza según la información incluida en la carpeta BACKUP_PATH. Si no hay ninguna clave disponible, se hace una copia de seguridad de los datos en la carpeta BACKUP_PATH.

- `-password PASSWORD`: Guarda o recupera el certificado del Servidor de administración. Para cifrar y descifrar el certificado, utilice la contraseña especificada por el parámetro PASSWORD.

  > Una contraseña olvidada no se puede recuperar. No hay requisitos para la contraseña. La longitud de la contraseña es ilimitada y también es posible la longitud cero (sin contraseña).

  Al restaurar datos, debe indicar la misma contraseña que se introdujo durante la creación de copias de seguridad. Si la ruta de una carpeta compartida cambió tras realizar la copia de seguridad, compruebe el funcionamiento de las tareas que utilizan datos restaurados (tareas de restablecimiento y tareas de instalación remota). Si fuera necesario, edite la configuración de estas tareas. Mientras los datos se están restaurando desde una copia de seguridad, nadie debe acceder a la carpeta compartida del Servidor de administración. La cuenta con la que se inicia la utilidad klbackup debe tener total acceso a la carpeta compartida.

- `-online`: Hace una copia de seguridad de los datos del Servidor de administración, mediante la creación de una instantánea de volumen para minimizar el tiempo sin conexión del Servidor de administración. Cuando utiliza la utilidad para recuperar datos, esta opción se ignora.

Mover un Servidor de administración a otro dispositivo

Para mover un Servidor de administración a otro dispositivo:

1. Cree una copia de seguridad de datos del Servidor de administración.

2. Instale el Servidor de administración en el dispositivo seleccionado.

   Para simplificar el proceso de mantener la estructura de los grupos de administración, le recomendamos que se asegure de que la dirección del nuevo Servidor de administración sea la misma que la dirección del Servidor de administración anterior. La dirección (es decir, el nombre del dispositivo en la red Windows o una dirección IP) está especificada en la configuración del Agente de red, en el grupo de ajustes de **Conexión al Servidor de administración**.

3. En el nuevo Servidor de administración, recupere los datos del Servidor de administración a partir de una copia de seguridad.

4. Si la dirección (es decir, el nombre de dispositivo en la red de Windows o la dirección IP) del nuevo Servidor de administración no es la misma que la del anterior, conecte los dispositivos clientes con el nuevo Servidor de administración creando una tarea *Cambiar Servidor de administración* para el grupo **Dispositivos administrados** en el Servidor de administración anterior.

   Si la dirección es la misma, no es necesario que cree esta tarea. La conexión se realizará a la dirección especificada en la configuración.

5. Elimine el Servidor de administración anterior.

Si lo desea, también puede utilizar un nuevo dispositivo para el DBMS. Para la correcta transferencia de información, asegúrese de que el nuevo DBMS tenga los mismos esquemas de clasificación que el anterior.

Evitar conflictos entre múltiples Servidores de administración

Si tiene más de un Servidor de administración en su red, pueden ver los mismos dispositivos cliente. Esto puede dar como resultado, por ejemplo, la instalación remota de la misma aplicación en uno y el mismo dispositivo desde más de un Servidor y otros conflictos. Para evitar tal situación, Kaspersky Security Center 14 le permite evitar que una aplicación se instale en un dispositivo administrado por otro Servidor de administración.

También puede usar la propiedad **Administrado por otro Servidor de administración** diferente como criterio para los siguientes propósitos:

- Búsqueda de dispositivos
- Selecciones de dispositivos
- Reglas de movimiento de dispositivos
- Reglas de etiquetado automático

Kaspersky Security Center 14 usa heurísticas para determinar si un dispositivo cliente está administrado por el Servidor de administración con el que está trabajando o por un Servidor de administración diferente.

Verificación en dos pasos

Esta sección describe cómo puede usar la verificación en dos pasos para reducir el riesgo de acceso no autorizado a la Consola de administración o a Kaspersky Security Center 14 Web Console.

Escenario: configurar la verificación en dos pasos para todos los usuarios

Este escenario describe cómo activar la verificación en dos pasos para todos los usuarios y cómo excluir las cuentas de usuario de la verificación en dos pasos. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para otros usuarios, la aplicación abre primero la ventana para habilitar la verificación en dos pasos para su cuenta. Este escenario también describe cómo activar la verificación en dos pasos para su propia cuenta.

Si habilitó la verificación en dos pasos para su cuenta, puede proceder a activar la verificación en dos pasos para todos los usuarios.

Requisitos previos

Antes de empezar:

- Asegúrese de que su cuenta de usuario tenga derechos de Modificar ACL de objeto del área funcional **Funciones generales: Permisos de usuario** para modificar la configuración de seguridad de las cuentas de otros usuarios.
- Asegúrese de que los demás usuarios del Servidor de administración instalen una aplicación de autenticación en sus dispositivos.

Etapas

La activación de la verificación en dos pasos para todos los usuarios se realiza en etapas:

1. **Instalación de una aplicación de autenticación en un dispositivo**

   Puede instalar Google Authenticator, Microsoft Authenticator o cualquier otra aplicación de autenticación que admita el algoritmo de contraseña única basada en tiempo.

2. **Sincronización de la hora de la aplicación de autenticación con la hora del dispositivo en el que está instalado el Servidor de administración**

   Asegúrese de que la hora establecida en la aplicación de autenticación esté sincronizada con la hora del Servidor de administración.

3. **Activación de la verificación en dos pasos para su cuenta y recepción de la clave secreta de su cuenta**

   Instrucciones:

   - Para la consola de administración basada en MMC: Activación de la verificación en dos pasos de su propia cuenta
   - Para Kaspersky Security Center 14 Web Console: Activación de la verificación en dos pasos para su propia cuenta

   Después de activar la verificación en dos pasos para su cuenta, puede activar la verificación en dos pasos para todos los usuarios.

4. **Activación de la verificación en dos pasos para todos los usuarios**

   Los usuarios que tengan activada la verificación en dos pasos deben usarla para iniciar sesión en el Servidor de administración.

   Instrucciones:

   - Para la consola de administración basada en MMC: Activar la verificación en dos pasos para todos los usuarios
   - Para Kaspersky Security Center 14 Web Console: Activar la verificación en dos pasos para todos los usuarios

5. **Modificar el nombre de un emisor del código de seguridad**

Si tiene varios Servidores de administración con nombres similares, es posible que deba cambiar los nombres de los emisores del código de seguridad para reconocer mejor los diferentes Servidores de administración.

Instrucciones:

- Para la consola de administración basada en MMC: Modificar el nombre del emisor de un código de seguridad
- Para Kaspersky Security Center 14 Web Console: Modificar el nombre de un emisor de código de seguridad

6. **Exclusión de las cuentas de usuario para las que no necesita activar la verificación en dos pasos**

   Si es necesario, puede excluir usuarios de la verificación en dos pasos. Los usuarios con cuentas excluidas no tienen que utilizar la verificación en dos pasos para iniciar sesión en el Servidor de administración.

   Instrucciones:

   - Para la consola de administración basada en MMC: Excluir cuentas de la verificación en dos pasos
   - Para Kaspersky Security Center 14 Web Console: Excluir cuentas de la verificación en dos pasos

Resultados

Una vez completado este escenario:

- La verificación en dos pasos queda activada para su cuenta.
- La verificación en dos pasos queda activada para todas las cuentas de usuario del Servidor de administración, excepto para las cuentas de usuario que fueron excluidas.

Acerca de la verificación en dos pasos

Kaspersky Security Center proporciona verificación en dos pasos para los usuarios de la Consola de administración o de Kaspersky Security Center 14 Web Console. Cuando la verificación en dos pasos está activada para su propia cuenta, cada vez que inicie sesión en la Consola de administración o en Kaspersky Security Center 14 Web Console, debe introducir su nombre de usuario, contraseña y un código de seguridad adicional de un solo uso. Si usa la autenticación de dominio para su cuenta, basta con ingresar un código de seguridad adicional de un solo uso. Para recibir un código de seguridad de un solo uso, debe tener una aplicación de autenticación en su equipo o dispositivo móvil.

Un código de seguridad tiene un identificador denominado *nombre del emisor*. El nombre del emisor del código de seguridad se utiliza como un identificador del Servidor de administración en la aplicación de autenticación. Puede cambiar el nombre del emisor del código de seguridad. El nombre del emisor del código de seguridad tiene un valor predeterminado que es el mismo que el nombre del Servidor de administración. El nombre del emisor se utiliza como un identificador del Servidor de administración en la aplicación de autenticación. Si cambia el nombre del emisor del código de seguridad, debe volver a emitir una nueva clave secreta y pasarla a la aplicación de autenticación. Los códigos de seguridad son de un solo uso y válidos por hasta 90 segundos (el tiempo exacto puede variar).

Cualquier usuario que tenga activada la verificación en dos pasos puede volver a emitir su propia clave secreta. Cuando un usuario se autentica con la clave secreta reemitida y la usa para iniciar sesión, el Servidor de administración guarda la nueva clave secreta de la cuenta de usuario. Si un usuario introduce la clave secreta de forma incorrecta al formulario de autenticación, el Servidor de administración no guarda la nueva clave secreta y conserva la validez de la clave secreta vigente para la autenticación posterior.

Cualquier software de autenticación que admita el algoritmo de contraseña de un solo uso basado en tiempo (TOTP) se puede utilizar como aplicación de autenticación, por ejemplo, Google Authenticator. Para generar el código de seguridad, debe sincronizar la hora configurada en la aplicación de autenticación con la hora configurada del Servidor de administración.

Una aplicación de autenticación genera el código de seguridad de la siguiente manera:

1. El Servidor de administración genera una clave secreta especial y un código QR.
2. Usted pasa la clave secreta generada o el código QR a la aplicación de autenticación.
3. La aplicación de autenticación genera un código de seguridad de un solo uso que usted pasa a la ventana de autenticación del Servidor de administración.

Insistimos en recomendarle que instale una aplicación de autenticación en más de un dispositivo móvil. Guarde la clave secreta (o el código QR) y conservelos en un lugar seguro. Esto le ayudará a restaurar el acceso a la Consola de administración o a Kaspersky Security Center 14 Web Console si pierde el acceso a su dispositivo móvil.

Para proteger el uso de Kaspersky Security Center, puede habilitar la verificación en dos pasos para su propia cuenta y habilitar la verificación en dos pasos para todos los usuarios.

Puede excluir cuentas de la verificación en dos pasos. Esto puede ser necesario para las cuentas de servicio que no pueden recibir un código de seguridad para la autenticación.

La verificación en dos pasos funciona según las siguientes reglas:

- Solo una cuenta de usuario que tenga los derechos Modificar objeto ACL en el área funcional **Funciones generales: Permisos de usuario** puede activar la verificación en dos pasos para todos los usuarios.
- Solo un usuario que haya habilitado la verificación en dos pasos para su propia cuenta puede habilitar la opción de verificación en dos pasos para todos los usuarios.
- Solo un usuario que haya habilitado la verificación en dos pasos para su propia cuenta puede excluir otras cuentas de usuario de la lista de verificación en dos pasos habilitada para todos los usuarios.
- Un usuario puede activar la verificación en dos pasos solo para su propia cuenta.
- Una cuenta de usuario que tiene el derecho Modificar las LCA de objetos en el área funcional **Características generales: permisos de usuario** y está conectado a la Consola de administración o a Kaspersky Security Center 14 Web Console mediante la verificación en dos pasos puede deshabilitar la verificación en dos pasos: a) para cualquier otro usuario solo si la verificación en dos pasos para todos los usuarios está deshabilitada; b) para un usuario excluido de la lista de verificación en dos pasos que esté habilitada para todos los usuarios.
- Cualquier usuario que haya iniciado sesión en la Consola de administración o en Kaspersky Security Center 14 Web Console mediante la verificación en dos pasos puede volver a emitir su clave secreta.
- Puede habilitar la opción de verificación en dos pasos para todos los usuarios para el Servidor de administración con el que está trabajando en un momento dado. Si activa esta opción en el Servidor de administración, también activa esta opción para las cuentas de usuario de sus Servidores de administración virtuales y no activa la verificación en dos pasos para las cuentas de usuario de los Servidores de administración secundarios.

Si la verificación en dos pasos está activada para una cuenta de usuario en el Servidor de administración de Kaspersky Security Center versión 13 o posterior, el usuario no podrá conectarse a las versiones 12, 12.1 o 12.2 de Kaspersky Security Center Web Console.

Activar la verificación en dos pasos para su propia cuenta

Antes de activar la verificación en dos pasos para su cuenta, asegúrese de que haya una aplicación de autenticación instalada en su dispositivo móvil. Asegúrese de que la hora establecida en la aplicación de autenticación esté sincronizada con la hora del Servidor de administración.

Para activar la verificación en dos pasos para su cuenta:

1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana Propiedades del Servidor de administración, vaya al panel **Secciones**, seleccione **Avanzado**, y luego **Verificación en dos pasos**.
3. En la sección **Verificación en dos pasos**, haga clic en el botón **Configuración**.

   En la ventana de propiedades de la verificación en dos pasos que se abre, se muestra la clave secreta.
4. Ingrese la clave secreta en la aplicación del autenticador para recibir un código de seguridad que se puede usar una sola vez. Puede especificar la clave secreta en la aplicación de autenticación manualmente o escanear el código QR con su dispositivo móvil.
5. Especifique el código de seguridad generado por la aplicación de autenticación y luego haga clic en el botón **Aceptar** para salir de la ventana de propiedades de la verificación en dos pasos.
6. Haga clic en el botón **Aplicar**.
7. Haga clic en el botón **Aceptar**.

La verificación en dos pasos queda activada para su cuenta.

Activación de la verificación en dos pasos para todos los usuarios

Puede activar la verificación en dos pasos para todos los usuarios del Servidor de administración si su cuenta tiene el derecho Modificar ACL de objetos en el área funcional **Funciones generales: Permisos de usuario** y si está autenticado mediante la verificación en dos pasos. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para todos los usuarios, la aplicación abre la ventana para habilitar la verificación en dos pasos para su propia cuenta.

Para activar la verificación en dos pasos para todos los usuarios:

1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.

2. En la ventana Propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado**, y luego **Verificación en dos pasos**.

3. Haga clic en el botón **Establecer como obligatoria** para activar la verificación en dos pasos para todos los usuarios.

4. En la sección **Verificación en dos pasos**, haga clic en el botón **Aplicar** y luego haga clic en el botón **Aceptar**.

La verificación en dos pasos queda activada para todos los usuarios. A partir de ahora, todos los usuarios del Servidor de administración, incluidos los usuarios que se agregaron después de habilitar esta opción, tienen que configurar la verificación en dos pasos para sus cuentas. La excepción son los usuarios cuyas cuentas estén excluidas de la verificación en dos pasos.

Desactivación de la verificación en dos pasos de una cuenta de usuario

Para desactivar la verificación en dos pasos para su propia cuenta:

1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.

2. En la ventana Propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado**, y luego **Verificación en dos pasos**.

3. En la sección **Verificación en dos pasos**, haga clic en el botón **Desactivar**.

4. Haga clic en el botón **Aplicar**.

5. Haga clic en el botón **Aceptar**.

La verificación en dos pasos queda desactivada para su cuenta.

Puede desactivar la verificación en dos pasos de las cuentas de otros usuarios. Esto provee protección en caso de que, por ejemplo, un usuario pierda o rompa un dispositivo móvil.

> Puede desactivar la verificación en dos pasos de la cuenta de otro usuario solo si tiene el derecho Modificar LCA de objeto en el área funcional **Características generales: Permisos de usuario**. Siguiendo los pasos a continuación, también puede desactivar la verificación en dos pasos para su propia cuenta.

Para desactivar la verificación en dos pasos de cualquier cuenta de usuario:

1. En el árbol de consola, abra la carpeta **Cuentas de usuario**.

   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado** de forma predeterminada.

2. En el espacio de trabajo, haga doble clic en la cuenta de usuario para la que desea desactivar la verificación en dos pasos.

3. En la ventana **Propiedades:<user name>** que se abre, seleccione la sección **Verificación en dos pasos**.

4. En la sección **Verificación en dos pasos**, seleccione las siguientes opciones:

   - Si desea desactivar la verificación en dos pasos para una cuenta de usuario, haga clic en el botón **Desactivar**.

- Si desea excluir esta cuenta de usuario de la verificación en dos pasos, seleccione la opción **El usuario puede y pasar la autenticación utilizando solo el nombre de usuario y la contraseña**.

5. Haga clic en el botón **Aplicar**.

6. Haga clic en el botón **Aceptar**.

La verificación en dos pasos para una cuenta de usuario queda desactivada.

Desactivar la verificación en dos pasos para todos los usuarios

Puede desactivar la verificación en dos pasos para todos los usuarios del Servidor de administración si su cuenta tiene el derecho Modificar ACL de objetos en el área funcional **Funciones generales: Permisos de usuario** y si está autenticado mediante la verificación en dos pasos.

Para desactivar la verificación en dos pasos para todos los usuarios:

1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.

2. En la ventana Propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado**, y luego **Verificación en dos pasos**.

3. Haga clic en el botón **Establecer como opcional** para desactivar la verificación en dos pasos para todos los usuarios.

4. Haga clic en el botón **Aplicar** en la sección **Verificación en dos pasos**.

5. Haga clic en el botón **Aceptar** en la sección **Verificación en dos pasos**.

La verificación en dos pasos queda desactivada para todos los usuarios.

Exclusión de cuentas de la verificación en dos pasos

Puede excluir una cuenta de la verificación en dos pasos s si su cuenta tiene el derechos Modificar LCA de objetos en el área funcional **Funciones generales: Permisos de usuario**.

Si una cuenta de usuario se excluye de la verificación en dos pasos, ese usuario puede iniciar sesión en la Consola de administración o en Kaspersky Security Center 14 Web Console sin la verificación en dos pasos.

Puede ser necesario excluir cuentas de la verificación en dos pasos para las cuentas de servicio que no pueden pasar el código de seguridad durante la autenticación.

Para excluir una cuenta de usuario de la verificación en dos pasos, haga lo siguiente:

1. Si desea excluir una cuenta de Active Directory, realice un sondeo de Active Directory para actualizar la lista de usuarios del Servidor de administración.

2. En el árbol de consola, abra la carpeta **Cuentas de usuario**.

La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta **Avanzado** de forma predeterminada.

3. En el espacio de trabajo, haga doble clic en la cuenta de usuario que desea excluir de la verificación en dos pasos
4. En la ventana **Propiedades:<user name>** que se abre, seleccione la sección **Verificación en dos pasos**.
5. En la sección abierta, seleccione la opción **El usuario puede y pasar la autenticación utilizando solo el nombre de usuario y la contraseña**.
6. En la sección **Verificación en dos pasos**, haga clic en el botón **Aplicar** y luego haga clic en el botón **Aceptar**.

Esta cuenta de usuario está excluida de la verificación en dos pasos. Puede consultar las cuentas excluidas en la lista de cuentas de usuario.

Modificar el nombre de un emisor del código de seguridad

Puede tener varios identificadores (se denominan emisores) para diferentes Servidores de administración. Puede cambiar el nombre de un emisor de código de seguridad, por ejemplo, en caso de que el Servidor de administración ya utilice un nombre similar de emisor de código de seguridad para otro Servidor de administración. De forma predeterminada, el nombre del emisor del código de seguridad es el mismo que el del Servidor de administración.

Después de cambiar el nombre del emisor del código de seguridad, debe volver a emitir una nueva clave secreta y pasarla a la aplicación de autenticación.

Para especificar un nuevo nombre de un emisor del código de seguridad:

1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y luego seleccione **Propiedades**.
2. En la ventana Propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Avanzado**, y luego **Verificación en dos pasos**.
3. Especifique un nuevo nombre de emisor de código de seguridad en el campo **Emisor del código de seguridad**.
4. Haga clic en el botón **Aplicar** en la sección **Verificación en dos pasos**.
5. Haga clic en el botón **Aceptar** en la sección **Verificación en dos pasos**.

Se especifica un nuevo nombre de emisor de código de seguridad para el Servidor de administración.

Gestión de grupos de administración

Esta sección proporciona información sobre la forma de manejar grupos de administración.

Puede realizar las acciones siguientes en los grupos de administración:

- Agregar a los grupos de administración cualquier número de grupos anidados de cualquier nivel de jerarquía.
- Agregar dispositivos a grupos de administración.

- Cambiar la jerarquía de los grupos de administración moviendo dispositivos individuales y los grupos enteros a otros grupos.
- Quitar grupos anidados y dispositivos de los grupos de administración.
- Añadir Servidores de administración secundarios y virtuales a los grupos de administración.
- Mover los dispositivos de los grupos de administración de un Servidor de administración a los de otro servidor.
- Definir qué aplicaciones Kaspersky se instalarán automáticamente en los dispositivos incluidos en un grupo.

Puede realizar estas acciones solo si tiene el permiso Modificar en el área **Administración de grupos de administración** para los grupos de administración que desea administrar (o para el Servidor de administración al que pertenecen estos grupos).

Creación de grupos de administración

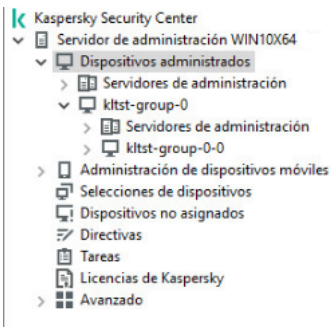
La jerarquía de los grupos de administración se crea en la ventana principal de la aplicación de Kaspersky Security Center, en la carpeta **Dispositivos administrados**. Los grupos de administración se muestran como carpetas en el árbol de consola (consulte la figura siguiente).

Inmediatamente después de la instalación de Kaspersky Security Center, la carpeta **Dispositivos administrados** contiene solo una carpeta **Servidores de administración** vacía.

> Los parámetros de la interfaz de usuario determinan si aparece en el árbol de consola la carpeta **Servidores de administración**. Para mostrar esta carpeta, en la barra del menú, seleccione **Ver → Configuración de la interfaz** y en la ventana **Configuración de la interfaz** que se abre seleccione la casilla **Mostrar Servidores de administración secundarios**.

Al crear una jerarquía de grupos de administración, puede añadir dispositivos y máquinas virtuales a la carpeta **Dispositivos administrados** y añadir grupos anidados. Se pueden añadir Servidores de administración secundarios y virtuales en la carpeta **Servidores de administración**.

Al igual que el grupo **Dispositivos administrados**, inicialmente, cada grupo creado contiene únicamente la carpeta **Servidores de administración**, que está vacía y cuyo objetivo es trabajar con los Servidores de administración secundarios y virtuales de este grupo. La información sobre las directivas y las tareas de este grupo, así como la información sobre los dispositivos incluidos en este grupo, se muestra en las pestañas con los nombres correspondientes en el espacio de trabajo de este grupo.



Visualización de la jerarquía de los grupos de administración

Para crear un grupo de administración:

1. En el árbol de consola, expanda la carpeta **Dispositivos administrados**.
2. Si quiere crear un subgrupo en un grupo de administración existente, en la carpeta **Dispositivos administrados** seleccione la subcarpeta que corresponda a ese grupo, que va a incluir el grupo de administración nuevo.

   Si crea un grupo de administración nuevo de nivel superior, puede saltarse este paso.
3. Inicie de creación del grupo de administración de una de las maneras siguientes:

   - Mediante el comando **Nuevo** → **Grupo** en el menú contextual.
   - Haciendo clic en el botón **Grupo nuevo** que se encuentra en el espacio de trabajo de la ventana principal de la aplicación, en la ficha **Dispositivos**.
4. En la ventana **Nombre de grupo** que se abrirá, introduzca un nombre para el grupo y haga clic en **Aceptar**.

Aparecerá una nueva carpeta del grupo de administración con el nombre especificado en el árbol de consola.

La aplicación permite crear una jerarquía de grupos de administración basada en la estructura de Active Directory o la estructura de la red de dominios. También es posible crear una estructura de grupos a partir de un archivo de texto.

Para crear una estructura de grupos de administración:

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
2. En el menú contextual de la carpeta **Dispositivos administrados**, seleccione **Todas las tareas** → **Nueva estructura de grupo**.

Asistente de nueva estructura de grupos de administración. Siga las instrucciones del Asistente.

Traslado de grupos de administración

Se pueden mover grupos de administración anidados dentro de la jerarquía de grupo.

Un grupo de administración se mueve junto con todos sus grupos secundarios, Servidores de administración secundarios, dispositivos, directivas y tareas de grupo. El sistema aplicará al grupo todos los parámetros que correspondan a la nueva posición en la jerarquía de grupos de administración.

El nombre del grupo debería ser único dentro de un mismo nivel jerárquico. Si en la carpeta a la que se traslada el grupo de administración ya existe un grupo con el mismo nombre, deberá cambiar el nombre del último. Si no cambia el nombre del grupo que ha movido, se agrega automáticamente un índice con el formato **(<siguiente número secuencial>)** a su nombre cuando se mueva; por ejemplo: **(1)**, **(2)**.

No se puede renombrar la carpeta **Dispositivos administrados** porque es un elemento integrado de la Consola de administración.

Para trasladar un grupo a otra carpeta del árbol de consola, realice lo siguiente:

1. Seleccione un grupo para trasladar del árbol de consola.
2. Realice una de las siguientes acciones:

   - Mueva el grupo con el menú contextual:

1. Seleccione **Cortar** en el menú contextual del grupo.
2. Seleccione **Pegar** en el menú contextual del grupo de administración al que necesita mover el grupo seleccionado.

- Mueva el grupo con el menú principal de la aplicación:
  a. En el menú principal, seleccione **Acción → Cortar**.
  b. Seleccione el grupo de administración al que necesita mover el grupo seleccionado del árbol de consola.
  c. En el menú principal, seleccione **Acción → Pegar**.
- Con el ratón, mueva el grupo a otro grupo en el árbol de consola.

Eliminación de grupos de administración

Se puede eliminar un grupo de administración siempre que no tenga Servidores de administración secundarios, grupos anidados o dispositivos cliente, y que no se le haya creado ninguna tarea o directiva de grupo.

Antes de eliminar un grupo de administración, hay que eliminar todos los Servidores de administración secundarios, grupos anidados y dispositivos cliente que pueda tener.

Para eliminar un grupo, realice lo siguiente:

1. Seleccione un grupo de administración en el árbol de consola.
2. Realice una de las siguientes acciones:
   - Seleccione **Eliminar** en el menú contextual del grupo.
   - En el menú de la aplicación principal, seleccione **Acción → Eliminar**.
   - Pulse la tecla **`SUPRIMIR`**.

Creación automática de una estructura de grupos de administración

Kaspersky Security Center le permite crear una estructura de grupos de administración con el Asistente para crear una jerarquía de grupos.

El Asistente crea una estructura de grupos de administración en función de los datos siguientes:

- Estructuras de dominios de Windows y grupos de trabajo
- Estructuras de los grupos de Active Directory
- Contenido del archivo de texto creado manualmente por el administrador

Cuando el archivo de texto se genera, se deben cumplir los requisitos siguientes:

- El nombre de cada grupo nuevo debe comenzar con una nueva línea; el separador con un salto de línea. Las líneas en blanco se ignoran.

  Ejemplo:

  Oficina 1

  Oficina 2

  Oficina 3

  Se deben crear tres grupos del primer nivel de jerarquía en el grupo de destino.

- El nombre del grupo anidado se debe introducir con una barra (/).

  Ejemplo:

  Oficina 1/División 1/Departamento 1/Grupo 1

  Se crearán cuatro subgrupos anidados unos dentro de otros en el grupo de destino.

- Para crear varios grupos anidados del mismo nivel de jerarquía, debe especificar la "ruta completa al grupo".

  Ejemplo:

  Oficina 1/División 1/Departamento 1

  Oficina 1/División 2/Departamento 1

  Oficina 1/División 3/Departamento 1

  Oficina 1/División 4/Departamento 1

  Deberá crearse un grupo de la Oficina 1 del primer nivel de jerarquía en el grupo de destino. Este grupo incluirá cuatro grupos anidados del mismo nivel jerárquico: "División 1", "División 2", "División 3" y "División 4". En cada uno de ellos se incluirá el grupo "Departamento 1".

La creación de la jerarquía de grupos de administración a través del Asistente no afecta a la integridad de la red: en vez de reemplazar los grupos existentes, los nuevos grupos se añaden. Un dispositivo cliente no se puede incluir en un grupo de administración por segunda vez, porque el dispositivo se elimina del grupo de dispositivos **Dispositivos no asignados** cuando se mueve al grupo de administración.

Si al crear la estructura del grupo de administración, un dispositivo no se incluyera en el grupo **Dispositivos no asignados** por la razón que sea (se apagó o se desconectó de la red), el dispositivo no se moverá automáticamente al grupo de administración. Puede agregar manualmente dispositivos a los grupos de administración después de que el Asistente concluya su operación.

Para iniciar la creación automática de una estructura de grupos de administración:

1. Seleccione la carpeta **Dispositivos administrados** en el árbol de consola.
2. En el menú contextual de la carpeta **Dispositivos administrados**, seleccione **Todas las tareas** → **Nueva estructura de grupo**.

   Asistente de nueva estructura de grupos de administración. Siga las instrucciones del Asistente.

Instalación automática de aplicaciones en dispositivos dentro de un grupo de administración

Puede especificar qué paquetes de instalación deben utilizarse para la instalación remota automática de aplicaciones Kaspersky en los dispositivos cliente que hayan sido agregados al grupo recientemente.

Siga estos pasos para configurar la instalación automática de aplicaciones en los nuevos dispositivos de un grupo de administración:

1. En el árbol de consola, seleccione el grupo de administración requerido.
2. Abra la ventana de propiedades del grupo de administración.
3. En el panel **Secciones**, seleccione **Instalación automática** y, en el espacio de trabajo, seleccione los paquetes de instalación de las aplicaciones que se instalarán en los nuevos dispositivos.
4. Haga clic en **Aceptar**.

Se crean tareas de grupo. Estas tareas se ejecutarán en los dispositivos cliente inmediatamente después de que hayan sido añadidos al grupo de administración.

Si algunos paquetes de instalación de una aplicación se seleccionaron para su instalación automática, la tarea de instalación se creará únicamente para la versión más reciente de la aplicación.

Administración de dispositivos cliente

Esta sección contiene información sobre cómo trabajar con los dispositivos cliente.

Conexión de dispositivos cliente al Servidor de administración

La conexión del dispositivo cliente al Servidor de administración se establece a través del Agente de red instalado en el dispositivo cliente.

Cuando un dispositivo cliente se conecta con el Servidor de administración, se realizan las siguientes operaciones:

- Sincronización automática de datos:
  - Sincronización de la lista de aplicaciones para el dispositivo cliente.
  - Sincronización de las directivas, ajustes de la aplicación, tareas y parámetros de tarea.
- Recuperación de información actualizada por el Servidor de administración acerca de la condición de las aplicaciones, ejecución de tareas y estadísticas del funcionamiento de la aplicación.
- Envío de la información de los eventos al Servidor de administración para su procesamiento.

La sincronización automática de datos se realiza regularmente de acuerdo con los parámetros del Agente de red (por ejemplo, cada 15 minutos). Se puede especificar el intervalo de conexión manualmente.

La información acerca de un evento se envía al Servidor de administración en cuanto se produce.

Si un Servidor de administración está ubicado remotamente fuera de una red corporativa, los dispositivos cliente se conectarán a este a través de Internet.

Para que los dispositivos se conecten a un Servidor de administración a través de Internet, se deben cumplir los siguientes requisitos:

- El Servidor de administración remoto deberá disponer de una dirección IP externa y el puerto de entrada 13000 deberá permanecer abierto (para la conexión de Agentes de red). Le recomendamos que también abra el puerto UDP 13000 (para recibir notificaciones cuando se apaguen los dispositivos).
- Primero deben instalarse los Agentes de red en los dispositivos.
- Al instalar el Agente de red en dispositivos, debe especificar la dirección IP externa del Servidor de administración remoto. Si se utiliza un paquete de instalación, especifique manualmente la dirección IP externa en las propiedades del paquete de instalación en la sección **Configuración**.
- Para usar el Servidor de administración remoto con el fin de administrar las aplicaciones y tareas de un dispositivo, en la ventana de propiedades de ese dispositivo, en la sección **General**, elija la casilla **No desconectar del Servidor de administración**. Una vez que la casilla está seleccionada, espere a que el Servidor de administración esté sincronizado con el dispositivo cliente remoto. El número de dispositivos cliente que mantienen una conexión continua con un Servidor de administración remoto no puede superar los 300.

Para aumentar el rendimiento de las tareas generadas por un Servidor de administración remoto, puede abrir el puerto 15000 en el dispositivo. En este caso, para ejecutar una tarea, el Servidor de administración envía un paquete especial al Agente de red a través del puerto 15000 sin esperar a que se complete la sincronización con el dispositivo.

Kaspersky Security Center le permite configurar la conexión entre un dispositivo cliente y el Servidor de administración para que la conexión permanezca activa después de completarse todas las operaciones. Se debe utilizar una conexión sin interrupciones en el caso de que se requiera la monitorización en tiempo real del estado de una aplicación y que el Servidor de administración sea incapaz de establecer una conexión con el cliente por algún motivo (por ejemplo, la conexión se encuentra protegida por un firewall, no se permite la apertura de los puertos del dispositivo cliente, la dirección IP del cliente es desconocida, etc.). Puede establecer una conexión ininterrumpida entre un dispositivo cliente y el Servidor de administración en la ventana de propiedades del dispositivo cliente, en la sección **General**.

Le recomendamos que establezca una conexión ininterrumpida con los dispositivos más importantes. El número total de conexiones mantenidas simultáneamente por el Servidor de administración se limita a 300.

Cuando se sincroniza manualmente, el sistema utiliza un método de conexión auxiliar que permite al Servidor de administración iniciar la conexión. Antes de establecer la conexión en un dispositivo cliente, deberá abrir el puerto UDP. El Servidor de administración envía una petición de conexión al puerto UDP del dispositivo cliente. En respuesta, se verifica el certificado del Servidor de administración. Si el certificado del Servidor de administración coincide con la copia del certificado almacenada en el dispositivo cliente, se inicia el establecimiento de la conexión.

Ejecutar la sincronización manualmente también se utiliza para obtener información actualizada acerca de la condición de las aplicaciones, la ejecución de tareas y las estadísticas de funcionamiento de las aplicaciones.

Conexión manual del dispositivo cliente al Servidor de administración. Utilidad Klmover

Si necesita conectar un dispositivo cliente al Servidor de administración, puede usar la utilidad klmover en el dispositivo cliente.

Cuando se instala el Agente de red en un dispositivo cliente, la utilidad se copia automáticamente a la carpeta de instalación del Agente de red.

Para conectar de forma manual un dispositivo cliente al Servidor de administración con la utilidad klmover,

inicie la utilidad klmover desde la línea de comandos en el dispositivo cliente.

Cuando se inicia desde la línea de comandos, la utilidad klmover puede realizar las siguientes acciones (según cuáles sean las claves que estén en uso):

- Conectar el Agente de red al Servidor de administración con los parámetros especificados.
- Registrar los resultados del funcionamiento en el archivo de registro de eventos o mostrarlos en pantalla.

Sintaxis de línea de comandos de la utilidad:

```
klmover [-logfile <nombre de archivo>] [-address <dirección del servidor>] [-pn <número de puerto>] [-ps < número de puerto SSL>] [-nossl] [-cert <ruta al archivo de certificado>] [-silent] [-dupfix]
```

Se requieren derechos de administrador para ejecutar la utilidad.

Descripciones de las claves:

- `-logfile <nombre de archivo>`: Registrar los resultados de ejecución de la utilidad en un archivo de registro.

  De forma predeterminada, la información se almacenará en el flujo de salida estándar (stdout). Si la clave no está en uso, los resultados y los mensajes de error se mostrarán en pantalla.

- `-address <dirección del servidor>:` Dirección del Servidor de administración para la conexión.

  Como dirección de un dispositivo, se puede especificar una dirección IP, un nombre NetBIOS o un nombre DNS.

- `-pn <número de puerto>`: número del puerto por el que se establecerá la conexión no cifrada al Servidor de administración.

  El número de puerto predeterminado es el 14000.

- `-ps <número de puerto SSL>`: número del puerto SSL por el que se establecerá la conexión cifrada al Servidor de administración, con protocolo SSL.

  El número de puerto predeterminado es el 13000.

- `-nossl`: Usar conexión no cifrada al Servidor de administración.

  Si la clave no está en uso, el Agente de red se conecta al Servidor de administración mediante el protocolo cifrado SSL.

- `-cert <ruta al archivo certificado>`: Utilizar el archivo de certificado especificado para la autenticación del acceso al Servidor de administración.

  Si la clave no está en uso, el Agente de red recibirá un certificado la primera vez que se conecte al Servidor de administración.

- `-silent`: Ejecutar la utilidad en modo silencioso.

  El uso de la clave puede ser útil cuando, por ejemplo, la utilidad se inicia con el script de inicio de sesión al registrarse el usuario.

- `-dupfix`: Esta clave se utiliza si el Agente de red se ha instalado con un método distinto del habitual (con el paquete de distribución); por ejemplo, recuperado de una imagen de disco ISO.

Conexión de túnel entre un dispositivo cliente y el Servidor de administración

Kaspersky Security Center permite los túneles de conexiones de TCP desde la Consola de administración mediante el Servidor de administración y, luego, mediante el Agente de red a un puerto especificado en un dispositivo administrado. El túnel está diseñado para conectar una aplicación cliente en un dispositivo con la Consola de administración instalada en un puerto TCP en un dispositivo administrado si una conexión directa entre la Consola de administración y el dispositivo de destino no es posible.

Por ejemplo, el túnel se utiliza para las conexiones con un escritorio remoto, tanto para la conexión con una sesión existente como para crear una nueva sesión remota.

El túnel también puede activarse usando herramientas externas. Por ejemplo, el administrador puede ejecutar la utilidad putty, el cliente VNC y otras herramientas de esta manera.

Se requerirá una conexión por túnel entre un dispositivo cliente remoto y el Servidor de administración si el puerto usado para la conexión con el Servidor de administración no está disponible en el dispositivo. Es posible que el puerto del dispositivo no esté disponible en los siguientes casos:

- El dispositivo remoto está conectado a una red local que utiliza un mecanismo NAT.
- El dispositivo remoto forma parte de la red local del Servidor de administración pero su puerto está cerrado en el firewall.

Para hacer una conexión de túnel entre el dispositivo cliente y el Servidor de administración:

1. En el árbol de consola seleccione el grupo de administración que contiene el dispositivo cliente.
2. En la ficha **Dispositivos**, seleccione el dispositivo.
3. En el menú contextual del dispositivo, seleccione **Todas las tareas → Conexión de túnel**.
4. Cree un túnel en la ventana **Conexión de túnel** que se abre.

Conexión remota con el escritorio de un dispositivo cliente

El administrador puede obtener acceso remoto al escritorio de un dispositivo cliente mediante el Agente de red instalado en el dispositivo. También se puede realizar la conexión remota a un dispositivo con Agente de red, incluso si los puertos TCP y UDP del dispositivo cliente están cerrados.

Cuando se establece una conexión con el dispositivo, el administrador obtiene acceso total a la información almacenada en dicho dispositivo, de modo que podrá administrar las aplicaciones que haya instaladas en él.

La conexión remota con un dispositivo se puede establecer de una de estas formas:

- Mediante un componente estándar de Microsoft Windows denominado Conexión a Escritorio remoto. La conexión a un escritorio remoto se establece con la utilidad estándar mstsc.exe de Windows de acuerdo con la configuración de esta utilidad.

  La conexión a la sesión del escritorio remoto actual del usuario se establece sin que el usuario lo sepa. Cuando el administrador se conecta a la sesión, el usuario del dispositivo se desconecta de la sesión sin previo aviso.

- Mediante la tecnología Uso compartido del escritorio de Windows. Al conectarse a una sesión existente del escritorio remoto, el usuario de la sesión del dispositivo recibe una solicitud del administrador para establecer la conexión. No se guardará ninguna información sobre la actividad en remoto del dispositivo ni de sus resultados en los informes creados por Kaspersky Security Center.

  El administrador se puede conectar a una sesión existente en un dispositivo cliente sin desconectar al usuario que la está utilizando. En ese caso, tanto el administrador como el usuario de la sesión del dispositivo comparten el acceso al escritorio.

  El administrador puede configurar una auditoría de la actividad del usuario en un dispositivo cliente remoto. Durante la auditoría, la aplicación guarda información sobre los archivos del dispositivo cliente que el administrador haya abierto o modificado.

Para conectarse al escritorio de un dispositivo cliente mediante Uso compartido del escritorio de Windows, se deben cumplir estas condiciones:

- En el dispositivo cliente está instalado Microsoft Windows Vista o un sistema operativo de Windows posterior.
- En la estación de trabajo del administrador está instalado Microsoft Windows Vista o un sistema operativo de Windows posterior. El tipo de sistema operativo del dispositivo que aloja el Servidor de administración no impone ninguna restricción a la conexión mediante Uso compartido del escritorio de Windows.
- Kaspersky Security Center usa una licencia para la Administración de vulnerabilidades y parches.

Para conectarse al escritorio de un dispositivo cliente mediante el componente Conexión a Escritorio remoto:

1. En el árbol de la Consola de administración, seleccione el dispositivo al que necesita acceder.
2. En el menú contextual del dispositivo, seleccione **Todas las tareas → Conectar a dispositivo → Sesión RDP nueva**.

   Se inicia la utilidad estándar mstsc.exe de Windows, que ayuda a establecer la conexión al escritorio remoto.
3. Siga las instrucciones que se muestran en los cuadros de diálogo de la utilidad.

Cuando se establece la conexión al dispositivo, el escritorio está disponible en la ventana Conexión a escritorio remoto de Microsoft Windows.

Para conectarse al escritorio de un dispositivo cliente mediante el componente Uso compartido del escritorio de Windows:

1. En el árbol de la Consola de administración, seleccione el dispositivo al que necesita acceder.
2. En el menú contextual del dispositivo, seleccione **Todas las tareas → Conectar a dispositivo → Uso compartido del escritorio de Windows**.
3. En la ventana **Seleccionar la sesión del escritorio remoto** que se abre, seleccione la sesión en el dispositivo al que necesite conectarse.

   Si la conexión al dispositivo se establece correctamente, el escritorio del dispositivo estará disponible en la ventana **Visor de sesión del escritorio remoto de Kaspersky**.
4. Para comenzar a interactuar con el dispositivo, en el menú principal de la ventana **Visor de sesión del escritorio remoto de Kaspersky**, seleccione **Acciones → Modo interactivo**.

Conexión con los dispositivos mediante Uso compartido del escritorio de Windows

Para conectar un dispositivo cliente mediante el Uso compartido del escritorio de Windows:

1. En el árbol de consola, en la ficha **Dispositivos**, seleccione la carpeta **Dispositivos administrados**.

   El espacio de trabajo de esta carpeta muestra la lista de dispositivos.

2. En el menú contextual del dispositivo al que desea conectarse, seleccione **Conectar a dispositivo → Uso compartido del escritorio de Windows**.

   Se abre la ventana **Seleccionar la sesión del escritorio remoto**.

3. En la ventana **Seleccionar la sesión del escritorio remoto**, seleccione una sesión de escritorio para la conexión al dispositivo cliente.

4. Haga clic en **Aceptar**.

El dispositivo está conectado.

Configuración del reinicio de un dispositivo cliente

Al usar, instalar o quitar Kaspersky Security Center, debería reiniciar el dispositivo. Puede especificar la configuración de reinicio solo para dispositivos que ejecuten Windows.

Para configurar el reinicio de un dispositivo cliente:

1. En el árbol de consola, seleccione el grupo de administración cuyo reinicio se deba configurar.

2. En el espacio de trabajo del grupo, seleccione la tabla **Directivas**.

3. En el espacio de trabajo, seleccione una directiva del Agente de red de Kaspersky Security Center de la lista y, a continuación, seleccione **Propiedades** en el menú contextual de la directiva.

4. En la ventana de propiedades de la directiva, seleccione la ficha **Administración de reinicios**.

5. Seleccione la acción que se debe realizar cuando se requiera el reinicio del dispositivo:

   - Seleccione **No reiniciar el sistema operativo** para bloquear el reinicio automático.
   - Seleccione **Reiniciar el sistema operativo automáticamente de ser necesario** para permitir el reinicio automático.
   - Seleccione **Solicitar al usuario una acción** para habilitar la solicitud al usuario de permitir el reinicio.

   Puede especificar la frecuencia de las solicitudes de reinicio, y habilitar el reinicio forzado y el cierre forzado de aplicaciones de sesiones bloqueadas del dispositivo si selecciona las casillas de verificación correspondientes y las configuraciones de tiempo en casillas de giro.

6. Haga clic en el botón **Aceptar** para guardar los cambios y cerrar la ventana de propiedades de la directiva.

El reinicio del dispositivo se configurará ahora.

Auditoría de acciones de un dispositivo cliente remoto

La aplicación permite la auditoría de las acciones del administrador en dispositivos cliente remotos que ejecutan Windows. Durante la auditoría, la aplicación guarda en el dispositivo información sobre los archivos que el administrador ha abierto o modificado. La auditoría de las acciones del administrador puede realizarse cuando se cumplen estas condiciones:

- La licencia de Administración de vulnerabilidades y parches está en uso.
- El administrador dispone del derecho para iniciar el acceso compartido al escritorio del dispositivo remoto.

Para habilitar la auditoría de acciones en un dispositivo cliente remoto:

1. En el árbol de consola, seleccione el grupo de administración para el que debe configurar la auditoría de acciones del administrador.
2. En el espacio de trabajo del grupo, seleccione la tabla **Directivas**.
3. Seleccione una directiva del Agente de red de Kaspersky Security Center y, a continuación, seleccione **Propiedades** en el menú contextual de la directiva.
4. En la ventana de propiedades de la directiva, seleccione la ficha **Uso compartido del escritorio de Windows**.
5. Selecciona la casilla de verificación **Activar auditorías**.
6. En las listas **Máscaras de los archivos que se deben supervisar cuando se leen** y **Máscaras de archivos que supervisar cuando se modifiquen**, añada máscaras de archivos en las que la aplicación debe supervisar las acciones durante la auditoría.

   De forma predeterminada, la aplicación supervisa acciones en archivos con extensiones txt, rtf, doc, xls, docx, xlsx, odt y pdf.
7. Haga clic en el botón **Aceptar** para guardar los cambios y cerrar la ventana de propiedades de la directiva.

De este modo, queda configurada la auditoría de las acciones del administrador en el dispositivo remoto del usuario con acceso a escritorio compartido.

Las acciones del administrador en el dispositivo remoto se registran:

- En el registro de eventos del dispositivo remoto.
- En un archivo con extensión syslog ubicado en la carpeta de instalación del Agente de red en el dispositivo remoto (p. ej., C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- En la base de datos de eventos de Kaspersky Security Center.

Comprobación de la conexión entre un dispositivo cliente y el Servidor de administración.

Kaspersky Security Center permite comprobar automática o manualmente las conexiones entre un dispositivo cliente y el Servidor de administración.

En el Servidor de administración se realiza una comprobación automática de la conexión. La comprobación manual de la conexión se ejecuta en el dispositivo cliente.

Comprobación automática de la conexión entre un dispositivo cliente y el Servidor de administración.

Para iniciar una comprobación automática de la conexión entre un dispositivo cliente y el Servidor de administración:

1. En el árbol de consola seleccione el grupo de administración que incluye el dispositivo.
2. En el espacio de trabajo del grupo de administración, en la ficha **Dispositivos** seleccione el dispositivo.
3. En el menú contextual del dispositivo, seleccione **Comprobar accesibilidad del dispositivo**.

Esto abre una ventana que contiene información sobre la accesibilidad del dispositivo.

Comprobación manual de la conexión entre un dispositivo cliente y el Servidor de administración. Utilidad klnagchk

Se puede comprobar la conexión y obtener información detallada sobre los parámetros de conexión entre el dispositivo cliente y el Servidor de administración con la utilidad klnagchk.

Cuando se instala el Agente de red en un dispositivo, la utilidad klnagchk se copia automáticamente a la carpeta de instalación del Agente de red.

Cuando se inicia desde la línea de comandos, la utilidad klnagchk puede realizar las siguientes acciones (según cuáles sean las claves que haya en uso):

- Mostrar en la pantalla o los registros los valores de la configuración usada para conectar el Agente de red instalado en el dispositivo al Servidor de administración.
- Registra las estadísticas del Agente de red en un archivo de registro de eventos (desde el último inicio) y los resultados del funcionamiento, o muestra la información en pantalla.
- Hace un intento de establecer conexión entre el Agente de red y el Servidor de administración.

  Si el intento de conexión falla, la utilidad envía un paquete ICMP para comprobar el estado del dispositivo en el que está instalado el Servidor de administración.

Para comprobar la conexión entre el dispositivo cliente y el Servidor de administración con la utilidad klnagchk,

inicie la utilidad klnagchk desde la línea de comandos en el dispositivo cliente.

Sintaxis de línea de comandos de la utilidad:

```
klnagchk [-logfile <nombre de archivo>] [-sp] [-savecert <ruta al archivo de
certificado>] [-restart]
```

Descripciones de las claves:

- `-logfile <nombre de archivo>`: registra los valores de los parámetros de conexión entre el Agente de red y el Servidor de administración, y los resultados de funcionamiento de la utilidad en un archivo de registro.

De forma predeterminada, la información se almacenará en el flujo de salida estándar (stdout). Si la clave no está en uso, los parámetros, los resultados y los mensajes de error se mostrarán en pantalla.

- `-sp`: Mostrar la contraseña de autenticación del usuario en el servidor proxy.

  Este parámetro está en uso si la conexión al Servidor de administración se establece a través de un servidor proxy.

- `-savecert <nombre de archivo>`: Guardar en el archivo especificado el certificado usado para el acceso al Servidor de administración.

- `-restart`: Reinicia el Agente de red después de que se haya completado la utilidad.

Acerca de la comprobación de la hora de conexión entre un dispositivo y el Servidor de administración

Después de cerrar un dispositivo, el Agente de red notifica el Servidor de administración de este evento. En la Consola de administración, ese dispositivo se muestra como apagado. Sin embargo, el Agente de red no puede notificar al Servidor de administración de todos estos eventos. El Servidor de administración, por lo tanto, analiza periódicamente el atributo **Conectado al Servidor de administración** (el valor de este atributo se muestra en la Consola de administración, en las propiedades del dispositivo, en la sección **General**) para cada dispositivo y lo compara con el intervalo de sincronización de la configuración actual del Agente de red. Si un dispositivo no ha respondido durante más de tres intervalos de sincronización sucesivos, ese dispositivo se marca como apagado.

Identificación de dispositivos cliente en el Servidor de administración

Los dispositivos cliente se identifican según sus nombres. El nombre de un dispositivo es único entre todos los nombres de los dispositivos conectados al Servidor de administración.

El nombre de un dispositivo se transfiere al Servidor de administración cuando se sondea la red de Windows y se detecta un nuevo dispositivo o durante la primera conexión del Agente de red instalado en un dispositivo con el Servidor de administración. De forma predeterminada, el nombre coincide con el nombre del dispositivo en la red Windows (nombre NetBIOS). Si ya existe un dispositivo cliente registrado con ese nombre en el Servidor de administración, se agregará un número al nuevo nombre del dispositivo cliente, por ejemplo: **<Nombre>-1**, **<Nombre>-2**. El dispositivo cliente se agregará al grupo de administración con ese nombre.

Moviendo los dispositivos al grupo de administración

Puede mover dispositivos de un grupo de administración a otro solo si tiene el permiso **Modificar** en el **área Administración de grupos de administración** para los grupos de administración de origen y destino (o para el Servidor de administración al que pertenecen estos grupos).

Para incluir uno o varios dispositivos en un grupo de administración seleccionado:

1. En el árbol de consola, expanda la carpeta **Dispositivos administrados**.

2. En la carpeta **Dispositivos administrados**, seleccione la subcarpeta que corresponde al grupo en el que se incluirán los dispositivos cliente.

   Si quiere incluir los dispositivos en el grupo **Dispositivos administrados**, puede saltarse este paso.

3. En el espacio de trabajo del grupo de administración seleccionado, en la ficha **Dispositivos**, ejecute el proceso de inclusión de los dispositivos en el grupo mediante uno de los siguientes métodos:

- Al agregar dispositivos al grupo al hacer clic en el botón **Mover dispositivos al grupo** del recuadro de información para la lista de dispositivos.

- Al seleccionar **Crear** → **Dispositivo** en el menú contextual de la lista de dispositivos.

Se inicia el Asistente para mover dispositivos. Siga sus instrucciones y seleccione un método para mover los dispositivos al grupo y crear una lista de dispositivos que incluir en el grupo.

Si crea la lista de dispositivos de forma manual, puede utilizar una dirección IP (o un rango IP), un nombre NetBIOS o un nombre DNS como dirección de un dispositivo. Puede mover manualmente a la lista solo los dispositivos cuya información se haya agregado a la base de datos del Servidor de administración cuando se conecte el dispositivo o después de la detección de dispositivos.

Para importar la lista de dispositivos desde un archivo, especifique un archivo TXT con una lista que contenga las direcciones de los dispositivos que se van a agregar. Cada dirección debe especificarse en una línea independiente.

Cuando finaliza el Asistente, los dispositivos seleccionados se incluyen en el grupo de administración y se muestran en la lista de dispositivos con nombres generados por el Servidor de administración.

Puede mover un dispositivo cliente al grupo de administración seleccionado arrastrándolo de la carpeta **Dispositivos no asignados** a la carpeta del grupo de administración.

Cambio del Servidor de administración de los dispositivos cliente

Se puede cambiar el Servidor de administración que administra los dispositivos cliente por otro con la tarea **Cambiar Servidor de administración**.

Para cambiar el Servidor de administración que gestiona los dispositivos cliente a otro servidor:

1. Conéctese al Servidor de administración que administra los dispositivos.

2. Cree la tarea Cambiar Servidor de administración mediante uno de los siguientes métodos:

   - Si necesita cambiar el Servidor de administración de dispositivos incluidos en el grupo de administración seleccionado, cree una tarea para el grupo seleccionado.

   - Si necesita cambiar el Servidor de administración del dispositivo incluidos en distintos grupos de administración o que no están en ninguno de los grupos de administración existentes, cree una tarea para dispositivos específicos.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente. En la ventana **Seleccionar el tipo de tarea** del Asistente para añadir tareas, seleccione el nodo **Kaspersky Security Center**, abra la carpeta **Avanzado** y seleccione la tarea **Cambiar Servidor de administración**.

3. Ejecute la tarea creada.

Tras completarse la tarea, los dispositivos cliente para los que se la creó se ponen bajo la administración del Servidor de administración especificado en los parámetros de tarea.

Si el Servidor de administración admite el cifrado y la protección de datos, y está creando la tarea **Cambiar Servidor de administración**, aparecerá una advertencia. Esta advertencia especifica que, si hay datos cifrados almacenados en los dispositivos, después de que pasen a depender del nuevo Servidor, los usuarios podrán acceder solo a los datos cifrados con los cuales trabajaban anteriormente. En otros casos, no se proporcionará acceso a los datos cifrados. Para obtener descripciones detalladas sobre los escenarios en los que no se proporciona ningún acceso a datos cifrados, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows.

Matrices de servidores y clústeres

Kaspersky Security Center es compatible tecnología de clústeres. Si el Agente de red envía al Servidor de administración la información que confirma que la aplicación instalada en un dispositivo cliente pertenece a una matriz de servidores, el dispositivo cliente se convertirá en un nodo del clúster. El clúster se agregará como objeto individual a la carpeta **Dispositivos administrados** del árbol de consola con el icono  .

Pueden distinguirse algunas funciones típicas de un clúster:

- Un clúster y sus nodos siempre están en el mismo grupo de administración.
- Si el administrador intenta mover un nodo del clúster, el nodo se vuelve a su ubicación original.
- Si el administrador intenta mover un clúster a un grupo diferente, todos sus nodos se trasladarán con él.

Encendido, apagado y reinicio remotos de dispositivos cliente

Kaspersky Security Center le permite administrar dispositivos cliente de forma remota mediante su activación, cierre o reinicio.

Para administrar remotamente dispositivos cliente:

1. Conéctese al Servidor de administración que administra los dispositivos.
2. Cree una tarea de administración de dispositivos con uno de los métodos siguientes:
   - Si necesita encender, apagar o reiniciar Dispositivos incluidos en el grupo de administración seleccionado, cree una tarea para el grupo seleccionado.
   - Si necesita encender, apagar o reiniciar dispositivos incluidos en distintos grupos de administración o que no pertenecen a ninguno de ellos, cree una tarea para dispositivos específicos.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente. En la ventana **Seleccionar el tipo de tarea** del Asistente para añadir tareas, seleccione el nodo **Kaspersky Security Center**, abra la carpeta **Avanzado** y seleccione la tarea **Administrar dispositivos**.
3. Ejecute la tarea creada.

   Luego de finalizar la tarea, se ejecutará el comando (encender, apagar o reiniciar) en los dispositivos seleccionados.

Acerca del uso de la conexión continua entre un dispositivo administrado y el Servidor de administración

De forma predeterminada, Kaspersky Security Center no incluye la conectividad continua entre dispositivos administrados y el Servidor de administración. Los Agentes de red en los dispositivos administrados establecen conexiones periódicamente y se sincronizan con el Servidor de administración. El intervalo entre esas sesiones de sincronización se define en una directiva del Agente de red y es de 15 minutos de forma predeterminada. Si se requiere una sincronización temprana (por ejemplo, para forzar la aplicación de una directiva), el Servidor de administración envía un paquete de red firmado al Agente de red al puerto UDP 15000. (El Servidor de administración puede enviar este paquete a través de una red IPv4 o IPv6). Si no es posible ninguna conexión a través de UDP entre el Servidor de administración y un dispositivo administrado por ningún motivo, la sincronización se ejecutará en la siguiente conexión rutinaria entre el Agente de red y el Servidor de administración dentro del intervalo de sincronización.

Sin embargo, algunas operaciones no pueden realizarse sin una conexión temprana entre el Agente de red y el Servidor de administración. Estas operaciones incluyen la ejecución y detención de tareas locales, la recepción de estadísticas de una aplicación administrada y la creación de un túnel. Para posibilitar estas operaciones, debe activar la opción **No desconectar del Servidor de administración** en el dispositivo administrado.

Acerca de la sincronización forzada

Si bien Kaspersky Security Center sincroniza el estado, la configuración, las tareas y las directivas para los dispositivos administrados automáticamente, en algunos casos, el administrador debe saber exactamente si la sincronización ya se ha realizado para un dispositivo específico en ese momento.

En el menú contextual de los dispositivos administrados en la Consola de administración, el elemento de menú **Todas las tareas** contiene el comando **Forzar sincronización**. Cuando Kaspersky Security Center 14 ejecuta este comando, el Servidor de administración intenta conectarse al dispositivo. Si el intento tiene éxito, se realizará la sincronización forzada. De lo contrario, la sincronización se forzará y la casilla se desactivará únicamente después de la siguiente conexión planificada entre el Agente de red y el Servidor de administración.

Sobre la programación de conexiones

En la ventana de propiedades del Agente de red, en la sección **Conectividad**, en la subsección **Programación de conexiones**, puede especificar los intervalos de tiempo durante los cuales el Agente de red transmitirá datos al Servidor de administración.

Conectar cuando sea necesario. Si se selecciona esta opción, la conexión se establecerá cuando el Agente de red tenga que enviar datos al Servidor de administración.

Conectar en los periodos de tiempo especificados. Si se selecciona esta opción, el Agente de red se conectará al Servidor de administración a una hora concreta. Se pueden añadir varios períodos de tiempo de conexión.

Envío de mensajes a usuarios de dispositivos

Para enviar un mensaje a los usuarios de dispositivos:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. Cree una tarea de envío de mensaje a los usuarios de dispositivos de una de las siguientes formas:
   - Si desea enviar un mensaje a los usuarios de dispositivos que pertenecen al grupo de administración seleccionado, cree una tarea para el grupo seleccionado.
   - Si desea enviar un mensaje a los usuarios de dispositivos que pertenecen a diferentes grupos de administración o no pertenecen a ninguno, cree una tarea para dispositivos específicos.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.
3. En la ventana Tipo de tarea del Asistente para añadir tareas, seleccione el nodo **Servidor de administración de Kaspersky Security Center 14**, abra la carpeta **Avanzado** y seleccione la tarea **Enviar mensaje al usuario**. La tarea de enviar mensajes al usuario solo está disponible para dispositivos que ejecutan Windows. También puede enviar mensajes en el menú contextual del usuario en la carpeta **Cuentas de usuario**.
4. Ejecute la tarea creada.

   Una vez finalizada la tarea, el mensaje creado se enviará a los usuarios de los dispositivos seleccionados. La tarea de enviar mensajes al usuario solo está disponible para dispositivos que ejecutan Windows. También puede enviar mensajes en el menú contextual del usuario en la carpeta **Cuentas de usuario**.

Administración de la seguridad de Kaspersky Security for Virtualization

Kaspersky Security Center admite la opción de conexión de máquinas virtuales al Servidor de administración. Las máquinas virtuales se administran mediante Kaspersky Security for Virtualization. Para más información, consulte la documentación de esta aplicación.

Configuración del cambio de estado de los dispositivos

Puede cambiar las condiciones para asignar el estado *Crítico* o *Advertencia* a un dispositivo.

Para activar el cambio del estado del dispositivo a Crítico:

1. Abra la ventana de propiedades de alguno de los siguientes modos:
   - En la carpeta **Directivas** en el menú contextual de una directiva del Servidor de administración, seleccione **Propiedades**.
   - Seleccione **Propiedades** en el menú contextual de un grupo de administración.
2. En la ventana de propiedades que se abre, en el panel **Secciones**, seleccione **Estado del dispositivo**.
3. En el panel derecho, en la sección **Asignar Crítico si se especifican**, marque la casilla junto a una de las condiciones de la lista.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.
4. Configure el valor requerido para la condición seleccionada.

   Puede establecer valores para algunas condiciones pero no para todas.

5. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Crítico*.

Para activar el cambio del estado del dispositivo a Advertencia:

1. Abra la ventana de propiedades de alguno de los siguientes modos:

   - En la carpeta **Directivas** en el menú contextual de la directiva del Servidor de administración, seleccione **Propiedades**.
   - Seleccione **Propiedades** en el menú contextual del grupo de administración.

2. En la ventana de propiedades que se abre, en el panel **Secciones**, seleccione **Estado del dispositivo**.
3. En el panel derecho, en la sección **Asignar Advertencia si se especifican**, marque la casilla junto a una de las condiciones de la lista.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

4. Configure el valor requerido para la condición seleccionada.

   Puede establecer valores para algunas condiciones pero no para todas.

5. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Advertencia*.

Etiquetado de dispositivos y visualización de etiquetas asignadas

Kaspersky Security Center permite que usted etiquete dispositivos. Una *etiqueta* es el ID de un dispositivo que se puede utilizar para agrupar, describir o encontrar dispositivos. Las etiquetas asignadas a dispositivos se pueden utilizar para crear selecciones, para encontrar dispositivos y para distribuir dispositivos entre grupos de administración.

Puede etiquetar dispositivos manualmente o automáticamente. Etiquete un dispositivo manualmente en las propiedades del dispositivo; puede usar el etiquetado manual cuando tiene que etiquetar un dispositivo individual. El Servidor de administración realiza el etiquetado automático de acuerdo con las reglas de etiquetado especificadas.

En las propiedades de un Servidor de administración, puede configurar el etiquetado automático para dispositivos administrados por este Servidor de administración. Los dispositivos se etiquetan automáticamente cuando las reglas especificadas se cumplen. Una regla particular equivale a cada etiqueta. Las reglas se aplican a las propiedades de la red del dispositivo, sistema operativo, aplicaciones instaladas en el dispositivo y otras propiedades del dispositivo. Por ejemplo, puede configurar una regla que asignará la etiqueta *Win* a todos los dispositivos con Windows. A continuación, puede usar esta etiqueta al crear una selección de dispositivos; esto le ayudará a clasificar todos los dispositivos con Windows y a asignarles una tarea.

También puede usar etiquetas como condiciones de la activación del perfil de la directiva en un dispositivo administrado a fin de aplicar perfiles de la directiva específicos solo en dispositivos con etiquetas específicas. Por ejemplo, si un dispositivo etiquetado como *Mensajería* aparece en el grupo de administración *Usuarios* y si la activación del perfil de la directiva correspondiente por la etiqueta *Mensajería* se ha habilitado, entonces la directiva creada para el grupo *Usuarios* no se aplicará a este dispositivo — pero el perfil del perfil de la directiva se aplicará. El perfil de la directiva puede permitir que este dispositivo inicie algunas aplicaciones cuya ejecución ha sido bloqueada por la directiva.

Puede crear varias reglas de etiquetado. Pueden asignarse varias etiquetas a un solo dispositivo si ha creado varias reglas de etiquetado y si las condiciones respectivas de estas reglas se cumplen simultáneamente. Puede ver la lista de todas las etiquetas asignadas en las propiedades del dispositivo. Puede activar o desactivar cada una de las reglar de etiquetado. Si una regla se activa, se aplica a dispositivos administrados por el Servidor de administración. Si no usa una regla actualmente, pero la puede necesitar en el futuro, no la tiene que eliminar; simplemente puede desactivar la casilla **Activar regla**. En este caso, la regla se desactiva; no se ejecutará hasta que la casilla **Activar regla** se seleccione de nuevo. Es posible que tenga que desactivar una regla sin eliminarla si tiene que excluir la regla de la lista de reglas de etiquetado temporalmente y luego incluirla de nuevo.

Etiquetado automático de dispositivos

Puede crear y modificar reglas de etiquetado automáticas en la ventana de propiedades del Servidor de administración.

Para etiquetar dispositivos automáticamente:

1. En el árbol de la consola, seleccione el nodo con el nombre del Servidor de administración para el cual tiene que especificar reglas de etiquetado.

2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.

3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Reglas de etiquetado**.

4. En la sección **Reglas de etiquetado**, haga clic en el botón **Agregar**.

   Se abre la ventana **Nueva regla**.

5. En la ventana **Nueva regla**, configure las propiedades generales de la regla:

   - Especifique el nombre de la regla.

     El nombre de la regla no puede contener más de 255 caracteres de largo y no puede incluir ningún carácter especial (como `"*<>-_?:\"|`).

   - Habilite o deshabilite la regla mediante la casilla de verificación **Activar regla**.

     De forma predeterminada, la casilla de verificación **Activar regla** está seleccionada.

   - En el campo **Etiqueta**, escriba un nombre de etiqueta.

     El nombre de la etiqueta no puede contener más de 255 caracteres de largo y no puede incluir ningún carácter especial (como `"*<>-_?:\"|`).

6. En la sección **Condiciones** haga clic en el botón **Agregar** para agregar una nueva condición, o haga clic en el botón **Propiedades** para editar una condición existente.

   Se abre la ventana del Asistente de Nueva condición de regla de autoetiquetado.

7. En la ventana **Condición de asignación de etiquetas**, seleccione las casillas para las condiciones que deben afectar al etiquetado. Puede seleccionar varias condiciones.

8. Dependiendo de las condiciones de etiquetado que haya seleccionado, el Asistente muestra las ventanas para la instalación de las condiciones correspondientes. Configure la activación de la regla mediante las condiciones siguientes:

    - **Uso o asociación del dispositivo con una red específica**: las propiedades de la red del dispositivo, por ejemplo, nombre del dispositivo en la red Windows e inclusión del dispositivo en un dominio o una subred IP.
    - **Uso de Active Directory**: Presencia del dispositivo en la unidad organizativa de Active Directory e ingreso del dispositivo en un grupo de Active Directory.
    - **Aplicaciones específicas**: Presencia del Agente de red en el dispositivo, tipo del sistema operativo, versión y arquitectura.
    - **Máquinas virtuales**: inclusión del dispositivo en un tipo concreto de máquinas virtuales.
    - **Aplicación del registro de aplicaciones instalada**: Presencia de aplicaciones de proveedores diferentes en el dispositivo.

9. Una vez que la condición esté configurada, escriba un nombre para ella y luego cierre el Asistente.

    Si es necesario, puede establecer varias condiciones para una sola regla. En este caso, la etiqueta se asignará a un dispositivo si cumple al menos una condición. Las condiciones que ha añadido se mostrarán en la ventana de propiedades de la regla.

10. Haga clic **Aceptar** en la ventana **Nueva regla**; después, haga clic en **Aceptar** en la ventana de propiedades del Servidor de administración.

Las reglas recién creadas se hacen cumplir en dispositivos administrados por el Servidor de administración seleccionado. Si la configuración de un dispositivo cumple las condiciones de la regla, se asigna la etiqueta al dispositivo.

Visualización y configuración de etiquetas asignadas a un dispositivo

Puede ver la lista de todas las etiquetas que se han asignado a un dispositivo, así como proceder a la instalación de reglas de etiquetado automáticas en la ventana de propiedades del dispositivo.

Para ver y configurar las etiquetas que se han asignado a un dispositivo:

1. En el árbol de consola, abra la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo de la carpeta **Dispositivos administrados**, seleccione el dispositivo para el cual desea ver las etiquetas asignadas.
3. En el menú contextual del dispositivo móvil, seleccione **Propiedades**.
4. En la ventana de propiedades del dispositivo, seleccione la sección **Etiquetas**.

    Se muestra una lista de etiquetas asignadas al dispositivo seleccionado, así como la forma en la que cada una de las etiquetas se asignó: manualmente o según una regla.

5. Si es necesario, realice una de las acciones siguientes:

    - Para empezar con la instalación de reglas de etiquetado, haga clic en el vínculo **Configurar reglas de etiquetado automático** (solo para Windows).
    - Para renombrar una etiqueta, seleccione una y haga clic en el botón **Cambiar nombre**.

- Para eliminar una etiqueta, seleccione una y haga clic en el botón **Quitar**.
- Para agregar una etiqueta manualmente, introduzca una en el campo de la parte inferior de la sección **Etiquetas** y haga clic en el botón **Agregar**.

6. Haga clic en el botón **Aplicar**, si ha realizado cambios en la sección **Etiquetas** para que sus cambios sean efectivos.
7. Haga clic en **Aceptar**.

Si ha eliminado o renombrado una etiqueta en las propiedades del dispositivo, este cambio no afectará a las reglas de etiquetado que han estado configuradas en las propiedades del Servidor de administración. El cambio solo se aplicará al dispositivo de esas propiedades.

Diagnóstico remoto de los dispositivos cliente. Utilidad de diagnóstico remoto de Kaspersky Security Center

La utilidad para diagnóstico remoto de Kaspersky Security Center (de aquí en adelante, utilidad de diagnóstico remoto) está diseñada para la ejecución remota de las siguientes operaciones en dispositivos cliente:

- Activación y desactivación del seguimiento, modificación del nivel de seguimiento, descarga del archivo de seguimiento.
- Descargar información del sistema y configuración de la aplicación.
- Descarga de los registros de eventos.
- La generación de un archivo de volcado para una aplicación.
- Inicio del diagnóstico y descarga de los informes del diagnóstico.
- Inicio y detención de las aplicaciones.

Puede usar los registros de eventos e informes de diagnóstico descargados de un dispositivo cliente para solucionar problemas por su cuenta. Además, un especialista del Servicio de soporte técnico de Kaspersky puede pedirle que descargue archivos de seguimiento, archivos de volcado, registros de eventos e informes de diagnóstico desde un dispositivo cliente para un análisis más profundo en Kaspersky.

La utilidad de diagnóstico remoto se instala en el dispositivo automáticamente junto con la Consola de administración.

Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente

Para conectar la utilidad de diagnóstico remoto a un dispositivo cliente:

1. Seleccione cualquier grupo de administración en el árbol de consola.
2. En el espacio de trabajo, en la ficha **Dispositivos** y en el menú contextual de cualquier dispositivo cliente, seleccione **Herramientas personalizadas** → **Diagnósticos remotos**.

   Se abrirá la ventana principal de la utilidad de diagnóstico remoto.

3. Especifique las herramientas que quiere utilizar para conectarse al dispositivo cliente en el primer campo de la ventana principal de la utilidad de diagnóstico remoto:

   - **Acceso mediante la Red de Microsoft Windows**.
   - **Acceso mediante el Servidor de administración**.

4. Si en el primer campo de la ventana principal de la utilidad se ha seleccionado **Acceso mediante la Red de Microsoft Windows**, realice las siguientes acciones:

   - En el campo **Dispositivo**, especifique la dirección del dispositivo con el que necesita establecer conexión

     Se puede utilizar una dirección IP, nombre NetBIOS o nombre DNS como dirección del dispositivo.

     El valor predeterminado es la dirección del dispositivo que aparece en el menú contextual desde el que ha ejecutado la utilidad.

   - Especifique una cuenta para conectarse al dispositivo:

     - **Conectar como usuario actual** (seleccionado de forma predeterminada). Conéctese mediante la cuenta de usuario actual.
     - **Utilizar el nombre de usuario y la contraseña proporcionados para conectar**. Conéctese mediante una cuenta de usuario proporcionada. Especifique el **Nombre de usuario** y la **Contraseña** de la cuenta requerida.

     La conexión a un dispositivo solo es posible con la cuenta de un administrador local del dispositivo cliente.

5. Si en el primer campo de la ventana principal de la utilidad se ha seleccionado **Acceso mediante el Servidor de administración**, realice las siguientes acciones:

   - En el campo **Servidor de administración**, especifique la dirección del Servidor de administración desde el que se quiere conectar el dispositivo cliente.

     Se puede utilizar una dirección IP, un nombre NetBIOS o un nombre DNS como dirección del servidor.

     El valor predeterminado es la dirección del Servidor de administración desde el que se ejecuta la utilidad.

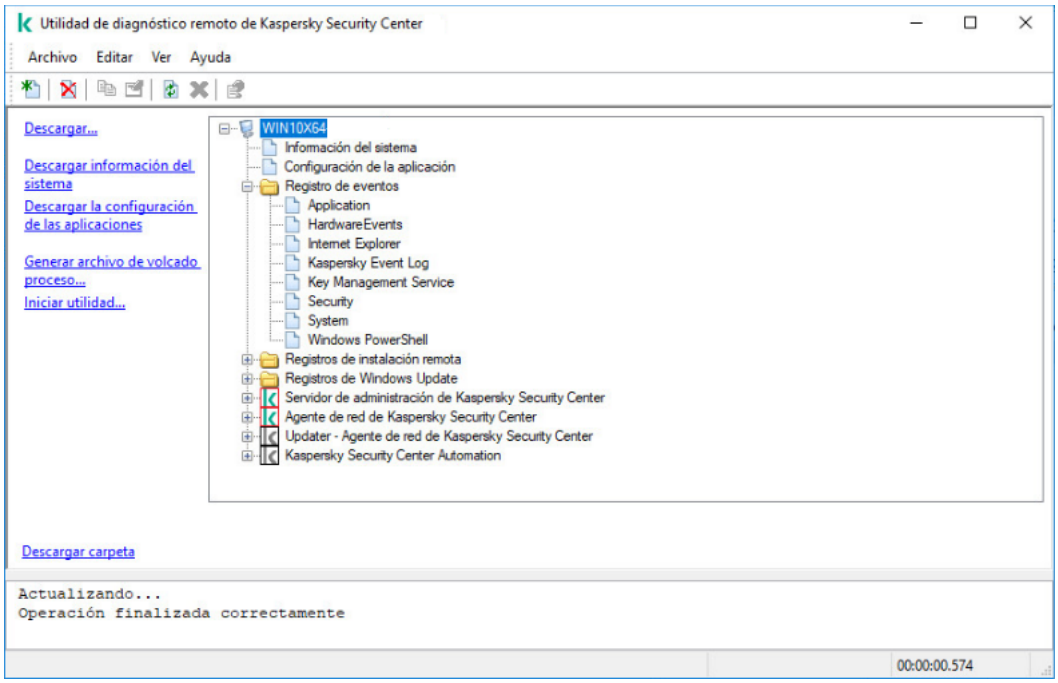
   - Si es necesario, seleccione las casillas de verificación **Utilizar SSL**, **Comprimir tráfico** y **El dispositivo pertenece al Servidor de administración secundario**.

     Si está marcada la casilla **El dispositivo pertenece al Servidor de administración secundario**, podrá rellenar el campo **El dispositivo pertenece al Servidor de administración secundario** con el nombre del Servidor de administración secundario que administra el dispositivo cliente al hacer clic en el botón **Examinar**.

6. Para conectarse al dispositivo, haga clic en el botón **Iniciar sesión**.

   Debe autorizar mediante la verificación en dos pasos si está activada para su cuenta.

De esta forma se abrirá la ventana del dispositivo cliente para realizar el diagnóstico remoto (consulte la figura siguiente). La parte izquierda de la ventana tiene unos enlaces a las operaciones de diagnóstico del dispositivo. La parte derecha de la ventana tiene el árbol de objetos del dispositivo cliente que la utilidad manejará. La parte inferior de la ventana muestra el progreso de las operaciones de la utilidad.



Utilidad de diagnóstico remoto. Ventana de diagnóstico remoto del dispositivo

La utilidad de diagnóstico remoto guarda los archivos descargados desde los dispositivos en el escritorio del dispositivo desde el que se lo ejecuta.

Activación y desactivación del seguimiento; descarga del archivo de seguimiento

Para habilitar el seguimiento en un dispositivo remoto:

1. Ejecute la utilidad de diagnóstico remoto y conecte el dispositivo requerido.
2. En el árbol de objetos del dispositivo, seleccione la aplicación para la que desee activar el seguimiento.

   El seguimiento solo se puede activar y desactivar en las aplicaciones con autodefensa si el dispositivo está conectado con las herramientas del Servidor de administración.

   Si desea habilitar el seguimiento para el Agente de red, también puede hacerlo mientras crea la tarea Instalar actualizaciones necesarias y corregir vulnerabilidades. En este caso, el Agente de red escribirá la información de seguimiento incluso si el seguimiento está desactivado para el Agente de red en la utilidad de diagnóstico remoto.
3. Activar trazado:
   a. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, haga clic en **Activar rastreo**.
   b. En la ventana **Seleccionar nivel de seguimiento** que se abre, le recomendamos que mantenga los valores predeterminados de la configuración. Cuando sea necesario, un especialista del Servicio de soporte técnico lo guiará a través del proceso de configuración. Están disponibles los siguientes ajustes:
      - Nivel de seguimiento

        El nivel de seguimiento define la cantidad de datos que contiene el archivo de seguimiento.

- **Seguimiento basado en rotación** (disponible solo para Kaspersky Endpoint Security)

  La aplicación sobrescribe la información de rastreo para evitar un aumento excesivo en el tamaño del archivo de seguimiento. Especifique la cantidad máximo de archivos que se utilizarán para almacenar la información de seguimiento y el tamaño máximo de cada archivo. Si se escribe el número máximo de archivos de seguimiento de tamaño máximo, el archivo de seguimiento más antiguo se eliminará para que se pueda escribir un nuevo archivo de seguimiento.

c. Haga clic en **Aceptar**.

4. Para Kaspersky Endpoint Security, un especialista del Servicio de soporte técnico puede solicitarle que habilite el seguimiento de Xperf para obtener información sobre el rendimiento del sistema.

   Para activar el seguimiento de Xperf:

   a. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, haga clic en **Activar seguimiento de Xperf**.

   b. En la ventana **Seleccionar nivel de seguimiento** que se abre, según la solicitud del especialista del Servicio de soporte técnico, seleccione uno de los siguientes niveles de seguimiento:

   - **Nivel ligero**

     Un archivo de seguimiento de este tipo contiene la cantidad mínima de información sobre el sistema.

     Esta opción está seleccionada de forma predeterminada.

   - **Nivel profundo**

     Un archivo de seguimiento de este tipo contiene información más detallada que los archivos de seguimiento del tipo *Ligero* y puede ser solicitado por especialistas del Servicio de soporte técnico cuando un archivo de seguimiento del tipo *Ligero* no es suficiente para la evaluación del rendimiento. Un archivo de seguimiento *Profundo* contiene información técnica sobre el sistema, incluida información sobre hardware, sistema operativo, lista de procesos y aplicaciones iniciadas y terminadas, eventos utilizados para la evaluación del rendimiento y eventos de la Herramienta de evaluación del sistema de Windows.

   c. Seleccione uno de los siguientes tipos de seguimientos:

   - **Tipo básico**

     La información de seguimiento se recibe durante el funcionamiento de la aplicación Kaspersky Endpoint Security.

     Esta opción está seleccionada de forma predeterminada.

   - **Tipo de reinicio**

     La información de seguimiento se recibe cuando el sistema operativo se inicia en el dispositivo administrado. Este tipo de seguimiento es efectivo cuando el problema que afecta al rendimiento del sistema ocurre después de que se encienda el dispositivo y antes de que se inicie Kaspersky Endpoint Security.

   d. También se le puede solicitar que habilite la opción de **Seguimiento basado en rotación** para evitar un aumento excesivo en el tamaño del archivo de seguimiento. Después, especifique el tamaño máximo del

archivo de seguimiento. Cuando el archivo alcanza el tamaño máximo, la información de seguimiento más antigua se sobrescribe con la información nueva.

e. Haga clic en **Aceptar**.

En algunos casos la aplicación de seguridad y su tarea se deberán reiniciar para activar el seguimiento.

La utilidad de diagnóstico remoto permite el seguimiento de la aplicación seleccionada.

Para descargar un archivo de seguimiento de una aplicación:

1. Ejecute la utilidad de diagnóstico remoto y conéctese al dispositivo necesario, como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En el nodo de la aplicación, en la carpeta **Archivos de seguimiento**, seleccione el archivo requerido.
3. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, haga clic en **Descargar archivo completo**.

   Para archivos de gran tamaño, se pueden descargar las partes en las que se ha realizado el seguimiento más recientemente.

   Se puede eliminar el archivo de seguimiento resaltado. El archivo se puede eliminar después de desactivar el seguimiento.

El archivo seleccionado se descarga en la ubicación especificada en la parte inferior de la ventana.

Para desactivar el seguimiento en un dispositivo remoto:

1. Ejecute la utilidad de diagnóstico remoto y conéctese al dispositivo necesario, como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En el árbol de objetos del dispositivo, seleccione la aplicación para la que desea desactivar el seguimiento.

   El seguimiento solo se puede activar y desactivar en las aplicaciones con autodefensa si el dispositivo está conectado con las herramientas del Servidor de administración.

3. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, haga clic en **Desactivar rastreo**.

La utilidad de diagnóstico remoto desactiva el seguimiento de la aplicación seleccionada.

Descarga de la configuración de las aplicaciones.

Para descargar la configuración de las aplicaciones desde un dispositivo remoto:

1. Ejecute la utilidad de diagnóstico remoto y conéctese al dispositivo necesario, como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En el árbol de objetos de la ventana de la utilidad de diagnóstico remoto, seleccione el nodo superior con el nombre del dispositivo.
3. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, seleccione la acción que necesita de entre las siguientes opciones:

- **Descargar información del sistema**
- **Descargar la configuración de las aplicaciones**
- **Generar archivo de volcado proceso**

  En la ventana que se abrirá después de hacer clic en este vínculo, especifique el archivo ejecutable de la aplicación para la que desee generar un archivo de volcado.

- **Iniciar utilidad**

  En la ventana que se abre después de hacer clic en este enlace, especifique el archivo ejecutable de la utilidad que desea iniciar y su configuración de ejecución.

La utilidad seleccionada se descargará y lanzará en el dispositivo.

Descarga de los registros de eventos

Para descargar un registro de eventos desde un dispositivo remoto:

1. Ejecute la utilidad de diagnóstico remoto y conéctese al dispositivo necesario, como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En la carpeta **Registro de eventos** del árbol de objetos del dispositivo, seleccione el registro relevante.
3. Descargue el registro seleccionado haciendo clic en el enlace **Descargar registro de eventos <Nombre del registro de eventos>** en la parte izquierda de la ventana de la utilidad de diagnóstico remoto.

El registro de eventos seleccionado se descarga en la ubicación especificada en el panel inferior.

Descargar elementos de información diagnósticos múltiples

La utilidad de diagnóstico remoto de Kaspersky Security Center le permite descargar múltiples elementos de información de diagnóstico, incluidos registros de eventos, información del sistema, archivos de seguimiento y archivos de volcado.

Para descargar información de diagnóstico desde un dispositivo remoto:

1. Ejecute la utilidad de diagnóstico remoto y conéctese al dispositivo necesario, como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".
2. En la parte izquierda de la ventana de la utilidad de diagnóstico remoto, haga clic en **Descargar**.
3. Seleccione las casillas al lado de los elementos que desea descargar.
4. Haga clic en **Iniciar**.

Cada elemento seleccionado se descarga en la ubicación especificada en el panel inferior.

Inicio del diagnóstico y descarga de los resultados

Para iniciar el diagnóstico de una aplicación en un dispositivo remoto y descargar sus resultados:

1. Ejecute la utilidad de diagnóstico remoto y conéctese al dispositivo necesario, como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".

2. En el árbol de objetos del dispositivo, seleccione la aplicación necesaria.

3. Inicie los diagnósticos haciendo clic en el enlace **Ejecutar diagnósticos** en la parte izquierda de la ventana de la utilidad de diagnóstico remoto.

   Aparecerá un informe de diagnósticos en el nodo del árbol de objeto de la aplicación seleccionada.

4. Seleccione el informe de diagnóstico que se acaba de generar en el árbol de objetos y haga clic en el enlace **Descargar carpeta** para descargarlo.

El informe seleccionado se descarga en la ubicación especificada en el panel inferior.

Inicio, detención y reinicio de aplicaciones

Solo se pueden iniciar, detener y reiniciar aplicaciones si se ha conectado el dispositivo cliente mediante las herramientas del Servidor de administración.

Para iniciar, detener o reiniciar una aplicación:

1. Ejecute la utilidad de diagnóstico remoto y conéctese al dispositivo necesario, como se describe en "Conexión de la utilidad de diagnóstico remoto a un dispositivo cliente".

2. En el árbol de objetos del dispositivo, seleccione la aplicación necesaria.

3. Seleccione una acción en la parte izquierda de la ventana de la utilidad de diagnóstico remoto:

   - **Detener aplicación**
   - **Reiniciar aplicación**
   - **Iniciar aplicación**

Dependiendo de la acción seleccionada, la aplicación se iniciará, detendrá o reiniciará.

Dispositivos con protección de UEFI

El *dispositivo con protección de UEFI* es un dispositivo con Kaspersky Anti-Virus for UEFI integrado al nivel de BIOS. La protección integrada garantiza la seguridad del dispositivo a partir del momento en que se inicia el sistema, mientras la protección en dispositivos sin el software integrado solo comienza a funcionar después de que se inicie la aplicación de seguridad. Kaspersky Security Center admite la administración de estos dispositivos.

Para modificar la configuración de conexión de dispositivos con protección de UEFI:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.

2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.

3. En la ventana de propiedades del Servidor de administración, seleccione **Configuración de la conexión del servidor** → **Puertos adicionales**.

4. En la sección **Puertos adicionales**, modifique la configuración relevante:

   - Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS

     Los dispositivos con protección de UEFI pueden conectarse al Servidor de administración.

   - Puerto para estos dispositivos

     Puede cambiar el número de puerto si la opción **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS** está activada. El número de puerto predeterminado es el 13294.

5. Haga clic en **Aceptar**.

Configuración de un dispositivo administrado

Para ver la configuración de un dispositivo administrado, siga estos pasos:

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.
2. En el espacio de trabajo de la carpeta, seleccione un dispositivo.
3. En el menú contextual del dispositivo, seleccione **Propiedades**.

Se abre la ventana de propiedades del dispositivo seleccionado, con la sección **General** seleccionada.

General

La sección **General** muestra información general sobre el dispositivo cliente. La información proporcionada se basa en los datos recibidos durante la última sincronización del dispositivo cliente con el Servidor de administración:

- Nombre

  En este campo se puede ver y modificar el nombre del dispositivo cliente en el grupo de administración.

- Descripción

  En este campo se puede introducir una descripción adicional para un dispositivo cliente.

- Dominio de Windows

  El dominio o grupo de trabajo de Windows que contiene el dispositivo.

- Nombre NetBIOS

  Nombre de red Windows del dispositivo cliente.

- **Nombre DNS**

  Nombre del dominio DNS del dispositivo cliente.

- **Dirección IP**

  Dirección IP del dispositivo.

- **Grupo**

  Grupo de administración que incluye el dispositivo cliente.

- **Última actualización**

  Fecha en que las bases de datos o las aplicaciones se actualizaron por última vez en el dispositivo.

- **Visible por última vez**

  Fecha y hora en que el dispositivo estuvo visible por última vez en la red.

- **Conectado al Servidor de administración**

  Fecha y hora en que el Agente de red instalado en el dispositivo cliente se conectó por última vez al Servidor de administración.

- **No desconectar del Servidor de administración**

  Si esta opción está activada, se mantiene la conectividad continua entre el dispositivo administrado y el Servidor de administración. Es posible que desee usar esta opción si no está utilizando servidores push, que proporcionan dicha conectividad.

  Si esta opción está desactivada y los servidores push no están en uso, el dispositivo administrado solo se conecta al Servidor de administración para sincronizar datos o transmitir información.

  El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

  Esta opción está desactivada de manera predeterminada en los dispositivos administrados. Esta opción está activada de manera predeterminada en el dispositivo donde está instalado el Servidor de administración y permanece así incluso si intenta desactivarla.

Protección

La sección **Protección** ofrece información sobre el estado actual de la protección antivirus en un dispositivo cliente:

- **Estado del dispositivo**

Estado del dispositivo cliente, asignado según los criterios definidos por el administrador para el estado de la protección antivirus en el dispositivo y la actividad del dispositivo en la red.

- **Todos los problemas**

  Esta tabla contiene una lista completa de problemas detectados por las aplicaciones administradas instaladas en el dispositivo cliente. Cada problema va acompañado de un estado, que la aplicación sugiere que asigne al dispositivo para este problema.

- **Protección en tiempo real**

  Este campo muestra el estado actual de la protección en tiempo real en el dispositivo cliente.

  Cuando el estado cambia en el dispositivo, el nuevo estado se muestra en la ventana de propiedades del dispositivo solo después de que el dispositivo cliente se sincronice con el Servidor de administración.

- **Último análisis a petición**

  Fecha y hora del último análisis antivirus realizado en el dispositivo cliente.

- **Número total de amenazas detectadas**

  Número total de amenazas detectadas en el dispositivo cliente desde la instalación de la aplicación antivirus (primer análisis del dispositivo) o desde la última fecha en que el contador de amenazas se puso a cero.

- **Amenazas activas**

  Número de archivos no procesados en el dispositivo cliente.

  Este campo omite el número de archivos no procesados en dispositivos móviles.

- **Estado del cifrado del disco**

  Estado actual del cifrado de archivo en las unidades locales del dispositivo.

Aplicaciones

La sección **Aplicaciones** enumera todas las aplicaciones Kaspersky instaladas en el dispositivo cliente:

- **Eventos**

  Haga clic en el botón para ver la lista de los eventos que se produjeron en el dispositivo cliente cuando se ejecutó la aplicación y para ver los resultados de la tarea para esa aplicación.

- **Estadísticas**

Haga clic en el botón para ver información estadística actual sobre la aplicación.

- Propiedades

  Haga clic en el botón para recibir información sobre la aplicación y para configurarla.

Tareas

En la sección **Tareas**, puede administrar tareas del dispositivo cliente: ver la lista de tareas existentes, crear nuevas, eliminar, iniciar y detener tareas, modificar su configuración y ver resultados de ejecución. La lista de tareas se proporciona a partir de los datos recibidos durante la última sesión de sincronización del cliente con el Servidor de administración. El Servidor de administración solicita los detalles de estado de la tarea desde el dispositivo cliente. No se mostrará el estado si no se ha establecido conexión.

Eventos

La sección **Eventos** muestra eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

Etiquetas

En la sección **Etiquetas** puede administrar la lista de palabras clave que se utilizan para buscar dispositivos cliente: ver la lista de etiquetas existentes, asignar etiquetas de la lista, configurar reglas de etiquetado automático, añadir etiquetas nuevas y cambiar el nombre de las antiguas y eliminar etiquetas.

Información del sistema

La sección **Información general del sistema** proporciona información sobre la aplicación instalada en el dispositivo cliente.

Registro de aplicaciones

En la sección **Registro de aplicaciones** se puede ver el registro de aplicaciones instaladas en el dispositivo cliente y sus actualizaciones, y se puede configurar la visualización del registro de aplicaciones.

La información acerca de las aplicaciones instaladas se proporciona si el Agente de red instalado en el dispositivo cliente envía la información requerida al Servidor de administración. Puede configurar el envío de información al Servidor de administración en la ventana de propiedades del Agente de red o de su directiva, en la sección **Repositorios**. La información sobre las aplicaciones instaladas se proporciona solo para dispositivos que ejecutan Windows.

El Agente de red proporciona información sobre las aplicaciones en función de los datos recibidos desde el registro del sistema.

- Mostrar únicamente las aplicaciones de seguridad incompatibles

Si se selecciona esta opción de verificación, la lista de aplicaciones tiene únicamente las aplicaciones de seguridad que son incompatibles con las aplicaciones Kaspersky.

Esta opción está desactivada de forma predeterminada.

- **Mostrar actualizaciones**

  Si esta opción está activada, la lista de aplicaciones no solo contiene las aplicaciones, sino también los paquetes de actualización instalados para las aplicaciones.

  Para mostrar la lista de actualizaciones, se necesitan 100 KB de tráfico. Si cierra la lista y la vuelve a abrir, tendrá que volver a gastar 100 KB de tráfico.

  Esta opción está desactivada de forma predeterminada.

- **Exportar a archivo**

  Haga clic en este botón para exportar la lista de aplicaciones instaladas en el dispositivo a un archivo CSV o TXT.

- **Historial**

  Haga clic en este botón para ver los eventos relacionados con la instalación de aplicaciones en el dispositivo. Se muestra la siguiente información:

  - Fecha y hora en que se instaló la aplicación en el dispositivo.
  - Nombre de la aplicación.
  - Versión de la aplicación.

- **Propiedades**

  Haga clic en este botón para ver las propiedades de la aplicación seleccionada en la lista de aplicaciones instaladas en el dispositivo. Se muestra la siguiente información:

  - Nombre de la aplicación.
  - Versión de la aplicación.
  - Proveedor de aplicaciones.

Archivos ejecutables

La sección **Archivos ejecutables** muestra los archivos ejecutables encontrados en el dispositivo cliente.

Registro de hardware

En la sección **Registro de hardware**, puede ver información sobre el hardware instalado en el dispositivo cliente. Puede ver esta información para dispositivos de Windows y dispositivos Linux.

Sesiones

La sección **Sesiones** muestra la información sobre el propietario del dispositivo cliente y las cuentas de usuarios que trabajan en el dispositivo cliente seleccionado.

La información sobre los usuarios del dominio se genera en función de los datos de Active Directory. Los detalles de los usuarios locales son proporcionados por el Windows Security Account Manager instalado en el dispositivo cliente.

- **Propietario del dispositivo**

  El campo **Propietario del dispositivo** muestra el nombre del usuario con el que puede contactar el administrador cuando es necesario efectuar determinadas operaciones con el dispositivo cliente.

  Utilice los botones **Asignar** y **Propiedades** para seleccionar el propietario del dispositivo y ver información sobre el usuario designado como tal.

  El botón con la cruz de color rojo se puede utilizar para eliminar el propietario actual del dispositivo.

La lista muestra las cuentas de usuarios que utilizan el dispositivo cliente.

- **Nombre**

  Nombre del dispositivo cliente en la red Windows.

- **Nombre del participante**

  Nombre (dominio o nombre local) del usuario que ha iniciado sesión en el dispositivo.

- **Cuenta**

  Cuenta del usuario que ha iniciado sesión en ese dispositivo.

- **Correo electrónico**

  Dirección de correo electrónico del usuario.

- **Teléfono**

  Número de teléfono del usuario.

Incidentes

En la sección **Incidentes**, puede ver, editar y crear incidentes para el dispositivo cliente. Los incidentes se pueden crear automáticamente, mediante las aplicaciones administradas por Kaspersky que están instaladas en el dispositivo cliente, o el administrador las puede crear de forma manual. Por ejemplo, si algunos usuarios mueven regularmente el malware de sus unidades extraíbles a los dispositivos, el administrador puede crear un incidente. El administrador puede proporcionar una breve descripción del caso y las acciones recomendadas (como las medidas disciplinarias que se deben tomar contra un usuario) en el texto del incidente y puede añadir un enlace al usuario o usuarios.

Un incidente para el cual se han tomado todas las acciones necesarias se llama *procesado*. La presencia de incidentes sin procesar se puede elegir como condición para cambiar el estado del dispositivo a *Crítico* o *Advertencia*.

Esta sección contiene una lista de incidentes que se han creado para el dispositivo. Los incidentes se clasifican por nivel de gravedad y tipo. El tipo de un incidente lo define la aplicación de Kaspersky que crea el incidente. Puede resaltar incidentes procesados en la lista seleccionando la casilla de verificación en la columna **Procesado**.

Vulnerabilidades de software

La sección **Vulnerabilidades de software** proporciona información sobre las vulnerabilidades de las aplicaciones de terceros instaladas en dispositivos cliente. Puede usar el campo de búsqueda encima de la lista para buscar vulnerabilidades por nombre.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar la lista de vulnerabilidades en un archivo. De forma predeterminada, la aplicación exporta la lista de vulnerabilidades a un archivo CSV.

- Mostrar solo las vulnerabilidades que se pueden reparar

  Si se selecciona esta opción, la sección muestra las vulnerabilidades que se pueden reparar mediante un parche.

  Si esta opción está desactivada, la sección muestra tanto las vulnerabilidades que se pueden reparar mediante un parche como aquellas para las que no existe ningún parche.

  Esta opción está activada de forma predeterminada.

- Propiedades

  Seleccione una vulnerabilidad de software en la lista y haga clic en el botón **Propiedades** para ver las propiedades de la vulnerabilidad de software seleccionado en una ventana separada. En la ventana, puede hacer lo siguiente:

  - Omita la vulnerabilidad de software en este dispositivo administrado (en la Consola de administración o en Kaspersky Security Center 14 Web Console).
  - Ver la lista de soluciones recomendadas para la vulnerabilidad.
  - Especifique manualmente las actualizaciones de software para corregir la vulnerabilidad (en la Consola de administración o en Kaspersky Security Center 14 Web Console).
  - Ver instancias de vulnerabilidad.
  - Ver la lista de tareas existentes para corregir la vulnerabilidad y crear nuevas tareas para corregir la vulnerabilidad.

Actualizaciones disponibles

Esta sección muestra una lista de actualizaciones de software encontradas en este dispositivo, pero no instaladas aún.

- Mostrar las actualizaciones instaladas

  Si se selecciona esta opción, la lista de actualizaciones muestra tanto las actualizaciones que no se han instalado, como las que ya se han instalado en el dispositivo cliente.

  Esta opción está desactivada de forma predeterminada.

Directivas activas

Esta sección muestra una lista de las directivas de aplicación de Kaspersky que actualmente están activas en este dispositivo.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar la lista de directivas activas a un archivo. De forma predeterminada, la aplicación exporta la lista de directivas a un archivo CSV.

Perfiles de directiva activos

- Perfiles de directiva activos

  La lista le permite consultar la información sobre los perfiles de directiva existentes, que están activos en dispositivos cliente. Utilice la barra de búsqueda que hay encima de la lista para encontrar perfiles de directiva activos en la lista introduciendo un nombre de directiva o bien un nombre de perfil de directiva.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar la lista de perfiles de directiva activos en un archivo. De forma predeterminada, la aplicación exporta una lista de perfiles de directiva a un archivo CSV.

Puntos de distribución

Esta sección proporciona una lista de puntos de distribución con los cuales interactúa el dispositivo.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar a un archivo una lista de puntos de distribución con los cuales interacciona el dispositivo. De forma predeterminada, la aplicación exporta la lista de dispositivos a un archivo CSV.

- Propiedades

Haga clic en el botón **Propiedades** para ver y configurar el punto de distribución con el cual interactúa el dispositivo.

Configuración general de las directivas

General

En la sección **General**, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- En el bloque **Estado de la directiva**, puede seleccionar uno de los modos de la directiva:
  - Directiva activa

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.
  - Directiva fuera de la oficina

    Si se selecciona esta opción, la directiva se activa cuando un dispositivo sale de la red corporativa.
  - Directiva inactiva

    Si se selecciona esta opción, se inactiva la directiva, pero sigue almacenada en la carpeta **Directivas**. Si fuera necesario, se puede activar la directiva.
- En la sección de grupo **Herencia de configuración**, se puede configurar la herencia de directivas:
  - Heredar configuración de la directiva primaria

    Si se activa esta opción, los valores de la configuración de la directiva se heredan de la directiva de grupos de nivel superior y, por lo tanto, quedan bloqueados.

    Esta opción está activada de forma predeterminada.
  - Forzar la herencia de la configuración en las directivas secundarias

Si se activa esta opción, después de aplicar modificaciones a las directivas, se realizarán las siguientes acciones:

- Los valores de los parámetros de las directivas se distribuirán a las directivas de los grupos de administración anidados, es decir, a las directivas secundarias.
- En el bloque **Herencia de configuración** de la sección **General** de la ventana de propiedades de cada directiva secundaria, se activará automáticamente la opción **Heredar configuración de la directiva primaria**.

Si se activa esta opción, la configuración de las directivas secundarias queda bloqueada.

Esta opción está desactivada de forma predeterminada.

Configuración de eventos

La sección **Configuración de eventos** le permite configurar el registro de eventos y la notificación de eventos. Los eventos se distribuyen en las fichas siguientes según el nivel de importancia:

- **Crítico**

  La ficha **Crítico** no se muestra en las propiedades de la directiva del Agente de red.
- **Fallo operativo**
- **Advertencia**
- **Información**

En cada ficha, la lista muestra los tipos de eventos y el plazo de almacenamiento de eventos predeterminado en el Servidor de administración (en días). Al hacer clic en el botón **Propiedades**, puede especificar el registro de eventos y las notificaciones relativas a los eventos seleccionados en la lista. De forma predeterminada, la configuración de la notificación común especificada para el Servidor de administración completo se utiliza para todos los tipos de evento. Sin embargo, puede cambiar la configuración específica para los tipos de evento requeridos.

Por ejemplo, en la pestaña **Advertencia**, puede configurar el tipo de evento **Se ha producido un incidente**. Este tipo de eventos pueden ocurrir, por ejemplo, cuando el espacio libre en disco de un punto de distribución es inferior a 2 GB (se requieren al menos 4 GB para instalar aplicaciones y descargar actualizaciones de forma remota). Para configurar el evento **Se ha producido un incidente**, selecciónelo y haga clic en el botón **Propiedades**. Después de eso, puede especificar dónde almacenar los eventos ocurridos y cómo notificarlos.

Si el Agente de red detectó un incidente, usted puede administrar este incidente utilizando la configuración de un dispositivo administrado.

Para seleccionar varios tipos de evento, use las teclas **Mayús** o **Ctrl**; para seleccionar todos los tipos, use el botón **Seleccionar todo**.

Configuración de la directiva del Agente de red

Para configurar la directiva del Agente de red:

1. En el árbol de consola, seleccione la carpeta **Directivas**.

2. En el espacio de trabajo de la carpeta, seleccione la directiva del Agente de red.

3. En el menú contextual de la directiva, seleccione **Propiedades**.

Se abre la ventana de propiedades de la directiva del Agente de red.

General

En la sección **General**, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- En el bloque **Estado de la directiva**, puede seleccionar uno de los modos de la directiva:
  - Directiva activa

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.

  - Directiva fuera de la oficina

    Si se selecciona esta opción, la directiva se activa cuando un dispositivo sale de la red corporativa.

  - Directiva inactiva

    Si se selecciona esta opción, se inactiva la directiva, pero sigue almacenada en la carpeta **Directivas**. Si fuera necesario, se puede activar la directiva.

- En la sección de grupo **Herencia de configuración**, se puede configurar la herencia de directivas:
  - Heredar configuración de la directiva primaria

    Si se activa esta opción, los valores de la configuración de la directiva se heredan de la directiva de grupos de nivel superior y, por lo tanto, quedan bloqueados.

    Esta opción está activada de forma predeterminada.

  - Forzar la herencia de la configuración en las directivas secundarias

    Si se activa esta opción, después de aplicar modificaciones a las directivas, se realizarán las siguientes acciones:
    - Los valores de los parámetros de las directivas se distribuirán a las directivas de los grupos de administración anidados, es decir, a las directivas secundarias.
    - En el bloque **Herencia de configuración** de la sección **General** de la ventana de propiedades de cada directiva secundaria, se activará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Si se activa esta opción, la configuración de las directivas secundarias queda bloqueada.

    Esta opción está desactivada de forma predeterminada.

Configuración de eventos

La sección **Configuración de eventos** le permite configurar el registro de eventos y la notificación de eventos. Los eventos se distribuyen en las fichas siguientes según el nivel de importancia:

- **Crítico**

  La ficha **Crítico** no se muestra en las propiedades de la directiva del Agente de red.

- **Fallo operativo**
- **Advertencia**
- **Información**

En cada ficha, la lista muestra los tipos de eventos y el plazo de almacenamiento de eventos predeterminado en el Servidor de administración (en días). Al hacer clic en el botón **Propiedades**, puede especificar el registro de eventos y las notificaciones relativas a los eventos seleccionados en la lista. De forma predeterminada, la configuración de la notificación común especificada para el Servidor de administración completo se utiliza para todos los tipos de evento. Sin embargo, puede cambiar la configuración específica para los tipos de evento requeridos.

Por ejemplo, en la pestaña **Advertencia**, puede configurar el tipo de evento **Se ha producido un incidente**. Este tipo de eventos pueden ocurrir, por ejemplo, cuando el espacio libre en disco de un punto de distribución es inferior a 2 GB (se requieren al menos 4 GB para instalar aplicaciones y descargar actualizaciones de forma remota). Para configurar el evento **Se ha producido un incidente**, selecciónelo y haga clic en el botón **Propiedades**. Después de eso, puede especificar dónde almacenar los eventos ocurridos y cómo notificarlos.

Si el Agente de red detectó un incidente, usted puede administrar este incidente utilizando la configuración de un dispositivo administrado.

Para seleccionar varios tipos de evento, use las teclas **Mayús** o **Ctrl**; para seleccionar todos los tipos, use el botón **Seleccionar todo**.

Configuración

En la sección **Configuración**, se puede configurar la directiva del Agente de red:

- **Distribuir archivos solo mediante puntos de distribución**

  Si esta opción está activada, los Agentes de red en los dispositivos administrados recuperan las actualizaciones solo de los puntos de distribución.

  Si esta opción está desactivada, los Agentes de red en los dispositivos administrados recuperan las actualizaciones de los puntos de distribución o del Servidor de administración.

  > Tenga en cuenta que las aplicaciones de seguridad en los dispositivos administrados recuperan actualizaciones del origen establecido en la tarea de actualización para cada aplicación de seguridad. Si activa la opción **Distribuir archivos solo mediante puntos de distribución**, asegúrese de que Kaspersky Security Center esté configurado como origen de actualización en las tareas de actualización.

  Esta opción está desactivada de forma predeterminada.

- Tamaño máximo de la cola del evento, en MB

  En este campo se puede especificar el espacio máximo en disco que puede ocupar una cola de eventos.

  El valor predeterminado es de 2 Megabytes (MB).

- La aplicación podrá obtener información adicional sobre la directiva en el dispositivo

  El Agente de red instalado en un dispositivo administrado transfiere información sobre la directiva de aplicación de seguridad aplicada a la aplicación de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows). Puede ver la información transferida en la interfaz de la aplicación de seguridad.

  El Agente de red transfiere la siguiente información:

  - Hora de entrega de la directiva al dispositivo administrado
  - Nombre de la directiva activa o fuera de la oficina en el momento de la entrega de la directiva al dispositivo administrado
  - Nombre y ruta completa al grupo de administración que contenía el dispositivo administrado en el momento de la entrega de la directiva al dispositivo administrado
  - Lista de perfiles de directivas activas

    Puede utilizar la información para asegurarse de que se aplique la directiva correcta al dispositivo y para solucionar problemas. Esta opción está desactivada de forma predeterminada.

- Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración

  Una vez que el Agente de red se instala en un dispositivo administrado, el componente no se puede eliminar ni reconfigurar sin los privilegios necesarios. El servicio del Agente de red no se puede detener.

  Esta opción está desactivada de forma predeterminada.

- Utilizar contraseña de desinstalación

  Si se selecciona esta opción, al hacer clic en el botón **Modificar** se puede especificar la contraseña para la desinstalación remota del Agente de red.

  Esta opción está desactivada de forma predeterminada.

Repositorios

En la sección **Repositorios**, puede seleccionar los tipos de objetos cuya información se enviará desde el Agente de red hasta el Servidor de administración. Si la modificación de algunos parámetros de esta sección está prohibida por la directiva del Agente de red, no se los podrá modificar. La configuración en la sección **Repositorios** está disponible solo en dispositivos que ejecutan Windows:

- Detalles de las actualizaciones de Windows Update

Si se selecciona esta opción, la información sobre las actualizaciones de Microsoft Windows Update que se deben instalar en los dispositivos cliente se envía al Servidor de administración.

A veces, incluso si la opción está desactivada, las actualizaciones se muestran en las propiedades del dispositivo en la sección **Actualizaciones disponibles**. Esto podría suceder en el caso de que, por ejemplo, los dispositivos de la organización tengan vulnerabilidades que estas actualizaciones puedan solucionar.

Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

- Detalles de vulnerabilidades de software y actualizaciones correspondientes

  Si esta opción está activada, la información sobre vulnerabilidades en el software de terceros (incluido el software de Microsoft), detectada en dispositivos administrados, y sobre actualizaciones de software para corregir vulnerabilidades de terceros (sin incluir el software de Microsoft) se envía al Servidor de administración.

  Al seleccionar esta opción (**Detalles de vulnerabilidades de software y actualizaciones correspondientes**) aumenta la carga de red, la carga de disco del Servidor de administración y el consumo de recursos del Agente de red.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

  Para administrar las actualizaciones de software de Microsoft, use la opción **Detalles de las actualizaciones de Windows Update**.

- Detalles de registro de hardware

  El Agente de red instalado en un dispositivo envía información sobre el hardware del dispositivo al Servidor de administración. Puede ver los detalles del hardware en las propiedades del dispositivo.

- Detalles de las aplicaciones instaladas

  Si esta opción está activada, la información sobre las aplicaciones instaladas en los dispositivos cliente se envía al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- Incluir información sobre parches

  La información sobre parches de aplicaciones instaladas en dispositivos cliente se envía al Servidor de administración. Si se activa esta opción, se puede incrementar la carga del Servidor de administración y el DBMS, así como el volumen de la base de datos.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

Vulnerabilidades y actualizaciones de software

En la sección **Vulnerabilidades y actualizaciones de software**, puede configurar la búsqueda y distribución de actualizaciones de Windows, así como activar el análisis de archivos ejecutables en busca de vulnerabilidades. La configuración en la sección **Vulnerabilidades y actualizaciones de software** está disponible solo en dispositivos que ejecutan Windows:

- Utilizar el Servidor de administración como servidor WSUS

Si esta opción está activada, las actualizaciones de Windows se descargan al Servidor de administración. El Servidor de administración proporciona actualizaciones descargadas a servicios de Windows Update en dispositivos cliente en el modo centralizado por medio de Agentes de red.

Si esta opción está desactivada, el Servidor de administración no se utiliza para descargar actualizaciones de Windows. En este caso, los dispositivos cliente reciben las actualizaciones de Windows por su propia cuenta.

Esta opción está desactivada de forma predeterminada.

- En **Permitir que los usuarios administren la instalación de actualizaciones de Windows Update**, puede limitar las actualizaciones de Windows que los usuarios pueden instalar en sus dispositivos de forma manual mediante el uso de Windows Update.

  En los dispositivos que ejecutan Windows 10, si Windows Update ya encontró actualizaciones para el dispositivo, la nueva opción que seleccione en **Permitir a los usuarios administrar la instalación de las actualizaciones de Windows Update** se aplicará solo después de que se hayan instalado las actualizaciones encontradas.

  Seleccione un elemento en la lista desplegable:

  - Permitir que los usuarios instalen todas las actualizaciones de Windows Update aplicables

    Los usuarios pueden instalar todas las actualizaciones de Microsoft Windows Update que sean aplicables a sus dispositivos.

    Seleccione esta opción si no desea interferir en la instalación de actualizaciones.

    Cuando el usuario instala actualizaciones de Microsoft Windows Update manualmente, las actualizaciones pueden descargarse de los servidores de Microsoft en lugar de hacerlo desde el Servidor de administración. Esto es posible si el Servidor de administración aún no ha descargado estas actualizaciones. La descarga de actualizaciones de los servidores de Microsoft genera un tráfico adicional.

  - Permitir que los usuarios instalen solo actualizaciones aprobadas de Windows Update

    Los usuarios pueden instalar todas las actualizaciones de Microsoft Windows Update que sean aplicables a sus dispositivos y que sean aprobadas por usted.

    Por ejemplo, es posible que desee verificar primero la instalación de actualizaciones en un entorno de prueba y asegurarse de que no interfieran con el funcionamiento de los dispositivos y solo entonces permitir la instalación de estas actualizaciones aprobadas en los dispositivos cliente.

    Cuando el usuario instala actualizaciones de Microsoft Windows Update manualmente, las actualizaciones pueden descargarse de los servidores de Microsoft en lugar de hacerlo desde el Servidor de administración. Esto es posible si el Servidor de administración aún no ha descargado estas actualizaciones. La descarga de actualizaciones de los servidores de Microsoft genera un tráfico adicional.

  - No permitir que los usuarios instalen actualizaciones de Windows Update

Los usuarios no pueden instalar actualizaciones de Microsoft Windows Update en sus dispositivos de manera manual. Todas las actualizaciones aplicables se instalan según lo configurado por usted.

Seleccione esta opción si desea administrar la instalación de actualizaciones de forma centralizada.

Por ejemplo, es posible que desee optimizar el programa de actualización para que la red no se sobrecargue. Puede programar actualizaciones fuera de horario, para que no interfieran con la productividad del usuario.

- En el grupo de configuración del **Modo de búsqueda de Windows Update**, puede seleccionar el modo de búsqueda de actualización:

  - **Activo**

    Si se selecciona esta opción, el Servidor de administración, secundado por el Agente de red, iniciará una solicitud de un agente de Windows Update en el dispositivo cliente al origen de actualizaciones: Servidores de Windows Update o WSUS. A continuación, el Agente de red transmite la información que recibe del Agente de Windows Update al Servidor de administración.

    La opción solo se activa si se selecciona la opción **Conectar al servidor de actualizaciones para actualizar los datos** de la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

    Esta opción está seleccionada de forma predeterminada.

  - **Pasivo**

    Si se selecciona esta opción, el Agente de red transmite periódicamente al Servidor de administración información sobre las actualizaciones recuperadas en la última sincronización del Agente de Windows Update con el origen de actualizaciones. Si no se realiza ninguna sincronización del Agente de Windows Update con un origen de actualizaciones, la información sobre actualizaciones del Servidor de administración se volverá anticuada.

    Seleccione esta opción si desea obtener actualizaciones de la memoria caché del origen de actualizaciones.

  - **Desactivado**

    Si selecciona esta opción, el Servidor de administración no solicita información alguna acerca de las actualizaciones.

    Seleccione esta opción si, por ejemplo, desea probar primero las actualizaciones en su dispositivo local.

- **Analizar los archivos ejecutables para buscar vulnerabilidades al iniciarlos**

  Si esta opción está seleccionada, los archivos ejecutables se analizan en busca de vulnerabilidades cuando se ejecutan.

  Esta opción está activada de forma predeterminada.

Reiniciar administración

En la sección **Administración de reinicios**, puede especificar la acción que debe realizarse si el sistema operativo de un dispositivo administrado se tiene que reiniciar para garantizar el uso correcto de una aplicación, su instalación o desinstalación. La configuración en la sección **Administración de reinicios** está disponible solo en dispositivos que ejecutan Windows:

- **No reiniciar el sistema operativo**

  No se reiniciará el sistema operativo.

- **Reiniciar el sistema operativo automáticamente de ser necesario**

  Si fuera necesario, el sistema operativo se reiniciaría automáticamente.

- **Solicitar al usuario una acción**

  La aplicación solicita al usuario autorización para reiniciar el sistema operativo.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir la solicitud cada (min)**

    Si esta opción está activada, la aplicación solicita al usuario autorización para reiniciar el sistema operativo con la frecuencia que se especifique en el campo que se encuentra junto a la casilla de verificación. De forma predeterminada, el período de solicitud es de 5 minutos.

    Si esta opción está desactivada, la aplicación no solicita al usuario que permita reiniciar repetidamente.

    Esta opción está activada de forma predeterminada.

  - **Forzar reinicio después de (min)**

    Si esta opción está activada y tras la solicitud al usuario, la aplicación fuerza el reinicio del sistema operativo cuando transcurre el intervalo de tiempo especificado en el campo que se encuentra junto a la casilla de verificación.

    Si esta opción está desactivada, la aplicación no fuerza el reinicio.

    Esta opción está activada de forma predeterminada.

  - **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

    Las aplicaciones se cierran a la fuerza cuando el dispositivo del usuario se bloquea (bien manualmente o bien automáticamente cuando transcurre el intervalo de inactividad especificado).

    Si se selecciona esta opción, las aplicaciones del dispositivo bloqueado se cierran a la fuerza cuando transcurre el intervalo de tiempo especificado en el campo de entrada.

    Si esta opción está desactivada, las aplicaciones del dispositivo bloqueado no se cerrarán.

    Esta opción está desactivada de forma predeterminada.

Uso compartido del escritorio de Windows

En la sección **Uso compartido del escritorio de Windows**, puede activar y configurar la auditoría de las acciones del administrador realizadas en un dispositivo remoto cuando se utiliza el acceso a escritorio compartido. La configuración en la sección **Uso compartido del escritorio de Windows** está disponible solo en dispositivos que ejecutan Windows:

- **Activar auditorías**

Si esta opción está activada, en el dispositivo remoto se habilita la auditoría de las acciones del administrador. Las acciones del administrador en el dispositivo remoto se registran:

- En el registro de eventos del dispositivo remoto
- En un archivo con extensión syslog ubicado en la carpeta de instalación del Agente de red en el dispositivo remoto
- En la base de datos de eventos de Kaspersky Security Center

La auditoría de las acciones del administrador puede realizarse cuando se cumplen estas condiciones:

- La licencia de Administración de vulnerabilidades y parches está en uso
- El administrador dispone del derecho para iniciar el acceso compartido al escritorio del dispositivo remoto

Si esta casilla está desactivada, se deshabilita la auditoría de las acciones del administrador en el dispositivo remoto.

Esta opción está desactivada de forma predeterminada.

- Máscaras de los archivos que se deben supervisar cuando se leen

  La lista muestra máscaras de archivos. Cuando se habilita la auditoría, la aplicación supervisa los archivos de lectura del administrador que coinciden con las máscaras y guarda información sobre la lectura de los archivos. Esta lista está disponible si se selecciona la casilla **Habilitar auditorías**. Puede modificar las máscaras de archivos y añadir otras nuevas a la lista. Cada máscara de archivos nueva se debe especificar en líneas distintas de la lista.

  De forma predeterminada, se especifican las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- Máscaras de archivos que supervisar cuando se modifiquen

  La lista contiene máscaras de archivos en el dispositivo remoto. Cuando se habilita la auditoría, la aplicación supervisa los cambios realizados por el administrador en los archivos que coinciden con máscaras y guarda información sobre esas modificaciones. Esta lista está disponible si se selecciona la casilla **Habilitar auditorías**. Puede modificar las máscaras de archivos y añadir otras nuevas a la lista. Cada máscara de archivos nueva se debe especificar en líneas distintas de la lista.

  De forma predeterminada, se especifican las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Administrar parches y actualizaciones

En la sección **Administrar parches y actualizaciones**, puede configurar la descarga y distribución de actualizaciones, como también la instalación de parches en los dispositivos administrados:

- Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir

Si esta opción está activada, los parches de Kaspersky que tienen la *Sin definir* se instalarán automáticamente en los dispositivos administrados tras descargarse desde los servidores de actualización. La instalación automática de parches con el estado *indeterminado* está disponible para Kaspersky Security Center Service Pack 2 y posteriores.

Si esta opción está desactivada, los parches de Kaspersky que se hayan descargado y etiquetado con el estado *Indeterminado* solo se instalarán después de que el administrador cambie su estado a *Aprobados*.

Esta opción está activada de forma predeterminada.

- **Descargar actualizaciones y bases de datos antivirus del Servidor de administración (recomendado)**

  Si esta opción está activada, se utiliza el modelo de descarga de actualizaciones sin conexión. Cuando el Servidor de administración recibe actualizaciones, notifica al Agente de red (en los dispositivos donde está instalado) las actualizaciones que serán necesarias para las aplicaciones administradas. Cuando el Agente de red recibe la información sobre las actualizaciones, descarga por anticipado los archivos relevantes desde el Servidor de administración. En la primera conexión con el Agente de red, el Servidor de administración inicia una descarga de actualización. Una vez que el Agente de red descarga todas las actualizaciones a un dispositivo cliente, las actualizaciones estarán disponibles para las aplicaciones en ese dispositivo.

  Cuando una aplicación administrada de un dispositivo cliente intenta acceder al Agente de red para descargar actualizaciones, el Agente de red comprueba si tiene todas las actualizaciones necesarias. Si las actualizaciones se reciben desde el Servidor de administración no más de 25 horas antes de que la aplicación administrada las solicite, el Agente de red no se conecta al Servidor de administración, sino que proporciona actualizaciones desde el caché local a la aplicación administrada. Es posible que la conexión con el Servidor de administración no se establezca cuando el Agente de red proporciona actualizaciones para las aplicaciones en los dispositivos cliente, pero no se requiere conexión para la actualización.

  Si esta opción está desactivada, el modelo de descarga de actualizaciones sin conexión no se utiliza. Las actualizaciones se distribuyen de acuerdo con el calendario de la tarea de descarga de actualizaciones.

  Esta opción está activada de forma predeterminada.

Conectividad

La sección **Conectividad** incluye tres subsecciones anidadas:

- **Red**
- **Perfiles de conexión** (solo para Windows y macOS)
- **Programación de conexiones**

En la subsección **Red**, puede configurar la conexión con el Servidor de administración, activar el uso de un puerto UDP y especificar su número. Están disponibles las siguientes opciones:

- El grupo de configuración **Conexión al Servidor de administración** le permite configurar la conexión al Servidor de administración y especificar el período para la sincronización de los dispositivos cliente y el Servidor de administración:
  - **Comprimir tráfico de red**

Si se selecciona esta opción, aumentará la velocidad de transferencia de datos del Agente de red, disminuirá la cantidad de información que se transfiere y disminuirá la carga en el Servidor de administración.

Puede incrementarse la carga de trabajo de la CPU del dispositivo cliente.

De forma predeterminada, esta opción está activada.

- **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**

  Si se selecciona esta opción, se añadirá un puerto UDP (necesario para el funcionamiento del Agente de red) a la lista de exclusiones del firewall de Microsoft Windows.

  Esta opción está activada de forma predeterminada.

- **Utilizar SSL**

  Si esta opción está activada, la conexión al Servidor de administración se establece a través de un puerto seguro a través de SSL.

  Esta opción está activada de forma predeterminada.

- **Utilizar la puerta de enlace de conexión del punto de distribución (si está disponible) en la configuración de la conexión predeterminada**

  Si se selecciona esta opción, la puerta de enlace de conexión en el punto de distribución se utilizará con la configuración especificada en las propiedades del grupo de administración.

  Esta opción está activada de forma predeterminada.

- **Usar puerto UDP**

  Si necesita que los dispositivos administrados se conecten al Servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado de conexión al Servidor proxy de KSN es 15111.

- **Número de puerto UDP**

  En este campo se introduce el nombre del puerto UDP. El número de puerto predeterminado es el 15000.

  Se usa el sistema decimal para los registros.

  Si un dispositivo cliente ejecuta Windows XP Service Pack 2, el firewall integrado bloqueará el puerto UDP 15000. Este puerto debe abrirse manualmente.

- **Utilice el punto de distribución para forzar la conexión con el Servidor de administración.**

  Seleccione esta opción si selecciona la opción **Utilice este punto de distribución como servidor push** en la ventana de configuración del punto de distribución. De lo contrario, el punto de distribución no funcionará como servidor push.

En la subsección **Perfiles de conexión**, puede especificar la configuración de la ubicación de red, configurar perfiles de conexión para el Servidor de administración y activar el modo fuera de la oficina cuando el Servidor de administración no esté disponible. Los ajustes de la sección **Perfiles de conexión** están disponibles solo en dispositivos que ejecutan Windows:

- **Configuración de la ubicación de red**

  La configuración de la ubicación de red define las características de la red a la que está conectado el dispositivo cliente y especifica las reglas para el cambio del Agente de red de un perfil de conexión Servidor de administración a otro cuando se alteran esas características de red.

- **Perfiles de conexión al Servidor de administración**

  En esta sección se pueden ver y añadir perfiles para la conexión del Agente de red al Servidor de administración. En esta sección, también puede crear reglas para cambiar el Agente de red a Servidores de administración diferentes cuando ocurren los siguientes eventos:

  - Cuando un dispositivo cliente se conecta a otra red local
  - Cuando un dispositivo pierde conexión con la red local de la organización
  - Cuando se cambia la dirección de la puerta de enlace de conexión o se modifica la dirección del servidor DNS

  Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

- **Activar modo Fuera de la oficina cuando el Servidor de administración no está disponible**

  Si se selecciona esta opción y en el caso de que la conexión se realice con este perfil, las aplicaciones instaladas en el dispositivo cliente utilizan los perfiles de directivas para dispositivos en modo fuera de la oficina, además de directivas fuera de la oficina. Si no se ha definido una directiva fuera de la oficina en la aplicación, se utilizará la directiva activa.

  Si esta opción está desactivada, las aplicaciones utilizarán las directivas activas.

  Esta opción está desactivada de forma predeterminada.

En la subsección **Programación de conexiones**, se pueden especificar los intervalos de tiempo en los que el Agente de red envía los datos al Servidor de administración:

- **Conectar cuando sea necesario**

  Si se selecciona esta opción, la conexión se establecerá cuando el Agente de red tenga que enviar datos al Servidor de administración.

  Esta opción está seleccionada de forma predeterminada.

- **Conectar en los periodos de tiempo especificados**

  Si se selecciona esta opción, el Agente de red se conectará al Servidor de administración a una hora concreta. Se pueden añadir varios períodos de tiempo de conexión.

Puntos de distribución

La sección **Puntos de distribución** incluye cuatro subsecciones anidadas:

- **Sondeo de la red**
- **Configuración de la conexión a Internet**
- **Proxy de KSN**
- **Actualizaciones**

En la subsección **Sondeo de la red**, puede configurar el sondeo automático de la red. Puede activar tres tipos de sondeo, es decir, sondeo de red, sondeo de rangos de IP y sondeo de Active Directory:

- **Permitir análisis de red**

  Si esta opción está activada, el Servidor de administración sondea automáticamente la red según la planificación que ha configurado al hacer clic en los enlaces **Programar un sondeo rápido** y **Programar un sondeo completo**.

  Si esta opción está desactivada, el Servidor de administración no sondea la red.

  El intervalo de detección de dispositivos para las versiones del Agente de red anteriores a 10.2 se pueden configurar en los campos **Frecuencia de los sondeos desde los dominios de Windows (min)** y **Frecuencia de los sondeos de la red (min)**. Los campos están disponibles si la opción está activada.

  Esta opción está desactivada de forma predeterminada.

- **Activar sondeos de rangos IP**

  Si esta opción está activada, el Servidor de administración sondea automáticamente los rangos de IP de acuerdo con la programación que ha configurado al hacer clic en el enlace **Programar sondeo**.

  Si esta opción está desactivada, el Servidor de administración no sondea los rangos de IP.

  La frecuencia de sondeos de rangos IP en las versiones del Agente de red anteriores a 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo está disponible si la opción está activada.

  Esta opción está desactivada de forma predeterminada.

- **Utilice el sondeo Zeroconf (solo en plataformas Linux; los rangos de IP especificados manualmente serán ignorados)**

  Si esta opción está activada, el punto de distribución automáticamente sondea la red con dispositivos IPv6 mediante el uso de las redes de configuración cero (también denominadas *Zeroconf*). En este caso, el sondeo de rangos de IP activados se ignora, porque el punto de distribución sondea toda la red.

  Para empezar a usar Zeroconf, se deben cumplir las siguientes condiciones:

  - El punto de distribución debe ejecutar Linux.
  - Debe instalar la utilidad avahi-browse en el punto de distribución.

  Si esta opción está desactivada, el punto de distribución no sondea las redes con dispositivos IPv6.

  Esta opción está desactivada de forma predeterminada.

- **Permitir sondeo de Active Directory**

Si esta opción está activada, el Servidor de administración sondea automáticamente Active Directory según la planificación que ha configurado al hacer clic en el enlace **Programar sondeo**.

Si esta opción está desactivada, el Servidor de administración no sondea Active Directory.

La frecuencia de sondeo de Active Directory en las versiones de Agente de red anteriores a la 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo está disponible si esta opción está activada.

Esta opción está desactivada de forma predeterminada.

En la subsección **Configuración de la conexión a Internet**, puede especificar la configuración del acceso a Internet:

- Usar servidor proxy

  Si se selecciona esta casilla, en los campos de entrada se podrá configurar la conexión al servidor proxy.

  De forma predeterminada, esta casilla está en blanco.

- Dirección del servidor proxy

  Dirección del servidor proxy.

- Número de puerto

  Número de puerto que se utiliza en la conexión.

- No utilizar el servidor proxy para direcciones locales

  Si se selecciona esta opción, no se utilizará el servidor proxy para conectarse a los dispositivos de la red local.

  Esta opción está desactivada de forma predeterminada.

- Autenticación del servidor proxy

  Si se activa esta casilla, podrá especificar las credenciales para la autenticación del servidor proxy en los campos de entrada.

  De forma predeterminada, esta opción está desactivada.

- Nombre de usuario

  La cuenta de usuario bajo la cual se establece la conexión al servidor proxy.

- Contraseña

  La contraseña de la cuenta bajo la cual la tarea se ejecutará.

En la subsección **Proxy de KSN**, puede configurar la aplicación para utilizar el punto de distribución para reenviar solicitudes de KSN desde los dispositivos administrados:

- **Activar el proxy de KSN en el punto de distribución**

  El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico en la red.

  El punto de distribución envía a Kaspersky las estadísticas de KSN, que se incluyen en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se guarda en %Archivos de programa%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Esta opción está desactivada de forma predeterminada. Esta opción solo se activa si las opciones **Utilizar el Servidor de administración como servidor proxy** y **Acepto usar Kaspersky Security Network** están activadas en la ventana de propiedades del Servidor de administración.

  Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y activar el proxy de KSN en ese nodo.

- **Reenviar solicitudes de KSN al Servidor de administración**

  El punto de distribución reenvía las solicitudes KSN de los dispositivos administrados al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- **Acceder a la nube de KSN / KSN privada directamente a través de Internet**

  El punto de distribución reenvía las solicitudes de KSN de los dispositivos administrados a KSN Cloud o KSN privada. Las solicitudes de KSN generadas en el punto de distribución también se envían directamente a KSN Cloud o KSN privada.

  Los puntos de distribución que tienen instalado el Agente de red versión 11 (o versiones anteriores) no pueden acceder a KSN Privada directamente. Si desea reconfigurar los puntos de distribución para enviar solicitudes KSN a KSN Privada, active la opción **Reenviar solicitudes de KSN al Servidor de administración** para cada punto de distribución.

  Los puntos de distribución que tienen instalado el Agente de red versión 12 (o versiones posteriores) pueden acceder a KSN privada directamente.

- **Puerto TCP**

  El número del puerto de TCP que los dispositivos administrados utilizarán para conectar al Servidor proxy de KSN. El número de puerto predeterminado es el 13111.

- **Usar puerto UDP**

  Si necesita que los dispositivos administrados se conecten al Servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado de conexión al Servidor proxy de KSN es 15111.

En la subsección **Actualizaciones**, puede especificar si el Agente de red debe descargar archivos diff activando o desactivando la opción **Descargar archivos diff**. (Esta opción está activada de forma predeterminada).

Historial de revisión

En la ficha **Historial de revisiones**, puede ver el historial de las revisiones de directivas del Agente de red. Puede comparar revisiones, ver revisiones y realizar operaciones avanzadas, como guardar revisiones en un archivo, revertir a una revisión y añadir y editar descripciones de revisiones.

Comparación de funciones de los sistemas operativos del Agente de red

La siguiente tabla muestra qué configuración de directiva del Agente de red puede usar para configurar el Agente de red con un sistema operativo específico.

Configuración de la directiva del Agente de red: comparación por sistemas operativos

Sección Directiva	Windows	Mac	Linux
General	✓	✓	✓
Configuración de eventos	✓	✓	✓
Configuración	✓	✓	✓ Solo las opciones **Tamaño máximo de la cola del evento, en MB** y **La aplicación podrá obtener información adicional sobre la directiva en el dispositivo** están disponibles.
Repositorios	✓	—	✓ Solo las opciones **Detalles de las aplicaciones instaladas** y **Detalles de registro de hardware** están disponibles.
Vulnerabilidades y actualizaciones de software	✓	—	—
Administración de reinicios	✓	—	—
Uso compartido del escritorio de Windows	✓	—	—
Administrar parches y actualizaciones	✓	—	—
Conectividad → Red	✓	✓	✓ Excepto la opción **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**.
Conectividad → Perfiles de conexión	✓	✓	—
Conectividad → Programación de conexiones	✓	✓	✓
Puntos de distribución → Sondeo de la red	✓	—	✓ Solo está disponible la sección **Sondeo de rangos IP**.
Puntos de distribución → Configuración de la conexión a Internet	✓	✓	✓
Puntos de distribución → Proxy de KSN	✓	—	—

Puntos de distribución → Actualizaciones	✓	—	—
Historial de revisiones	✓	✓	✓

Administración de cuentas de usuario.

Esta sección proporciona información sobre las cuentas y las funciones de usuarios que admite la aplicación. Esta sección proporciona instrucciones sobre cómo crear cuentas y funciones para usuarios de Kaspersky Security Center.

Kaspersky Security Center le permite administrar cuentas de usuario y grupos de cuentas. La aplicación admite dos tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración obtiene datos de las cuentas de esos usuarios cuando sondea la red de la organización.
- Cuentas de usuarios internos. Estas cuentas se aplican cuando se utilizan Servidores de administración virtuales. Las cuentas de los usuarios internos se crean y utilizan solo en Kaspersky Security Center.

Uso de cuentas de usuario

Kaspersky Security Center le permite administrar cuentas de usuario y grupos de cuentas. La aplicación admite dos tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración obtiene datos de las cuentas de esos usuarios cuando sondea la red de la organización.
- Cuentas de usuarios internos. Estas cuentas se aplican cuando se utilizan Servidores de administración virtuales. Las cuentas de los usuarios internos se crean y utilizan solo en Kaspersky Security Center.

Se pueden ver todas las cuentas de usuario en la carpeta **Cuentas de usuario** del árbol de consola. La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.

Puede realizar las acciones siguientes en las cuentas de usuario y en los grupos de cuentas:

- Configurar derechos de acceso de los usuarios a las funciones de la aplicación mediante el uso de funciones.
- Enviar mensajes a los usuarios por correo electrónico y SMS.
- Ver la lista de dispositivos móviles del usuario.
- Emitir e instalar certificados en los dispositivos móviles de los usuarios.
- Ver la lista de certificados emitidos al usuario.
- Desactivar la verificación en dos pasos de una cuenta de usuario.

Añadir una cuenta de un usuario interno

Para añadir una nueva cuenta de usuario interna a Kaspersky Security Center:

1. En el árbol de consola, abra la carpeta **Cuentas de usuario**.

   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.

2. En el espacio de trabajo, haca clic en el botón **Agregar usuario**.

3. En la ventana **Nuevo usuario** que se abre, especifique la configuración de la nueva cuenta de usuario:

   - (nombre de usuario)

     Sea cuidadoso al introducir el nombre de usuario. No podrá cambiarlo después de guardar los cambios.

   - **Descripción**
   - **Nombre completo**
   - **Correo electrónico principal**
   - **Teléfono principal**
   - **Contraseña** para la conexión del usuario a Kaspersky Security Center

     La contraseña debe cumplir con las siguientes reglas:

     - La contraseña debe tener entre 8 y 16 caracteres.
     - La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
       - Mayúsculas (A-Z)
       - Minúsculas (a-z)
       - Números (0-9)
       - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

     Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

     El número de intentos de introducción de la contraseña es limitado. De forma predeterminada, el número máximo de intentos de introducción de la contraseña permitidos es 10. Puede cambiar el número permitido de intentos para introducir una contraseña, como se describe en "Cambiar el número de intentos de ingreso de contraseña permitidos".

     Si el usuario introduce incorrectamente la contraseña el número especificado de veces, la cuenta de usuario quedará bloqueada durante una hora. En la lista de cuentas de usuario, el icono del usuario ( ) de una cuenta bloqueada está atenuado (no disponible). Puede desbloquear la cuenta de usuario cambiando solo la contraseña.

- Si es necesario, seleccione la casilla de verificación **Desactivar cuenta** para prohibir que el usuario se conecte a la aplicación. Puede desactivar una cuenta, por ejemplo, si desea crearla de antemano pero activarla más tarde.

- Marque la casilla **Solicitar la contraseña cuando se modifique la configuración de la cuenta** si desea activar una opción adicional para proteger una cuenta de usuario de modificaciones no autorizadas. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario requiere la autorización de un usuario que tenga el derecho Modificar LCA de objeto del área funcional **Funciones generales: Permisos de usuario**.

4. Haga clic en **Aceptar**.

La cuentas de usuario recién creada se muestra en el espacio de trabajo de la carpeta **Cuentas de usuario**.

Editar una cuenta de un usuario interno

Modificar una cuenta de usuario interna en Kaspersky Security Center:

1. En el árbol de consola, abra la carpeta **Cuentas de usuario**.

   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.

2. En el espacio de trabajo, haga doble clic en la cuenta de usuario interno que desee editar.

3. En la ventana **Propiedades: <nombre de usuario>** que se abre, cambie la configuración de la cuenta de usuario:

   - **Descripción**
   - **Nombre completo**
   - **Correo electrónico principal**
   - **Teléfono principal**
   - **Contraseña** para la conexión del usuario a Kaspersky Security Center

     La contraseña debe cumplir con las siguientes reglas:

     - La contraseña debe tener entre 8 y 16 caracteres.
     - La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
       - Mayúsculas (A-Z)
       - Minúsculas (a-z)
       - Números (0-9)
       - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

     Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

El número de intentos de introducción de la contraseña es limitado. De forma predeterminada, el número máximo de intentos de introducción de la contraseña permitidos es 10. Puede cambiar el número permitido de intentos para introducir una contraseña, como se describe en "Cambiar el número de intentos de ingreso de contraseña permitidos".

Si el usuario introduce incorrectamente la contraseña el número especificado de veces, la cuenta de usuario quedará bloqueada durante una hora. En la lista de cuentas de usuario, el icono del usuario () de una cuenta bloqueada está atenuado (no disponible). Puede desbloquear la cuenta de usuario cambiando solo la contraseña.

- Si es necesario, seleccione la casilla de verificación **Desactivar cuenta** para prohibir que el usuario se conecte a la aplicación. Puede desactivar una cuenta, por ejemplo, después de que un empleado abandone la empresa.
- Seleccione la opción **Solicitar la contraseña cuando se modifique la configuración de la cuenta** si desea activar una opción adicional para proteger una cuenta de usuario frente a modificaciones no autorizadas. Si esta opción está habilitada, la modificación de la configuración de la cuenta de usuario requiere la autorización de un usuario que tenga el derecho Modificar LCA de objeto del área funcional **Funciones generales: Permisos de usuario**.

4. Haga clic en **Aceptar**.

La cuenta de usuario editada se mostrará en el espacio de trabajo de la carpeta **Cuentas de usuario**.

Cambiar el número de intentos de entrada de contraseña permitidos

El usuario de Kaspersky Security Center puede introducir una contraseña no válida un número limitado de veces. Una vez que se alcanza el límite, la cuenta de usuario se bloquea durante una hora.

De forma predeterminada, el número máximo de intentos permitidos para introducir una contraseña es 10. Puede cambiar el número de intentos de entrada de contraseña permitidos, como se describe en esta sección.

Para cambiar el número de intentos de entrada de contraseña permitidos

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).
2. Vaya a la siguiente clave:
   - Para un sistema de 64 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
   - Para un sistema de 32 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. Si el valor SrvSplPpcLogonAttempts no está presente, créelo. El tipo del valor es DWORD.
   De forma predeterminada, este valor no se crea después de que Kaspersky Security Center se instala.
4. Especifique el número requerido de intentos en el valor de SrvSplPpcLogonAttempts.
5. Haga clic en **Aceptar** para guardar los cambios.

6. Reinicie el servicio del Servidor de administración.

Se cambia el número máximo de intentos de entrada de contraseña permitidos.

Configuración de la comprobación de que el nombre de un usuario interno no se repite

Puede configurar que se compruebe que el nombre de un usuario interno de Kaspersky Security Center no se repita cuando se lo agregue a la aplicación. La comprobación de que un nombre de usuario interno no se repite solo se puede realizar en un Servidor de administración virtual o en el Servidor de administración principal para el que se creó la cuenta de usuario, o en todos los Servidores de administración virtuales y en el Servidor de administración principal. De forma predeterminada, se comprueba que el nombre de un usuario interno no se repita en todos los Servidores de administración virtuales y en el Servidor de administración principal.

Para habilitar que se compruebe que el nombre de un usuario interno no se repita en un Servidor de administración virtual o en el Servidor de administración principal:

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).

2. Vaya al siguiente subárbol:

   - Para un sistema de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

   - Para un sistema de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Para la clave LP_InterUserUniqVsScope (DWORD), establezca el valor 00000001.

   El valor predeterminado especificado para esta clave es 0.

4. Reinicie el servicio del Servidor de administración.

Como resultado, solo se comprobará que el nombre no se repita en el Servidor de administración virtual donde se creó el usuario interno, o en el Servidor de administración principal si el usuario interno se creó en el Servidor de administración principal.

Para habilitar la comprobación de que el nombre de un usuario interno no se repita en todos los Servidores de administración virtuales y en el Servidor de administración principal:

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).

2. Vaya al siguiente subárbol:

   - Para un sistema de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\

   - Para un sistema de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM

3. Para la clave LP_InterUserUniqVsScope (DWORD), establezca el valor 00000000.

El valor predeterminado especificado para esta clave es 0.

4. Reinicie el servicio del Servidor de administración.

Se verificará si el nombre es único en todos los Servidores de administración virtuales y en el Servidor de administración principal.

Agregar un grupo de seguridad

Puede añadir grupos de seguridad (grupos de usuarios), realizar configuraciones flexibles de grupos y acceso de grupos de seguridad a varias funciones de la aplicación. A los grupos de seguridad se les pueden asignar nombres que corresponden a sus respectivos propósitos. Por ejemplo, el nombre puede aludir a la ubicación de los usuarios en la oficina o a la unidad organizativa de la empresa a la que pertenecen los usuarios.

Un usuario puede pertenecer a varios grupos de seguridad. Una cuenta de usuario administrada por un Servidor de administración virtual solo puede pertenecer a grupos de seguridad de dicho servidor virtual y tener derechos de acceso únicamente a este servidor virtual.

Agregar un grupo de seguridad:

1. En el árbol de consola, seleccione la carpeta **Cuentas de usuario**.

   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.

2. Haga clic en el botón **Agregar grupo de seguridad**.

   Se abre la ventana **Agregar grupo de seguridad**.

3. En la ventana **Agregar grupo de seguridad**, en la sección **General**, especifique el nombre del grupo.

   La longitud máxima del nombre del grupo es de 255 caracteres, ni contener símbolos especiales, como *, <, >, ?, \, :, |. El nombre del grupo debe ser único.

   Se puede introducir la descripción del grupo en el campo de entrada **Descripción**. Rellenar el campo **Descripción** es opcional.

4. Haga clic en **Aceptar**.

El grupo de seguridad que ha agregado aparece en la carpeta **Cuentas de usuario** del árbol de consola. Puede añadir a usuarios al grupo recién creado.

Adición de un usuario a un grupo

Para agregar un usuario a un grupo:

1. En el árbol de consola, seleccione la carpeta **Cuentas de usuario**.

   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.

2. En la lista de cuentas y grupos de usuarios, seleccione el grupo al que desea agregar el usuario.

3. En la ventana de propiedades de grupo, seleccione la sección **Usuarios del grupo** y haga clic en el botón **Agregar**.

   Se abre una ventana con una lista de usuarios.

4. En la lista, seleccione el usuario que desea incluir en el grupo.

5. Haga clic en **Aceptar**.

El usuario se añade al grupo y se muestra en la lista de usuarios del grupo.

Configuración de los derechos de acceso a las funciones de la aplicación. Control de acceso basado en funciones

Kaspersky Security Center proporciona recursos para el acceso basado en funciones a las funciones de Kaspersky Security Center o las aplicaciones administradas de Kaspersky.

Puede configurar los derechos de acceso a las funciones de la aplicación para los usuarios de Kaspersky Security Center de una de las siguientes formas:

- Mediante la configuración por separado de los derechos de cada usuario o grupo de usuarios.
- Mediante la creación de funciones de usuario estándar con un conjunto de derechos preestablecido y la asignación de esas funciones a los usuarios según su ámbito de responsabilidad.

La función de usuario (también denominada función) es un conjunto predefinido de derechos de acceso a las funciones de Kaspersky Security Center o las aplicaciones administradas de Kaspersky. Se puede asignar una función a un usuario o a un grupo de usuarios.

La aplicación de funciones de usuario tiene como objetivo simplificar y acortar los procedimientos de rutina para configurar los derechos de acceso de los usuarios a las funciones de la aplicación. Los derechos de acceso de una función se configuran según las tareas estándares y el ámbito de las responsabilidades de los usuarios.

A las funciones de usuario se les puede asignar nombres que se correspondan con sus respectivos propósitos. Puede crear un número ilimitado de funciones en la aplicación.

Puede utilizar las funciones de usuario predefinidas con un conjunto de derechos ya configurado, o crear nuevas funciones y configurar los derechos necesarios usted mismo.

Derechos de acceso a las funciones de la aplicación

La siguiente tabla muestra las funciones de Kaspersky Security Center con los derechos de acceso para administrar las tareas, informes y configuraciones asociados y realizar las acciones de usuario asociadas.

Para realizar las acciones de usuario enumeradas en la tabla, un usuario debe tener el derecho especificado junto a la acción.

Los derechos de **lectura**, **modificación** y **ejecución** pueden aplicarse a cualquier tarea, informe o configuración. Además de estos derechos, el usuario debe tener el derecho de **Realizar operaciones en selecciones de dispositivos** para administrar tareas, informes o configuraciones en selecciones de dispositivos.

Todas las tareas, informes, configuraciones y paquetes de instalación que faltan en la tabla pertenecen al área funcional **Características generales: funcionalidad básica**.

Derechos de acceso a las funciones de la aplicación

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe

Características generales: **Gestión de grupos de administración**	**Modificación**	• Añadir dispositivos a un grupo de administración: **Modificación** • Eliminar dispositivos de un grupo de administración: **Modificación** • Agregar un grupo de administración a otro grupo de administración: **Modificación** • Eliminar un grupo de administración de otro grupo de administración: **Modificación**	Ninguno	Ninguno
Características generales: **Acceder a objetos independientemente de sus ACL**	**Lectura**	Obtener acceso de lectura a todos los objetos: **Leer**	Ninguno	Ninguno
Características generales: **Funcionalidad básica**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Reglas de movimiento de dispositivos (crear, modificar o eliminar) para el Servidor virtual: **Modificación**, **realizar operaciones en selecciones de dispositivos** • Obtener certificado personalizado del protocolo móvil (LWNGT): **Lectura** • Establecer certificado personalizado del protocolo móvil (LWNGT): **Escritura** • Obtener lista de redes definidas por NLA: **Lectura** • Añadir, modificar o eliminar una lista de	• "Descargar actualizaciones en el repositorio del Servidor de administración" • "Entregar informes" • "Distribuir paquetes de instalación" • "Instalar una aplicación de forma remota en Servidores de administración secundarios"	• "Informe del estado de la protección" • "Informe de amenazas" • "Informe sobr los dispositivo más infectado • "Informe sobr el estado de l bases de dato antivirus" • "Informe de errores" • "Informe sobr ataques a la re • "Informe resumido sob las aplicacione de protección del sistema de correo instaladas"

		redes definida por NLA: **Modificación** • Ver lista de control de acceso de grupos: **Lectura** • Ver el registro de eventos de Kaspersky: **Lectura**		• "Informe resumido sob las aplicacione de defensa perimetral instaladas" • "Informe resumido sob los tipos de aplicaciones instalados" • "Informe sobr usuarios de dispositivos infectados" • "Informe sobr incidentes" • "Informe sobr eventos" • "Informe sobr la actividad de los puntos de distribución" • "Informe sobr Servidores de administració secundarios" • "Informe sobr eventos de control de dispositivos" • "Informe de vulnerabilidad • "Informe sobr aplicaciones prohibidas" • "Informe de Control web" • "Informe sobr el estado del cifrado de los dispositivos administrados • "Informe sobr el estado del cifrado de los

				dispositivos d almacenamier masivo" • "Informe sobr errores en el cifrado de archivos" • "Informe sobr el bloqueo del acceso a archivos cifrados" • "Informe sobr los derechos d acceso a dispositivos cifrados" • "Informe sobr permisos de usuario vigentes" • "Informe sobr derechos"
Características generales: **Objetos eliminados**	• **Lectura** • **Modificación**	• Ver objetos eliminados en la Papelera de reciclaje: **Lectura** • Eliminar objetos de la Papelera de reciclaje: **Modificación**	Ninguno	Ninguno
Características generales: **Procesamiento de eventos**	• **Eliminación de eventos** • **Edición de la configuración de notificación de eventos** • **Edición de la configuración del registro de eventos** • **Modificación**	• Cambiar la configuración del registro de eventos: **Edición de la configuración del registro de eventos** • Cambiar la configuración de notificación de eventos: **Edición de la configuración de notificación de eventos** • Eliminar eventos: **Eliminación de**	Ninguno	Ninguno

		eventos		
Características generales: **Operaciones en el Servidor de administración**	• **Lectura** • **Modificación** • **Ejecución** • **Modificación de las LCA de objetos** • **Realizar operaciones en selecciones de dispositivos**	• Especificar puertos del Servidor de administración para la conexión del Agente de red: **Modificación** • Especificar los puertos del Proxy de activación que se está ejecutando en el Servidor de administración: **Modificación** • Especificar los puertos del Proxy de activación de dispositivos móviles que se está ejecutando en el Servidor de administración: **Modificación** • Especificar los puertos del Servidor web para la distribución de paquetes independientes: **Modificación** • Especificar los puertos del Servidor web para la distribución de	• "Copia de seguridad de los datos del Servidor de administración" • "Mantenimiento de bases de datos"	Ninguno

		perfiles MDM: **Modificación** • Especificar los puertos SSL del Servidor de administración para la conexión a través de Kaspersky Security Center Web Console: **Modificación** • Especificar puertos del Servidor de administración para conexión de dispositivos móviles: **Modificación** • Especificar el número máximo de eventos que pueden almacenar en la base de datos del Servidor de administración: **Modificación** • Especificar el número máximo de eventos que el Servidor de administración puede enviar: **Modificación** • Especificar el periodo de tiempo durante el cual el Servidor de administración puede enviar eventos: **Modificación**		
Funciones generales: **despliegue del software de Kaspersky**	• **Administración de parches de Kaspersky** • **Lectura** • **Modificación** • **Ejecución**	Aprobar o rechazar la instalación del parche: **Administración de parches de Kaspersky**	Ninguno	• "Informe sobre el uso de clave de licencia por parte del Servidor de administración virtual" • "Informe de versiones de software de Kaspersky"

	• **Realizar operaciones en selecciones de dispositivos**			• "Informe de aplicaciones incompatibles • "Informe sobre las versiones de las actualizaciones del módulo de software de Kaspersky" • "Informe del despliegue de protección"
Características generales: **Administración de claves**	• **Exportar archivo clave** • **Modificación**	• Exportar archivo clave: **Exportar archivo clave** • Modificar la configuración de la clave de licencia del Servidor de administración: **Modificación**	Ninguno	Ninguno
Características generales: **Administración de informes**	• **Lectura** • **Modificación**	• Crear informes independientemente de sus ACL: **Escritura** • Ejecutar informes independientemente de sus ACL: **Lectura**	Ninguno	Ninguno
Funciones generales: **Jerarquía de Servidores de administración**	**Configuración de jerarquía de Servidores de administración**	Registrar, actualizar o eliminar Servidores de administración secundarios: **Configuración de la jerarquía del Servidor de administración**	Ninguno	Ninguno
Características generales: **Permisos de usuario**	**Modificación de las LCA de objetos**	• Cambiar las propiedades de "seguridad" de cualquier objeto: **Modificación de las LCA de objetos** • Administrar roles de usuario: **Modificación de las LCA de objetos**	Ninguno	Ninguno

		• Administrar usuarios internos: **Modificación de las LCA de objetos** • Administrar grupos de seguridad: **Modificación de las LCA de objetos** • Administrar alias: **Modificación de las LCA de objetos**		
Características generales: **Servidores de administración virtuales**	• **Administración de Servidores de administración virtuales** • **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Obtener lista de Servidores de administración: **Lectura** • Obtener información sobre el Servidor de administración virtual: **Lectura** • Crear, actualizar o eliminar un Servidor de administración virtual: **Administración de Servidores de administración virtuales** • Mover un Servidor de administración virtual a otro grupo: **Administración de Servidores de administración virtuales** • Establecer permisos de Servidor virtual de administración: **Administración de Servidores de administración virtuales**	Ninguno	"Informe sobre lo resultados de la instalación de actualizaciones d software de terceros"
Administración de dispositivos móviles: **General**	• **Conectar nuevos dispositivos** • **Enviar solo comandos de información a**	• Obtener datos de restauración del Servicio de administración de claves: **Leer**	Ninguno	Ninguno

	dispositivos móviles • **Enviar comandos a dispositivos móviles** • **Administración de certificados** • **Lectura** • **Modificación**	• Eliminar certificados de usuario: **Administración de certificados** • Obtener la parte pública del certificado de usuario: **Lectura** • Comprobar si la infraestructura de clave pública está activada: **Lectura** • Comprobar la cuenta de infraestructura de clave pública: **Lectura** • Obtener plantillas de infraestructura de clave pública: **Lectura** • Obtener plantillas de infraestructura de clave pública mediante certificado de uso extendido de clave: **Lectura** • Comprobar si el certificado de infraestructura de clave pública está revocado: **Lectura** • Actualizar la configuración de emisión de certificados de usuario: **Administración de certificados** • Obtener la configuración de emisión del certificado de usuario: **Lectura** • Obtener paquetes por nombre de aplicación y versión: **Lectura**	

		• Establecer o cancelar el certificado de usuario: **Administración de certificados** • Renovar certificado de usuario: **Administración de certificados** • Establecer etiqueta de certificado de usuario: **Administración de certificados** • Ejecutar la generación del paquete de instalación de MDM; cancelar la generación del paquete de instalación de MDM: **Conexión de nuevos dispositivos**		
Administración del sistema: **Conectividad**	• **Iniciar sesiones de RDP** • **Conectarse a sesiones de RDP existentes** • **Iniciar tunelización** • **Guardar archivos de dispositivos en la estación de trabajo del administrador** • **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones**	• Crear sesión para compartir escritorio: **Derecho a crear una sesión para compartir escritorio** • Crear sesión RDP: **Conectarse a sesiones RDP existentes** • Crear túnel: **Iniciar tunelización** • Guardar lista de contenido de red: **Guardar archivos de dispositivos en la estación de trabajo del administrador**	Ninguno	"Informe sobre usuarios de dispositivos"

	en selecciones de dispositivos			
Administración del sistema: **Inventario de hardware**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Obtener o exportar objeto de inventario de hardware: **Lectura** • Añadir, establecer o eliminar objeto de inventario de hardware: **Escritura**	Ninguno	• "Informe sobr el registro de hardware" • "Informe sobr cambios de configuración • "Informe sobr hardware"
Administración del sistema: **Control de acceso a la red**	• **Lectura** • **Modificación**	• Ver la configuración de CISCO: **Lectura** • Cambiar la configuración de CISCO: **Escritura**	Ninguno	Ninguno
Administración del sistema: **Despliegue del sistema operativo**	• **Desplegar servidores PXE** • **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Desplegar servidores PXE: **Desplegar servidores PXE** • Ver una lista de servidores PXE: **Lectura** • Iniciar o detener el proceso de instalación en clientes PXE: **Ejecución** • Administrar controladores para WinPE y las imágenes del sistema operativo: **Modificación**	"Crear paquete de instalación basado en la imagen del sistema operativo del dispositivo de referencia"	Ninguno
Administración del sistema: **Administración de vulnerabilidades y parches**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Ver propiedades de parches de terceros: **Lectura** • Cambiar las propiedades del parche de terceros: **Modificación**	• "Realizar la sincronización de Windows Update" • "Instalar actualizaciones de Windows Update"	"Informe de actualizaciones d software"

			• "Reparar vulnerabilidades" • "Instalar las actualizaciones necesarias y corregir vulnerabilidades"	
Administración del sistema: **Instalación remota**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Consulte las propiedades del paquete de instalación basado en Administración de vulnerabilidades y parches de terceros: **Leer** • Cambiar las propiedades del paquete de instalación basado en Administración de vulnerabilidades y parches de terceros: **Modificar**	Ninguno	Ninguno
Administración del sistema: **Inventario de software**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	Ninguno	Ninguno	• "Informe sobr aplicaciones instaladas" • "Historial de informes sobr el registro de aplicaciones" • "Informe sobr el estado de l grupos de aplicaciones c licencia" • "Informe sobr claves de licencia de software de terceros"

Funciones de usuario predefinidas

Las funciones de usuario asignadas a los usuarios de Kaspersky Security Center les proporcionan conjuntos de derechos de acceso a las funciones de la aplicación.

Puede utilizar las funciones de usuario predefinidas con un conjunto de derechos ya configurado, o crear nuevas funciones y configurar los derechos necesarios usted mismo. Algunas de las funciones de usuario predefinidas disponibles en Kaspersky Security Center se pueden asociar con puestos de trabajo específicos, por ejemplo, **Auditor**, **Director de seguridad**, **Supervisor** (estas funciones están presentes en Kaspersky Security Center a partir de la versión 11). Los derechos de acceso de estas funciones están preconfiguradas de acuerdo con las tareas estándar y el alcance de las responsabilidades de los puestos asociados. La siguiente tabla muestra como las funciones pueden estar asociadas con puestos de trabajo específicos.

Ejemplos de funciones para puestos de trabajo específicos

Función	Comentario
Auditor	Permisos de todas las operaciones con todos los tipos de informes, todas las operaciones de visualización, incluyendo la visualización de objetos eliminados (concede los permisos **Leer** y **Editar** en el área de **objetos eliminados**). No permite otras operaciones. Puede asignar esta función a una persona que realice la auditoría de su organización.
Supervisor	Permite todas las operaciones de visualización, no permite otras operaciones. Puede asignar esta función a un director de seguridad y otros gerentes a cargo de la seguridad de TI en su organización.
Director de seguridad.	Permite todas las operaciones de visualización, permite la administración de informes; otorga permisos limitados en la **administración del sistema**: área de **Conectividad**. Puede asignar esta función a un responsable a cargo de la seguridad de TI en su organización.

La siguiente tabla muestra los derechos de acceso asignados a cada función de usuario predefinida.

Derechos de acceso de las funciones de usuario predefinidas

Función	Descripción

Administrador del Servidor de administración	Permite todas las operaciones en las siguientes áreas funcionales:
	• **Funciones generales**:
	  • **Funcionalidad básica**
	  • **Procesamiento de eventos**
	  • **Jerarquía de Servidores de administración**
	  • **Servidores de administración virtual**
	• **Administración del sistema**:
	  • **Conectividad**
	  • **Inventario de hardware**
	  • **Inventario de software**

Operador del Servidor de administración	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes:
	• **Funciones generales**:
	  • **Funcionalidad básica**
	  • **Servidores de administración virtual**
	• **Administración del sistema**:

	• **Conectividad** • **Inventario de hardware** • **Inventario de software**
Auditor	Permite todas las operaciones de las áreas funcionales, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL** • **Objetos eliminados** • **Gestión reforzada de informes** Puede asignar esta función a una persona que realice la auditoría de su organización.

Administrador de instalación	Permite todas las operaciones en las siguientes áreas funcionales:
	• **Funciones generales**:
	  • **Funcionalidad básica**
	  • **Despliegue del software de Kaspersky**
	  • **Administración de claves de licencia**
	• **Administración del sistema**:
	  • **Despliegue del sistema operativo**
	  • **Administración de vulnerabilidades y parches**
	  • **Instalación remota**
	  • **Inventario de software**
	Otorga los derechos de **lectura** y **ejecución** en el área funcional **Características generales: Servidores de administración virtual**.

Operador de instalación	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes:
	• **Funciones generales**:
	  • **Funcionalidad básica**
	  • **Despliegue del software Kaspersky** (también otorga el derecho **Administrar parches de Kaspersky** en esta área)
	  • **Servidores de administración virtual**
	• **Administración del sistema**:
	  • **Despliegue del sistema operativo**
	  • **Administración de vulnerabilidades y parches**
	  • **Instalación remota**

	• **Inventario de software**
Administrador de Kaspersky Endpoint Security	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: Funcionalidad básica** • Área de Kaspersky Endpoint Security, incluidas todas las funciones
Operador de Kaspersky Endpoint Security	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes: • **Características generales: Funcionalidad básica** • Área de Kaspersky Endpoint Security, incluidas todas las funciones
Administrador principal	Permite todas las operaciones en áreas funcionales, *excepto* en las siguientes áreas, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL** • **Gestión reforzada de informes**

Operador principal	Otorga los derechos de **lectura** y **ejecución** (cuando corresponda) en todas las áreas funcionales siguientes:
	• **Funciones generales**:
	  • **Funcionalidad básica**
	  • **Objetos eliminados**
	  • **Operaciones en el Servidor de administración**
	  • **Despliegue del software de Kaspersky**
	  • **Servidores de administración virtual**
	• **Administración de dispositivos móviles: General**
	• **Administración del sistema**, incluidas todas las funciones
	• Área de Kaspersky Endpoint Security, incluidas todas las funciones

Administrador de Administración de dispositivos móviles	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: Funcionalidad básica** • **Administración de dispositivos móviles: General**
Operador de Administración de dispositivos móviles	Otorga los derechos de **lectura** y **ejecución** en el área funcional **Funciones generales**: **Funcionalidad básica**. Otorga derechos de **lectura** y **Enviar solo comandos de información a dispositivos móviles** en el área funcional **Administración de dispositivos móviles**: **General**.
Director de seguridad.	Permite todas las operaciones de las siguientes áreas funcionales, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL**

	• **Gestión reforzada de informes** Otorga derechos de **Lectura**, **Modificación**, **Ejecución**, **Guardar archivos desde los dispositivos a la estación de trabajo del administrador** y **Realizar operaciones para las selecciones de dispositivos** en el área funcional **Administración del sistema: Conectividad**. Puede asignar esta función a un responsable a cargo de la seguridad de TI en su organización.
Usuario del Self Service Portal	Permite todas las operaciones en el área funcional **Administración de dispositivos móviles: Self Service Portal**. Esta función no es compatible con Kaspersky Security Center 11 y versiones posteriores.
Supervisor	Otorga el derecho de **lectura** en las áreas funcionales **Funciones generales**: **Acceder a objetos, independientemente de sus ACL** y **Funciones generales**: **Gestión reforzada de informes**. Puede asignar esta función a un director de seguridad y otros gerentes a cargo de la seguridad de TI en su organización.
Administrador de Administración de vulnerabilidades y parches	Permite todas las operaciones en las áreas funcionales **Funciones generales**: **Funcionalidad básica** y **Administración del sistema** (incluidas todas las funciones).
Operador de Administración de vulnerabilidades y parches	Otorga derechos de **lectura** y **ejecución** (cuando corresponda) en las áreas funcionales **Funciones generales**: **Funcionalidad básica** y **Administración del sistema** (incluidas todas las funciones).

Adición de una función de usuario

Para añadir una función de usuario, siga estos pasos:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Funciones de usuario** y haga clic en el botón **Agregar**.

   La sección **Funciones de usuario** está disponible si la opción Mostrar secciones de configuración de seguridad está habilitada.

4. En la ventana de propiedades **Nueva función**, configure la función:

   - En las **Secciones**, seleccione **General** y especifique el nombre del papel.

     El nombre de una función no puede tener más de 100 caracteres.

   - Seleccione la sección **Derechos** y seleccione las casillas de verificación **Permitir** y **Denegar** que se encuentran junto a las funciones de la aplicación para configurar los derechos.

   Si está operando en el Servidor de administración principal, puede activar la opción **Retransmitir lista de funciones para Servidores de administración secundarios**.

5. Haga clic en **Aceptar**.

   Se añade la función.

Las funciones de un usuario que se hayan creado para el Servidor de administración se muestran en la ventana de propiedades del Servidor de administración, en la sección **Funciones de usuario**. Puede modificar y eliminar funciones de usuario, así como asignar funciones a grupos de usuarios o a usuarios seleccionados.

Asignación de una función a un usuario o a un grupo de usuarios

Para asignar una función a un usuario o a un grupo de usuarios, siga estos pasos:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Seguridad**.

   La sección **Seguridad** está disponible si se selecciona la casilla de verificación **Mostrar secciones de configuración de seguridad** en la ventana de configuración de la interfaz.

4. En el campo **Nombres de grupos o usuarios**, seleccione un usuario o un grupo de usuarios a los que quiera asignar una función.

   Si el usuario o el grupo no están incluidos en el campo, puede añadirlos haciendo clic en el botón **Agregar**.

   Al añadir un usuario haciendo clic en el botón **Agregar**, puede seleccionar el tipo de autenticación del usuario: Microsoft Windows o Kaspersky Security Center. La autenticación con Kaspersky Security Center se emplea para seleccionar las cuentas de los usuarios internos que se utilizan para trabajar con los Servidores de administración virtuales.

5. Seleccione la ficha **Funciones** y haga clic en el botón **Agregar**.

   Se abrirá la ventana **Funciones de usuario**. Esta ventana muestra las funciones de usuario que se han creado.

6. En la ventana **Funciones de usuario**, seleccione una función para el grupo de usuarios.
7. Haga clic en **Aceptar**.

La función con un conjunto de derechos para trabajar con el Servidor de administración se asigna al usuario o al grupo de usuarios. Las funciones asignadas se muestran en la ficha **Funciones** de la sección **Seguridad** de la ventana de propiedades del Servidor de administración.

Asignar permisos a usuarios y grupos

Puede otorgar a los usuarios y a los grupos permisos para usar diferentes funciones del Servidor de administración y de los programas de Kaspersky para los cuales tiene complementos de administración, por ejemplo, Kaspersky Endpoint Security para Windows.

Para asignar permisos a un usuario o un grupo de usuarios:

1. En el árbol de la consola, realice una de las siguientes acciones:

- Expanda el nodo del **Servidor de administración** y seleccione la subcarpeta con el nombre del Servidor de administración requerido.
- Seleccione el grupo de administración.

2. Seleccione **Propiedades** en el menú contextual del Servidor de administración o grupo de administración.
3. En la ventana de propiedades del Servidor de administración (o la ventana de propiedades del grupo de administración) que se abre, en el panel **Secciones** de la izquierda, seleccione **Seguridad**.

   La sección **Seguridad** está disponible si se selecciona la casilla de verificación **Mostrar secciones de configuración de seguridad** en la ventana de configuración de la interfaz.

4. En la sección **Seguridad**, en la lista **Nombres de grupos o usuarios**, seleccione un usuario o un grupo.
5. En la lista de permisos en la parte inferior del espacio de trabajo, en la ficha **Derechos** configurar el conjunto de derechos para el usuario o grupo:
   a. Haga clic en los signos más (+) para expandir los nodos en la lista y obtener acceso a los permisos.
   b. Seleccione las casillas de verificación **Permitir** y **Denegar** junto a los permisos que desee.

      Ejemplo 1: Expanda los objetos de **Acceder a objetos independientemente de sus ACL** o su nodo **Objetos eliminados**, y seleccione **Leer**.

      Ejemplo 2: Amplíe el nodo de funcionalidad **Básico** y seleccione **Escribir**.
6. Cuando haya configurado el conjunto de derechos, haga clic en **Aplicar**.

Se configurará el conjunto de derechos para el usuario o grupo de usuarios.

Los permisos del Servidor de administración (o el grupo de administración) se dividen en las siguientes áreas:

- Funciones generales
  - Gestión de grupos de administración (solo para Kaspersky Security Center 11 o versiones posteriores)
  - Acceder a objetos independientemente de sus ACL (solo para Kaspersky Security Center 11 o versiones posteriores)
  - Funcionalidad básica
  - Objetos eliminados (solo para Kaspersky Security Center 11 o versiones posteriores)
  - Procesamiento de eventos
  - Operaciones en el Servidor de administración (solo en la ventana de propiedades del Servidor de administración)
  - Desplegar aplicaciones de Kaspersky
  - Administración de claves de licencia
  - Administración del informe forzada (solo para Kaspersky Security Center 11 o versiones posteriores)
  - Jerarquía de servidores

    - Derechos del usuario
    - Servidores de administración virtual
- Administración de dispositivos móviles
    - General
- Administración del sistema
    - Conectividad
    - Inventario de hardware
    - Control de acceso a la red
    - Desplegar sistema operativo
    - Administrar vulnerabilidades y parches
    - Instalación remota
    - Inventario de software

Si no se selecciona **Permitir** ni **Denegar** para un permiso, el permiso se considera *indefinido*: se deniega hasta que se deniegue o permita explícitamente al usuario.

Los derechos de un usuario son la suma de:

- los propios derechos del usuario
- los derechos de todas las funciones asignadas a este usuario
- los derechos de todo el grupo de seguridad al que pertenece el usuario
- los derechos de todas las funciones asignadas a los grupos de seguridad a los que pertenece el usuario

Si al menos uno de estos conjuntos de derechos tiene **Denegar** para un permiso, al usuario se le niega este permiso, incluso si otros conjuntos lo permiten o lo dejan sin definir.

Propagación de las funciones de los usuario a Servidores de administración secundarios

De forma predeterminada, las listas de funciones del usuario de los Servidores de administración secundarios y principales son independientes. Puede configurar la aplicación para propagar automáticamente las funciones de usuario creadas en el Servidor de administración principal a todos los Servidores de administración secundarios. Las funciones de usuario también pueden propagarse desde un Servidor de administración secundario a sus propios Servidores de administración secundarios.

Para propagar funciones de usuario desde el Servidor de administración principal a los Servidores de administración secundarios:

1. Abra la ventana principal de la aplicación.
2. Realice una de las siguientes acciones:

- En el árbol de la consola, haga clic con el botón derecho en el nombre del Servidor de administración y seleccione **Propiedades** en el menú contextual.

- Si tiene una directiva del Servidor de administración activa, en el espacio de trabajo de la carpeta **Directivas**, haga clic en esta directiva con el botón derecho del ratón y seleccione **Propiedades** en el menú contextual.

3. En la ventana de propiedades del Servidor de administración o en la ventana de la configuración de la directiva, en el panel **Secciones** seleccione **Funciones de usuario**.

   La sección **Funciones de usuario** está disponible si la opción **Mostrar secciones de configuración de seguridad** está habilitada.

4. Active la opción **Retransmitir lista de roles para Servidores de administración secundarios**.

5. Haga clic en **Aceptar**.

   La aplicación copia las funciones de usuario del Servidor de administración principal a los Servidores de administración secundarios.

Cuando la opción **Retransmitir lista de funciones a Servidores de administración secundarios** está activada y las funciones de usuario se propagan, no se pueden editar ni eliminar en los Servidores de administración secundarios. Cuando crea una nueva función o edita una existente en el Servidor de administración principal, los cambios se copian automáticamente en los Servidores de administración secundarios. Cuando elimina una función de usuario en el Servidor de administración principal, esta función permanece en los Servidores de administración secundarios posteriormente, pero se puede editar o eliminar.

Las funciones que se propagan al Servidor de administración secundario desde el Servidor principal se muestran con el icono de bloqueo (🔒). No puede modificar estas funciones en el Servidor de administración secundario.

Si crea una función en el Servidor de administración principal y hay una función con el mismo nombre en su Servidor de administración secundario, el nuevo rol se copia al Servidor de administración secundario con el índice añadido a su nombre, por ejemplo, ~~ 1, ~~ 2 (el índice puede ser aleatorio).

Si deshabilita la opción **Retransmitir lista de funciones para Servidores de administración secundarios**, todas las funciones de usuario permanecen en los Servidores de administración secundarios, pero se vuelven independientes de los del Servidor de administración principal. Después de ser independientes, las funciones de usuario en los Servidores de administración secundarios se pueden editar o eliminar.

Designación del usuario como propietario del dispositivo

Puede designar a un usuario como propietario del dispositivo para confirmarlo como usuario del dispositivo. Si hace falta efectuar algunas acciones en el dispositivo, por ejemplo actualizar el software, el administrador puede notificar al propietario del dispositivo para que autorice dichas acciones.

Para designar un usuario como propietario del dispositivo:

1. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.

2. En el espacio de trabajo de la carpeta, en la ficha **Dispositivos**, seleccione el dispositivo para el que necesita designar un propietario.

3. En el menú contextual del dispositivo, seleccione **Propiedades**.

4. En la ventana de propiedades del dispositivo, seleccione **Información del sistema** → **Sesiones**.

5. Haga clic en el botón **Asignar** junto al campo **Propietario del dispositivo**.

6. En la ventana **Selección del usuario**, seleccione el usuario que quiere designar como propietario del dispositivo y haga clic en el botón **Aceptar**.

7. Haga clic en **Aceptar**.

Quedará designado el propietario del dispositivo. De forma predeterminada, el campo **Propietario del dispositivo** se rellena con un valor procedente de Active Directory y se actualiza durante cada Sondeo de Active Directory. En el **Informe sobre propietarios de dispositivos**, puede ver la lista de propietarios de dispositivos. Puede crear un informe con el Asistente para informes nuevos.

Enviar mensajes a usuarios

Para enviar un mensaje a un usuario por el correo electrónico, siga estos pasos:

1. En el árbol de consola, seleccione un usuario en la carpeta **Cuentas de usuario**.

   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.

2. En el menú contextual del usuario, seleccione **Notificar por correo electrónico**.

3. Rellene los campos relevantes en la ventana **Enviar mensaje al usuario** y haga clic en el botón **Aceptar**.

El mensaje se enviará a la dirección de correo electrónico especificada en las propiedades del usuario.

Para enviar un mensaje de texto a un usuario, siga estos pasos:

1. En el árbol de consola, seleccione un usuario en la carpeta **Cuentas de usuario**.

2. En el menú contextual del usuario, seleccione **Enviar un SMS**.

3. Rellene los campos relevantes en la ventana **Texto SMS** y haga clic en el botón **Aceptar**.

El mensaje se enviará al dispositivo móvil con el número especificado en las propiedades del usuario.

Ver la lista de dispositivos móviles de los usuarios

Para ver la lista de los dispositivos móviles de un usuario, siga estos pasos:

1. En el árbol de consola, seleccione un usuario en la carpeta **Cuentas de usuario**.

   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.

2. En el menú contextual de la cuenta de usuario, seleccione **Propiedades**.

3. En la ventana de propiedades de la cuenta de usuario, seleccione la sección **Dispositivos móviles**.

En la sección **Dispositivos móviles**, puede consultar la lista de dispositivos móviles del usuario e información sobre cada uno de ellos. Haga clic en el botón **Exportar a archivo** para guardar la lista de dispositivos móviles en un archivo.

Instalación de certificados de un usuario

Puede instalar tres tipos de certificados para un mismo usuario:

- Un certificado compartido, requerido para identificar el dispositivo móvil del usuario.
- Un certificado de correo, requerido para configurar el correo corporativo en el dispositivo móvil del usuario.
- Un certificado de VPN, requerido para configurar la red privada virtual en el dispositivo móvil del usuario.

Para emitir un certificado a un usuario e instalarlo, siga estos pasos:

1. En el árbol de consola, abra la carpeta **Cuentas de usuario** y seleccione una cuenta de usuario.
   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.
2. En el menú contextual de la cuenta de usuario, seleccione **Instalar certificado**.

Se inicia el Asistente de instalación de certificados. Siga las instrucciones del Asistente.

Cuando el Asistente de instalación de certificados finalice, se habrá creado e instalado el certificado del usuario. Puede ver la lista de certificados de usuario instalados y exportarlos a un archivo.

Visualización de la lista de certificados que se emiten a un usuario

Para ver la lista de todos los certificados emitidos a un usuario, siga estos pasos:

1. En el árbol de consola, seleccione un usuario en la carpeta **Cuentas de usuario**.
   La carpeta **Cuentas de usuario** es una subcarpeta de la carpeta predeterminada **Avanzado**.
2. En el menú contextual de la cuenta de usuario, seleccione **Propiedades**.
3. En la ventana de propiedades de la cuenta de usuario, seleccione la sección **Certificados**.

En la sección **Certificados**, puede consultar la lista de certificados del usuario e información sobre cada uno de ellos. Haga clic en el botón **Exportar a archivo** para guardar la lista de certificados en un archivo.

Acerca del administrador de Servidor de administración virtual

Un administrador de la red empresarial administrada a través de un Servidor de administración virtual inicia Kaspersky Security Center 14 Web Console en la cuenta de usuario especificada en esta ventana para ver los detalles de la protección antivirus.

Si fuera necesario, pueden crearse varias cuentas de administrador en un Servidor virtual.

El administrador de un Servidor de administración virtual es un usuario interno de Kaspersky Security Center. No se transfiere ningún dato de los usuarios internos al sistema operativo. Kaspersky Security Center autentifica los usuarios internos.

Instalación remota de sistemas operativos y aplicaciones

Kaspersky Security Center permite crear imágenes de los sistemas operativos y desplegarlas en los dispositivos cliente de la red, como también permite realizar la instalación remota de las aplicaciones de Kaspersky y de otros proveedores.

Para crear imágenes de sistemas operativos, debe instalar la herramienta Windows ADK y el complemento de Windows PE para Windows ADK en el Servidor de administración. Le recomendamos que instale las últimas versiones de Windows ADK y del complemento de Windows PE para Windows ADK. Puede crear una imagen de cualquier versión del sistema operativo Windows que cumpla con los requisitos de Kaspersky Security Center.

Captura de imágenes de sistemas operativos

Kaspersky Security Center puede capturar imágenes de sistemas operativos de los dispositivos y transferirlas al Servidor de administración. Estas imágenes de sistemas operativos se almacenan en el Servidor de administración en una carpeta exclusiva. La imagen del sistema operativo de un dispositivo de referencia se captura y luego se crea a través de una tarea de creación de paquete de instalación.

La funcionalidad de captura de imágenes del sistema operativo tiene las siguientes funciones:

- No se puede capturar una imagen del sistema operativo en un dispositivo donde esté instalado el Servidor de administración.
- Mientras se captura una imagen del sistema operativo, una utilidad denominada sysprep.exe restablece la configuración del dispositivo de referencia. Si necesita restaurar la configuración del dispositivo de referencia, seleccione la casilla **Crear una copia de seguridad del estado del dispositivo** en el Asistente de creación de imágenes del sistema operativo.
- El proceso de captura de imágenes posibilita el reinicio del dispositivo de referencia.

Despliegue de imágenes de sistemas operativos en dispositivos nuevos

Puede usar las imágenes recibidas para desplegarlas en los nuevos dispositivos de red en los que aún no se ha instalado ningún sistema operativo. En este caso, se usa una tecnología denominada entorno de ejecución de prearranque (PXE). Usted selecciona un dispositivo en red que actuará como servidor PXE. Este dispositivo debe cumplir los siguientes requisitos:

- El Agente de red debe estar instalado en el dispositivo.
- No debe haber ningún servidor DHCP activo en el dispositivo, ya que el servidor PXE utiliza los mismos puertos que un servidor DHCP.
- El segmento de red en el que se encuentra el dispositivo no debe contener ningún otro servidor PXE.

Se deben cumplir las siguientes condiciones para implementar un sistema operativo:

- El dispositivo debe tener instalada una tarjeta de red.
- El dispositivo debe estar conectado a la red.
- La opción Inicio de red debe seleccionarse en el BIOS al iniciar el dispositivo.

El despliegue de un sistema operativo se realiza del siguiente modo:

1. El servidor PXE establece conexión con un dispositivo cliente nuevo mientras este se está iniciando.
2. El dispositivo cliente se convierte en parte integrante del Entorno de preinstalación de Windows (WinPE).

   Agregar el dispositivo al entorno WinPE puede requerir que se configure el conjunto de controladores de WinPE.

3. El dispositivo cliente se registra en el Servidor de administración.
4. El administrador le asigna al dispositivo cliente un paquete de instalación con una imagen del sistema operativo.

   El administrador puede agregar controladores requeridos al paquete de instalación con la imagen del sistema operativo. El administrador también puede especificar un archivo de configuración con la configuración del sistema operativo (archivo de respuesta) que se debe aplicar durante la instalación.

5. El sistema operativo se despliega en el dispositivo cliente.

El administrador puede especificar manualmente las direcciones MAC de los dispositivos cliente que aún no se han conectado y asignarles el paquete de instalación con la imagen del sistema operativo. Cuando los dispositivos cliente seleccionados se conectan al servidor PXE, el sistema operativo se instala automáticamente en esos dispositivos.

Despliegue de imágenes de sistemas operativos en dispositivos donde ya se ha instalado otro sistema operativo

El despliegue de imágenes de sistemas operativos en dispositivos cliente donde ya se ha instalado otro sistema operativo se realiza a través de la tarea de instalación remota para dispositivos específicos.

Instalación de aplicaciones Kaspersky y de otros proveedores

El administrador puede crear paquetes de instalación de cualquier aplicación, incluso aquellas especificadas por el usuario, e instalar estas aplicaciones en dispositivos cliente a través de la tarea de instalación remota.

Creación de imágenes de sistemas operativos

Las imágenes de sistemas operativos se crean usando la tarea de eliminación de la imagen del sistema operativo del dispositivo de referencia.

Siga estos pasos para crear la tarea de creación de imágenes de sistema operativo:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. Haga clic en el botón **Crear paquete de instalación** para ejecutar el Asistente de nuevo paquete.
3. En la ventana **Seleccione el tipo de paquete de instalación** del Asistente, haga clic en el botón **Crear un paquete de instalación con una imagen del sistema operativo**.

4. Siga las instrucciones del Asistente.

   Cuando el Asistente termina, se crea una tarea del Servidor de administración denominada **Crear un paquete de instalación basado en la imagen del SO del dispositivo de referencia**. Puede ver la tarea en la carpeta **Tareas**.

Cuando se completa la tarea **Crear un paquete de instalación basado en la imagen del SO del dispositivo de referencia**, se crea un paquete de instalación que puede usar para desplegar el sistema operativo en los dispositivos cliente a través de un servidor PXE o de la tarea de instalación remota. Puede ver el paquete de instalación en la carpeta **Paquetes de instalación**.

Instalación de imágenes de sistemas operativos

Kaspersky Security Center le permite desplegar imágenes WIM de sistemas operativos de Windows® de escritorio y basados en el servidor en dispositivos dentro de una red de la organización.

Pueden utilizarse los siguientes métodos para recuperar la imagen de un sistema operativo que podría desplegarse usando herramientas de Kaspersky Security Center:

- Importar desde el archivo install.wim incluido en el paquete de distribución de Windows.
- Capturar una imagen de un dispositivo de referencia.

Se admiten dos situaciones para el despliegue de imágenes del sistema operativo:

- El despliegue en un dispositivo "limpio", es decir, sin ningún sistema operativo instalado.
- El despliegue en un dispositivo que ejecuta Windows.

El Servidor de administración incluye implícitamente una imagen de servicio del entorno de preinstalación de Windows (Windows PE), que se usa siempre tanto para capturar imágenes del sistema operativo como para su despliegue. Todos los controladores requeridos para el correcto funcionamiento de todos los dispositivos de destino se deben añadir a WinPE. Generalmente, los controladores de chipset requeridos para el funcionamiento de la interfaz de redes de Ethernet se deben añadir.

Se debe cumplir con los siguientes requisitos a fin de implementar situaciones para el despliegue y la captura de la imagen:

- El Kit de Instalación automática de Windows (WAIK) versión 2.0 o posterior o el Kit de Evaluación y despliegue de Windows (WADK) deben instalarse en el Servidor de administración. Si la situación permite la instalación o la captura de imágenes en Windows XP, WAIK debe instalarse.
- Un servidor DHCP debe estar disponible en la red donde se ubica el dispositivo de destino.
- La carpeta compartida del Servidor de administración debe estar abierta a la lectura desde la red donde se ubica el dispositivo de destino. Si la carpeta compartida se ubica en el Servidor de administración, se requiere acceso a la cuenta de KlPxeUser (esta cuenta se crea automáticamente mientras se ejecuta el programa de instalación del Servidor de administración). Si la carpeta compartida se ubica fuera del Servidor de administración, se debe conceder acceso a todos.

Al seleccionar la imagen del sistema operativo para instalar, el administrador debe especificar explícitamente la arquitectura de la CPU del dispositivo de destino: x86 o x86-64.

Configurar la dirección del proxy de KSN

Por defecto, el nombre de dominio del Servidor de administración coincide con la dirección del proxy de KSN. Si cambia el nombre de dominio del Servidor de administración, debe especificar la dirección correcta del proxy de KSN para evitar que se pierda la conexión entre los dispositivos host y el KSN.

Para configurar la dirección del proxy de KSN, siga estos pasos:

1. En el árbol de consola, vaya a **Avanzado** → **Instalación remota** → **Paquetes de instalación**.
2. En el menú contextual de **Paquetes de instalación**, seleccione **Propiedades**.
3. En la ventana que se abre, especifique la nueva dirección del proxy de KSN en la pestaña **General**.
4. Haga clic en el botón **Aplicar**.

A partir de ahora, la dirección especificada se utiliza como dirección del proxy de KSN.

Adición de controladores para el entorno de preinstalación de Windows (WinPE)

Para agregar controladores para el Entorno de preinstalación de Windows (WinPE):

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Desplegar imágenes de dispositivos**.
2. En el espacio de trabajo de la carpeta **Desplegar imágenes de dispositivos**, haga clic en el botón **Acciones adicionales** y seleccione **Configurar el conjunto de controladores para el entorno de preinstalación de Windows (WinPE)** en la lista desplegable.

   Se abre la ventana **Controladores del entorno de preinstalación de Windows**.
3. En la ventana **Controladores del entorno de preinstalación de Windows**, haga clic en el botón **Agregar**.

   Se abre la ventana **Seleccionar controlador**.
4. En la ventana **Seleccionar controlador**, seleccione uno en la lista.

   Si el controlador requerido no está en la lista, haga clic en el botón **Agregar** y especifique el nombre del controlador y la carpeta del paquete de distribución correspondiente en la ventana **Agregar controlador** emergente.

   Puede seleccionar una carpeta haciendo clic en el botón **Examinar**.

   En la ventana **Agregar controlador**, haga clic en **Aceptar**.
5. En la ventana **Seleccionar controlador**, haga clic en **Aceptar**.

   El controlador se agregará al repositorio del Servidor de administración. Cuando se agrega al repositorio, el controlador aparece en la ventana **Seleccionar controlador**.
6. En la ventana **Controladores del entorno de preinstalación de Windows**, haga clic en **Aceptar**.

El controlador se agregará al entorno de preinstalación de Windows (WinPE).

Adición de controladores en un paquete de instalación con una imagen de sistema operativo

Siga estos pasos para agregar controladores a un paquete de instalación con una imagen de sistema operativo:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. En el menú contextual de un paquete de instalación con una imagen de sistema operativo, seleccione **Propiedades**.

   Se abre la ventana de propiedades del paquete de instalación.
3. En la ventana de propiedades del paquete de instalación, seleccione la sección **Controladores adicionales**.
4. Haga clic en el botón **Agregar** de la sección **Controladores adicionales**.

   Se abre la ventana **Seleccionar controlador**.
5. En la ventana **Seleccionar controlador**, seleccione los controladores que desea agregar al paquete de instalación con la imagen de sistema operativo.

   Puede agregar los nuevos controladores al repositorio del Servidor de administración haciendo clic en el botón **Agregar** en la ventana **Seleccionar controlador**.
6. Haga clic en **Aceptar**.

Los controladores agregados aparecen en la sección **Controladores adicionales** de la ventana de propiedades del paquete de instalación con la imagen de sistema operativo.

Configuración de la utilidad sysprep.exe

La utilidad sysrep.exe sirve para preparar el dispositivo para la creación de una imagen del sistema operativo.

Siga estos pasos para configurar la utilidad sysprep.exe:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. En el menú contextual de un paquete de instalación con una imagen de sistema operativo, seleccione **Propiedades**.

   Se abre la ventana de propiedades del paquete de instalación.
3. En la ventana de propiedades del paquete de instalación, seleccione la sección **Configuración de sysprep.exe**.
4. En la sección **Configuración de sysprep.exe**, especifique un archivo de configuración que se usará al desplegar el sistema operativo en el dispositivo cliente:

   - **Usar archivo de configuración predeterminado**. Seleccione esta opción para utilizar el archivo de respuesta generado de forma predeterminada durante la captura de una imagen de sistema operativo.
   - **Especificar valores personalizados de la configuración principal**. Seleccione esta opción para especificar valores de configuración a través de la interfaz de usuario.
   - **Especificar archivo de configuración**. Seleccione esta opción para utilizar un archivo personalizado de respuesta.
5. Para aplicar los cambios realizados, haga clic en el botón **Aplicar**.

Despliegue de sistemas operativos en los nuevos dispositivos de la red

Para desplegar un sistema operativo en dispositivos nuevos a los que aún no se les ha instalado ningún sistema operativo, realice lo siguiente:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Desplegar imágenes de dispositivos**.

2. Haga clic en el botón **Acciones adicionales** y seleccione **Administrar la lista de servidores PXE de la red** en la lista desplegable.

   Se abre la ventana **Propiedades**: **Desplegar imágenes de dispositivos** y muestra la sección **Servidores PXE**.

3. En la sección **Servidores PXE**, haga clic en el botón **Agregar** y, en la ventana **Servidores PXE** que se abra, seleccione el dispositivo que se utilizará como servidor PXE.

   El dispositivo que añadió se muestra en la sección Servidores PXE.

4. En la sección **Servidores PXE**, seleccione un servidor PXE y haga clic en el botón **Propiedades**.

5. En la ventana de propiedades del servidor PXE seleccionado, en la ficha **Configuración de la conexión del servidor PXE**, defina la conexión entre el Servidor de administración y el servidor PXE.

6. Inicie el dispositivo cliente en el que desea desplegar el sistema operativo.

7. En el BIOS del dispositivo cliente, seleccione la opción de instalación de arranque de red.

   El dispositivo cliente se conecta al servidor PXE y, a continuación, se muestra en el espacio de trabajo de la carpeta **Desplegar imágenes de dispositivos**.

8. En la sección **Acciones**, haga clic en el enlace **Asignar paquete de instalación** para seleccionar el paquete de instalación que se usará para instalar el sistema operativo en el dispositivo seleccionado.

   Tras agregar un dispositivo y haberle asignado un paquete de instalación, se inicia automáticamente el despliegue del sistema operativo en dicho dispositivo.

9. Para cancelar el despliegue de un sistema operativo en un dispositivo cliente, haga clic en el enlace **Cancelar la instalación de imágenes del SO** en la sección **Acciones**.

Siga estos pasos para agregar los dispositivos según la dirección MAC:

- En la carpeta **Desplegar imágenes de dispositivos**, haga clic en **Agregar dirección MAC de dispositivo** para abrir la ventana **Nuevo dispositivo** y especificar la dirección MAC del dispositivo que desea agregar.

- En la carpeta **Desplegar imágenes de dispositivos**, haga clic en **Importar direcciones MAC de dispositivos desde un archivo** para seleccionar el archivo que contiene una lista de direcciones MAC de todos los dispositivos en los cuales desea desplegar un sistema operativo.

Despliegue de sistemas operativos en dispositivos cliente

Para desplegar un sistema operativo en dispositivos cliente con otro sistema operativo ya instalado:

1. En el árbol de la consola, abra la carpeta **Instalación remota** y haga clic en el enlace **Desplegar paquete de instalación en los dispositivos administrados (estaciones de trabajo)** para ejecutar el Asistente de

despliegue de la protección.

2. En la ventana **Seleccione un paquete de instalación** del Asistente, especifique paquete de instalación con una imagen de sistema operativo.

3. Siga las instrucciones del Asistente.

Cuando el Asistente complete su operación, se habrá creado una tarea de instalación remota para instalar el sistema operativo en dispositivos cliente. Puede iniciar o detener la tarea en la carpeta **Tareas**.

Creación de paquetes de instalación de aplicaciones

Para crear un paquete de instalación de aplicaciones:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.

2. Haga clic en el botón **Crear paquete de instalación** para ejecutar el Asistente de nuevo paquete.

3. En la ventana **Seleccione el tipo de paquete de instalación** del Asistente, haga clic en uno de los siguientes botones:

   - **Crear un paquete de instalación para una aplicación de Kaspersky**. Seleccione esta opción si desea crear un paquete de instalación para una aplicación Kaspersky.

   - **Crear un paquete de instalación para el archivo ejecutable especificado**. Seleccione esta opción si desea usar un archivo ejecutable para crear un paquete de instalación de aplicaciones de terceros. Normalmente, el archivo ejecutable es un archivo de instalación de la aplicación.

     - Copiar toda la carpeta en el paquete de instalación

       Seleccione esta opción si el archivo ejecutable viene acompañado de archivos adicionales necesarios para la instalación de la aplicación. Antes de habilitar esta opción, asegúrese de que todos los archivos requeridos estén almacenados en la misma carpeta. Si esta opción está habilitada, la aplicación agrega el contenido completo de la carpeta, incluido el archivo ejecutable especificado, al paquete de instalación.

     - Parámetros de instalación específicos

Para una instalación remota exitosa, la mayoría de las aplicaciones requieren que la instalación se realice en modo silencioso. Si este es el caso, debe especificar el parámetro para una instalación silenciosa.

Configure los parámetros de instalación:

- **Línea de comando de archivo ejecutable**

  Si la aplicación requiere parámetros adicionales para una instalación silenciosa, especifíquelos en este campo. Consulte la documentación del proveedor para más detalles.

  También puede introducir otros parámetros.

- **Convertir la configuración a valores recomendados para aplicaciones reconocidas por Kaspersky Security Center 14**

  La aplicación se instalará con la configuración recomendada, si la información sobre la aplicación especificada se encuentra en la base de datos de Kaspersky.

  Si ha ingresado parámetros en el campo **Línea de comando de archivo ejecutable**, se los reemplaza por los ajustes recomendados.

  Esta opción está activada de forma predeterminada.

  La base de datos de Kaspersky la crean y mantienen los analistas de Kaspersky. Para cada aplicación que se agrega a la base de datos, los analistas de Kaspersky definen la configuración de instalación óptima. La configuración se define para garantizar la instalación remota correcta de una aplicación en un dispositivo cliente. La base de datos se actualiza automáticamente en el Servidor de administración cuando ejecuta la tarea Descargar actualizaciones en el repositorio del Servidor de administración.

- **Seleccionar una aplicación de la base de datos de Kaspersky para crear un paquete de instalación**. Elija esta opción si desea seleccionar la aplicación de terceros correspondiente en la base de datos de Kaspersky para crear un paquete de instalación. La base de datos se crea automáticamente cuando ejecuta la tarea Descargar actualizaciones en el repositorio del Servidor de administración. Las aplicaciones se muestran en la lista.

- **Crear un paquete de instalación con la imagen del sistema operativo**. Seleccione esta opción si desea crear un paquete de instalación con una imagen del sistema operativo de un dispositivo de referencia.

  Cuando el Asistente termina, se crea una tarea del Servidor de administración con el nombre **Crear un paquete de instalación basado en la imagen del SO del dispositivo de referencia**. Cuando se complete esta tarea, se crea un paquete de instalación que puede utilizar para desplegar la imagen del sistema operativo mediante un servidor PXE o la tarea de instalación remota.

4. Siga las instrucciones del Asistente.

Al finalizar la operación del Asistente, se crea un paquete de instalación que se podrá usar para instalar la aplicación en dispositivos cliente. Puede ver el paquete de instalación seleccionando **Paquetes de instalación** en el árbol de la consola.

Emisión de un certificado para los paquetes de instalación de aplicaciones

Para emitir un certificado para el paquete de instalación de una aplicación:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.

   La carpeta **Instalación remota** es una subcarpeta de la carpeta predeterminada **Avanzado**.

2. En el menú contextual de la carpeta **Paquetes de instalación**, seleccione **Avanzado**.

   Se abre la ventana de propiedades de la carpeta **Paquetes de instalación**.

3. En la ventana de propiedades de la carpeta **Paquetes de instalación**, seleccione la sección **Firmar paquetes independientes**.

4. En la sección **Firmar paquetes independientes**, haga clic en el botón **Specify**.

   La ventana **Certificado**.

5. En el campo **Tipo de certificado**, especifique el tipo de certificado público o privado:

   - Si está seleccionado el valor **Contenedor PKCS #12**, especifique el archivo de certificado y la contraseña.
   - Si el valor **Certificado X.509** está seleccionado:

     a. Especifique el archivo clave privado (tiene la extensión *.prk o *.pem).

     b. Especifique la contraseña de la clave privada.

     c. Especifique el archivo clave público (tiene la extensión *.cer).

6. Haga clic en **Aceptar**.

Se emite un certificado para el paquete de instalación de la aplicación.

Instalación de aplicaciones en dispositivos cliente

Para instalar una aplicación en dispositivos cliente:

1. En el árbol de la consola, abra la carpeta **Instalación remota** y haga clic en **Desplegar paquete de instalación en los dispositivos administrados (estaciones de trabajo)** para ejecutar el Asistente de despliegue de la protección.

2. En la ventana **Seleccione un paquete de instalación** del Asistente, especifique el paquete de instalación de la aplicación que desee instalar.

3. Siga las instrucciones del Asistente.

Al termina la operación del Asistente, se crea una tarea de instalación remota para instalar la aplicación en dispositivos cliente. Puede iniciar o detener la tarea en la carpeta **Tareas**.

Usando el Asistente de despliegue de la protección, puede instalar el Agente de red en dispositivos cliente que ejecuten Windows, Linux y macOS.

Para administrar aplicaciones de seguridad de 64 bits mediante Kaspersky Security Center en dispositivos con sistemas operativos Linux, debe usar el Agente de red de 64 bits para Linux. Puede descargar la versión necesaria del Agente de red desde el sitio web del Servicio de soporte técnico.

Antes de la instalación remota de Agente de red en un dispositivo que funcione con Linux, debe preparar el dispositivo.

Administración de revisiones de objetos

Esta sección contiene información sobre la administración de la revisión de objetos. Kaspersky Security Center le permite rastrear la modificación de objeto. Cada vez que guarda cambios realizados en un objeto, se crea una *revisión*. Cada revisión tiene un número.

Los objetos de aplicación que admiten administración de la revisión incluyen:

- Servidores de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las acciones siguientes en revisiones de objetos:

- Compare una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Compare un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Vea una revisión seleccionada
- Deshaga cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como un archivo .txt

En la ventana de propiedades de cualquier objeto que admita administración de la revisión, la sección **Historial de revisiones** muestra una lista de revisiones de objetos con los siguientes datos:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto
- Acción que se ejecutó sobre el objeto
- Descripción de la revisión relacionada con el cambio realizado a la configuración de objeto

  De forma predeterminada, la descripción de la revisión de objeto está en blanco. Para agregar una descripción a una revisión, seleccione la revisión relevante y haga clic en el botón **Descripción**. En la ventana **Descripción de la revisión del objeto**, añada texto para la descripción de la revisión.

Sobre las revisiones de objetos

Puede realizar las acciones siguientes en revisiones de objetos:

- Compare una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Compare un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Vea una revisión seleccionada
- Deshaga cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como un archivo .txt

En la ventana de propiedades de cualquier objeto que admita administración de la revisión, la sección **Historial de revisiones** muestra una lista de revisiones de objetos con los siguientes datos:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto
- Acción que se ejecutó sobre el objeto
- Descripción de la revisión relacionada con el cambio realizado a la configuración de objeto

Ver la sección Historial de revisión

Puede comparar revisiones de un objeto con la revisión actual, comparar revisiones diferentes seleccionadas en la lista o comparar una revisión de un objeto con una revisión de otro objeto del mismo tipo.

*Para ver la sección **Historial de revisiones** de un objeto:*

1. En el árbol de consola, seleccione uno de los siguientes objetos:
   - Nodo del **Servidor de administración**
   - Carpeta **Directivas**
   - Carpeta **Tareas**
   - Carpeta de un grupo de administración
   - Carpeta **Cuentas de usuario**
   - Carpeta **Objetos eliminados**
   - Subcarpeta **Paquetes de instalación**, que está anidada en la carpeta **Instalación remota**

2. Según la ubicación del objeto relevante, realice una de las siguientes acciones:

   - Si el objeto está en el nodo del **Servidor de administración** o en un nodo del grupo de administración, haga clic con el botón derecho en el nodo y, en el menú contextual, seleccione **Propiedades**.
   - Si el objeto está en la carpeta **Directivas**, **Tareas**, **Cuentas de usuario**, **Objetos eliminados** o **Paquetes de instalación**, seleccione la carpeta y en el espacio de trabajo correspondiente seleccione el objeto.

   Se abre la ventana de propiedades del objeto.

3. En el panel izquierdo **Secciones**, seleccione **Historial de revisiones**.

   El historial de revisiones se muestra en el espacio de trabajo.

Comparación de revisiones de objeto

Puede comparar revisiones anteriores de un objeto con la revisión actual, comparar revisiones diferentes seleccionadas en la lista o comparar una revisión de un objeto con una revisión de otro objeto del mismo tipo.

Comparar revisiones de un objeto:

1. Seleccione un objeto y vaya a la ventana de propiedades del objeto.
2. En la ventana de propiedades, vaya a la sección **Historial de revisiones**.
3. En la lista de revisiones de objeto del espacio de trabajo, seleccione la revisión para la comparación.

   Para seleccionar más de una revisión del objeto, use las teclas **Mayús** y **Ctrl**.

4. Realice una de las siguientes acciones:

   - Haga clic en el botón **Comparar** y seleccione uno de los valores de la lista desplegable:

     - **Comparar con revisión actual**

       Seleccione esta opción para comparar la revisión seleccionada con la actual.

     - **Comparar revisiones seleccionadas**

       Seleccione esta opción para comparar dos revisiones seleccionadas.

     - **Comparar con otra tarea**

       Si trabaja con revisiones de la tarea, seleccione **Comparar con otra tarea** para comparar la revisión seleccionada con una revisión de otra tarea.

       Si trabaja con revisiones de la directiva, seleccione **Comparar con otra directiva** para comparar la revisión seleccionada con una revisión de otra directiva.

   - Haga doble clic en el nombre de una revisión y, en la ventana de propiedades de la revisión que se abre, haga clic en uno de los siguientes botones:

     - **Comparar con actual**

Haga clic en este botón para comparar la revisión seleccionada con la actual.

- **Comparar con anterior**

  Haga clic en este botón para comparar la revisión seleccionada de la anterior.

Se muestra un informe en formato HTML sobre la comparación de las revisiones en su navegador predeterminado.

En este informe, puede minimizar algunas secciones que contienen la configuración de la revisión. Para minimizar una sección con la configuración de la revisión de objeto, haga clic en el icono minimizado ( ) al lado de la sección Nombre.

Las revisiones del Servidor de administración incluyen todos los detalles de cambios realizados, excepto la información de las siguientes áreas:

- Sección **Tráfico**
- Sección **Reglas de etiquetado**
- Sección **Notificación**
- Sección **Puntos de distribución**
- Sección **Brote de virus**

  No hay información registrada de la sección **Brote de virus** sobre la configuración de la activación de la directiva que se produce cuando se activa un evento de brote de virus.

Puede comparar las revisiones de un objeto eliminado con una revisión de un objeto existente, pero no a la inversa: no puede comparar las revisiones de un objeto existente con una revisión de un objeto eliminado.

Configuración del plazo de almacenamiento para revisiones de objetos y para información de objetos eliminados

El plazo de almacenamiento para revisiones de objeto y para información sobre objetos eliminados es lo mismo. El plazo de almacenamiento predeterminado es de 90 días. Esto es suficiente tiempo para la auditoría habitual del programa.

Solo los usuarios con el permiso **Modificar** en el área de **Objetos eliminados** puede cambiar el periodo de almacenamiento.

Para cambiar el plazo de almacenamiento para las revisiones de objetos y para obtener información sobre los objetos eliminados:

1. En el árbol de la consola, seleccione el Servidor de administración para el que desea cambiar el periodo de almacenamiento.
2. Haga clic derecho y en el menú contextual seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración que se abre, en la sección **Repositorio del historial de revisiones**, introduzca el plazo de almacenamiento deseado (el número de días).

4. Haga clic en **Aceptar**.

Las revisiones de objetos y la información sobre los objetos eliminados se almacenarán durante el número de días que introdujo.

Ver una revisión de objeto

Si necesita saber qué modificaciones se hicieron a un objeto durante cierto período de tiempo, puede ver las revisiones de este objeto.

Para ver las revisiones de un objeto:

1. Vaya a la sección **Historial de revisiones** del objeto.
2. En la lista de revisiones de objetos, seleccione la revisión cuya configuración desea ver.
3. Realice una de las siguientes acciones:
   - Haga clic en el botón **Ver revisión**.
   - Abra la ventana de propiedades de la revisión haciendo doble clic sobre el nombre de la revisión y, luego, haciendo clic en el botón **Ver revisión**.

Se muestra un informe en formato HTML con la configuración de la revisión de objeto seleccionado. En este informe, puede minimizar algunas de las secciones con la configuración de la revisión del objeto. Para minimizar una sección con la configuración de la revisión de objeto, haga clic en el icono minimizado ( ) al lado de la sección Nombre.

Guardar una revisión de objeto en un archivo

Puede guardar una revisión de objeto como un archivo de texto, por ejemplo, para enviarlo por correo electrónico.

Guardar una revisión de objeto en un archivo:

1. Vaya a la sección **Historial de revisiones** del objeto.
2. En la lista de revisiones de un objeto, seleccione esa cuya configuración necesita guardar.
3. Haga clic en el botón **Avanzado** y seleccione el valor **Guardar en archivo** en la lista desplegable.

La revisión ahora se guarda como un archivo .txt.

Revertir cambios

Puede revertir los cambios realizados en un objeto, si es necesario. Por ejemplo, es posible que tenga que revertir la configuración de una directiva a su estado en una fecha específica.

Para revertir los cambios realizados en un objeto:

1. Vaya a la sección **Historial de revisiones** del objeto.

2. En la lista de revisiones de objetos, seleccione el número de la revisión a la que quiere revertir los cambios.

3. Haga clic en el botón **Avanzado** y seleccione el valor **Revertir** en la lista desplegable.

El objeto se revierte ahora a la revisión seleccionada. La lista de revisiones de objetos muestra un registro de la acción que se tomó. La descripción de la revisión muestra la información sobre el número de la revisión a la cual revertió el objeto.

Agregar una descripción a la revisión

Puede agregar una descripción a la revisión para simplificar la búsqueda de revisiones en la lista.

Para agregar una descripción para una revisión:

1. Vaya a la sección **Historial de revisiones** del objeto.

2. En la lista de revisiones de objetos, seleccione la revisión a la que necesita agregar una descripción.

3. Haga clic en el botón **Descripción**.

4. En la ventana **Descripción de la revisión del objeto**, añada texto para la descripción de la revisión.
   De forma predeterminada, la descripción de la revisión de objeto está en blanco.

5. Haga clic en **Aceptar**.

Eliminación de objetos

Esta sección proporciona información sobre la eliminación de objetos y la visualización de información sobre los objetos una vez que se eliminan.

Puede eliminar objetos, incluidos los siguientes:

- Directivas
- Tareas
- Paquetes de instalación
- Servidores de administración virtual
- Usuarios
- Grupos de seguridad
- Grupos de administración

Cuando elimina un objeto, la información sobre él permanece en la base de datos. El plazo de almacenamiento para la información sobre los objetos eliminados es el mismo que el plazo de almacenamiento para las revisiones de objetos (el plazo recomendado es de 90 días). Puede cambiar el plazo de almacenamiento solo si tiene el permiso **Modificar** en el área de derechos **Objetos eliminados**.

Eliminación de un objeto

Puede eliminar objetos como directivas, tareas, paquetes de instalación, usuarios internos y grupos de usuarios internos si tiene permiso de Modificar, que está en la categoría de derechos de la funcionalidad básica (consulte Asignación de permisos a usuarios y grupos para obtener más información).

Para eliminar un objeto:

1. En el árbol de la consola, en el espacio de trabajo de la carpeta requerida, seleccione un objeto.
2. Realice una de las siguientes acciones:
   - Haga clic con el botón derecho del ratón en el objeto y seleccione **Eliminar**.
   - Pulse la tecla **SUPRIMIR**.

   El objeto se eliminará y la información sobre él se guardará en la base de datos.

Visualización de información sobre objetos eliminados

La información sobre los objetos eliminados se almacena en la carpeta Objetos eliminados durante la misma cantidad de tiempo que las revisiones de objetos (el periodo recomendado es de 90 días).

Solo los usuarios con permiso de **Lectura** en el área de derechos **Objetos eliminados** pueden ver la lista de objetos eliminados (consulte Asignación de permisos a usuarios y grupos para obtener más información).

Para ver la lista de objetos eliminados,

En el árbol de la consola, seleccione **Objetos eliminados** (de forma predeterminada, **Objetos eliminados** es una subcarpeta de la carpeta **Avanzado**).

Si no tiene permiso de lectura en el área de derechos **Objetos eliminados**, se mostrará una lista vacía en la carpeta **Objetos eliminados**.

El espacio de trabajo de la carpeta **Objetos eliminados** contiene la siguiente información sobre los objetos eliminados:

- **Nombre**. Nombre del objeto.
- **Tipo**. Tipo de objeto, como directiva, tarea o paquete de instalación.
- **Hora**. Hora a la que se eliminó el objeto.
- **Usuario**. Nombre de cuenta del usuario que eliminó el objeto.

Para ver más información sobre un objeto:

1. En el árbol de la consola, seleccione **Objetos eliminados** (de forma predeterminada, **Objetos eliminados** es una subcarpeta de la carpeta **Avanzado**).

2. En el espacio de trabajo **Objetos eliminados**, seleccione el objeto que desee.

   El cuadro para trabajar con el objeto seleccionado aparece en el lado derecho del espacio de trabajo.

3. Realice una de las siguientes acciones:

   - Haga clic en el enlace **Propiedades** en el cuadro.
   - Haga clic con el botón derecho en el objeto que seleccionó en el espacio de trabajo y, en el menú contextual, seleccione **Propiedades**.

   Se abre la ventana de propiedades del objeto, que muestra las siguientes fichas:

   - **General**
   - Historial de revisiones

Eliminar objetos permanentemente de la lista de objetos eliminados

Solo los usuarios con permiso **Modificar** en el área de derechos **Objetos eliminados** pueden eliminar objetos permanentemente de la lista de objetos eliminados (consulte Asignación de permisos a usuarios y grupos para obtener más información).

Para eliminar objetos de la lista de objetos eliminados:

1. En el árbol de la consola, seleccione el nodo del Servidor de administración necesario y después seleccione la carpeta **Objetos eliminados**.
2. En el espacio de trabajo, seleccione los objetos que desea eliminar.
3. Realice una de las siguientes acciones:

   - Pulse la tecla **SUPRIMIR**.
   - En el menú contextual de los objetos que seleccionó, seleccione **Eliminar**.

4. En la ventana de diálogo de confirmación, haga clic en **Sí**.

   El objeto se elimina permanentemente de la lista de objetos eliminados. Toda la información sobre este objeto (incluidas todas sus revisiones) se elimina permanentemente de la base de datos. No se puede restaurar esta información.

Administración de dispositivos móviles

La administración de la protección de dispositivos móviles a través de Kaspersky Security Center se realiza mediante la función de administración de dispositivos móviles, que requiere una licencia dedicada. Si tiene la intención de administrar dispositivos móviles que son propiedad de los empleados de su organización, debe habilitar la Administración de dispositivos móviles.

Esta sección proporciona instrucciones para activar, configurar y desactivar la administración de dispositivos móviles. Esta sección también describe cómo administrar dispositivos móviles conectados al Servidor de administración.

Para obtener los detalles sobre Kaspersky Security para dispositivos móviles, consulte la *Ayuda de Kaspersky Security para dispositivos móviles*.

Escenario de despliegue de administración de dispositivos móviles

Esta sección proporciona un escenario para configurar la función Administración de dispositivos móviles en Kaspersky Security Center.

Requisitos previos

Asegúrese de tener una licencia que le dé acceso a la función Administración de dispositivos móviles.

Etapas

El despliegue de la función de Administración de dispositivos móviles se realiza en etapas:

1. **Preparación de los puertos**

   Asegúrese de que el puerto 13292 esté disponible en el Servidor de administración. Este puerto se requiere para conectar dispositivos móviles. Además, es posible que desee que el puerto 17100 esté disponible. Este puerto solo es necesario para el servidor proxy de activación para dispositivos móviles administrados. Si los dispositivos móviles administrados tienen acceso a Internet, no tiene que hacer que este puerto esté disponible.

2. **Activar Administración de dispositivos móviles**

   Puede habilitar la Administración de dispositivos móviles cuando ejecute el Asistente de inicio rápido del Servidor de administración o después.

3. **Especificación de la dirección externa del Servidor de administración**

   Puede especificar la dirección externa cuando ejecute el Asistente de inicio rápido del Servidor de administración o más tarde. Si no seleccionó Administración de dispositivos móviles para la instalación y no especificó la dirección en el Asistente de instalación, especifique la dirección externa en las propiedades del paquete de instalación.

4. **Asignar los dispositivos móviles al grupo de dispositivos administrados**

   Añada los dispositivos móviles al grupo de dispositivos administrados para poder administrar estos dispositivos mediante directivas. Puede crear una regla móvil en uno de los pasos del Asistente de inicio rápido del Servidor de administración. También puede crear la regla de movimiento más tarde. Si no crea una regla de este tipo, puede agregar dispositivos móviles al grupo de dispositivos administrados manualmente.

   Puede agregar dispositivos móviles al grupo de dispositivos administrados directamente o puede crear un subgrupo (o varios subgrupos) para ellos.

   En cualquier momento posterior, puede conectar cualquier dispositivo móvil nuevo al Servidor de administración mediante el Asistente para conectar un nuevo dispositivo móvil.

5. **Creación de directiva para dispositivos móviles**

   Para administrar dispositivos móviles, cree una directiva (o varias directivas) para ellos en los grupos a los que pertenecen. Puede cambiar la configuración de esta directiva en cualquier momento después.

Resultados

Después de completar estos pasos, puede administrar dispositivos móviles Android e iOS utilizando Kaspersky Security Center. Usted puede trabajar con certificados de dispositivos móviles y enviar comandos a dispositivos móviles.

Sobre una directiva de grupo para administrar dispositivos iOS con MDM y EAS

Para administrar dispositivos con EAS y con MDM para iOS, puede usar el complemento de administración de Kaspersky Device Management para iOS, que se incluye en el kit de distribución de Kaspersky Security Center. Kaspersky Device Management para iOS le permite crear directivas de grupo para especificar los ajustes de configuración de dispositivos EAS y MDM con iOS sin usar la Utilidad de configuración del iPhone® y el perfil de administración de Exchange ActiveSync.

Una directiva de grupo para administrar dispositivos iOS con MSM y EAS le brinda al administrador las siguientes opciones:

- Para administrar dispositivos EAS:
  - Configurar la contraseña de desbloqueo de los dispositivos.
  - Configurar el almacenamiento de datos cifrados de los dispositivos.
  - Configurar sincronización del correo corporativo.
  - Configurar las funciones de hardware de los dispositivos móviles, como el uso de unidades extraíbles, de la cámara o de Bluetooth.
  - Configurar las restricciones de uso de las aplicaciones móviles de los dispositivos.
- Para administrar dispositivos iOS con MDM:
  - Configurar la seguridad de contraseñas de los dispositivos.
  - Configurar las restricciones de uso de las funciones de hardware del dispositivo, y las restricciones de instalación y eliminación de apps.
  - Configurar las restricciones de uso de aplicaciones móviles preinstaladas, como YouTube™, iTunes® Store o Safari.
  - Configurar las restricciones de los contenidos multimedia que se ven (por ejemplo, películas y programas de TV) en función de la región en la que se encuentren los dispositivos.
  - Configurar la conexión del dispositivo a Internet mediante servidores proxy (proxy HTTP global).
  - Configuración de la cuenta con la que el usuario puede acceder a apps y a servicios corporativos (Tecnología de inicio de sesión único, Single Sign On (SSO)).
  - Supervisar el uso de Internet (visitas a los sitios web) en los dispositivos móviles.
  - Configurar redes inalámbricas (Wi-Fi), puntos de acceso (APN) y redes privadas virtuales (VPN) que utilizan distintos mecanismos de autenticación y protocolos de red.
  - Configurar la conexión a dispositivos AirPlay® para la transferencia de fotos, música y vídeos.

- Configurar la conexión a impresoras AirPrint™ para imprimir documentos desde el dispositivo de forma inalámbrica.
- Configurar la sincronización con el servidor Microsoft Exchange y las cuentas de usuario para utilizar el correo electrónico corporativo en los dispositivos.
- Configurar las credenciales de usuario para que se sincronicen con el servicio de directorio LDAP.
- Configurar las credenciales de usuario para que se conecten con los servicios de CalDAV y CardDAV que conceden a los usuarios acceso a los calendarios y a las listas de contactos corporativos.
- Configurar la interfaz de iOS, como fuentes o iconos de los sitios web favoritos, en los dispositivos de los usuarios.
- Agregar nuevos certificados de seguridad a los dispositivos.
- Configurar el servidor Protocolo de inscripción de certificados simple (SCEP) para que los dispositivos obtengan automáticamente certificados de la entidad de certificación.
- Agregar configuraciones utilice en personalizadas de apps móviles.

Una directiva para administrar dispositivos iOS con MDM y EAS es especial, ya que se asigna a un grupo de administración que incluye el Servidor de MDM para iOS y el servidor de dispositivos móviles Exchange ActiveSync (denominado colectivamente "Servidores de dispositivos móviles"). Todos los parámetros especificados en esta directiva se aplican primero a los servidores de dispositivos móviles y luego a los dispositivos móviles administrados por dichos servidores. En caso de que exista una estructura jerárquica de grupos de administración, los servidores de dispositivos móviles secundarios obtienen la configuración de la directiva de los servidores de dispositivos móviles principales y los distribuyen a los dispositivos móviles.

Para obtener más datos sobre cómo usar la directiva de grupo para administrar dispositivos iOS con MDM y EAS en la Consola de administración de Kaspersky Security Center, consulte la documentación de *Kaspersky Security for Mobile*.

Activar Administración de dispositivos móviles

Para administrar dispositivos móviles, debe activar la administración de dispositivos móviles. Si no activó esta función en el Asistente de inicio rápido, puede activarla más adelante. La Administración de dispositivos móviles requiere una licencia.

La activación de la Administración de dispositivos móviles solo está disponible en el Servidor de administración principal.

Para habilitar la Administración de dispositivos móviles:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta, haga clic en el botón **Activar Administración de dispositivos móviles**. Este botón solo está disponible si no ha activado antes la **Administración de dispositivos móviles**.

   Se muestra la página **Componentes adicionales** del Asistente de inicio rápido del Servidor de administración.
3. Seleccione **Activar Administración de dispositivos móviles** para administrar dispositivos móviles.

4. En la página **Seleccione el método de activación de la aplicación**, active la aplicación usando un archivo clave o un código de activación.

   La administración de dispositivos móviles no será posible a menos que active la función Administración de dispositivos móviles.

5. En la página **Configuración del servidor proxy para obtener acceso a Internet**, seleccione la casilla de verificación **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Cuando esta casilla de verificación está seleccionada, los campos están disponibles para introducir la configuración. Especifique la configuración para la conexión con el servidor proxy.

6. En la página **Verificación de actualizaciones para complementos y paquetes de instalación**, seleccione una de las siguientes opciones:

   - **Compruebe que los complementos y los paquetes de instalación estén actualizados**

     Iniciando la comprobación del estado actualizado. Si el control detecta versiones desactualizadas de algunos complementos o paquetes de instalación, el Asistente le solicita descargar versiones actualizadas para reemplazar las desactualizadas.

   - **Omitir comprobación**

     Continuar con el trabajo sin comprobar si los complementos y los paquetes de instalación están actualizados. Puede seleccionar esta opción si, por ejemplo, no tiene acceso a Internet o si desea proceder con la versión desactualizada de la aplicación por la razón que sea.

     Omitir la comprobación de actualizaciones de complementos puede ocasionar un funcionamiento deficiente de la aplicación.

7. En la página **Últimas versiones del complemento disponibles**, descargue e instale las últimas versiones de complementos en el idioma de la versión de su aplicación. La actualización de los complementos no requiere una licencia.

   Después de instalar los complementos y paquetes, la aplicación comprueba si todos los complementos requeridos para el correcto funcionamiento de los dispositivos móviles se han instalado. Si se detectan versiones desactualizadas de algunos complementos, el Asistente le solicita que descargue las versiones actualizadas para reemplazar las desactualizadas.

8. En la página **Configuración de conexión de dispositivos móviles**, configure los puertos del Servidor de administración.

Cuando el Asistente termine, se realizarán los siguientes cambios:

- Se creará la directiva de Kaspersky Endpoint Security for Android.
- Se creará la directiva de Kaspersky Device Management for iOS.
- Los puertos se abrirán en el Servidor de administración para dispositivos móviles.

Modificación de la configuración de la Administración de dispositivos móviles

Para activar la compatibilidad con dispositivos móviles:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta, haga clic en el enlace **Puertos de conexión para dispositivos móviles**.

   Se muestra la sección **Puertos adicionales** de la ventana de propiedades del Servidor de administración.
3. En la sección **Puertos adicionales**, modifique la configuración relevante:

   - **Puerto SSL para el servidor proxy de activación**

     Número de un puerto SSL para conectar Kaspersky Endpoint Security para Windows a los servidores de activación de Kaspersky.

     El número de puerto predeterminado es el 17000.

   - **Abrir puerto para dispositivos móviles**

     Se abre un puerto para que los dispositivos móviles se conecten al Servidor de licencias. Puede definir el número de puerto y otra configuración en los campos a continuación.

     Esta opción está activada de forma predeterminada.

   - **Puerto para la sincronización de dispositivos móviles**

     El número del puerto a través del cual los dispositivos móviles se conectarán al Servidor de administración e intercambiarán datos con él. El número de puerto predeterminado es el 13292.

     Puede asignar un puerto diferente si el puerto 13292 se está utilizando para otros fines.

   - **Puerto para la activación de dispositivos móviles**

     Puerto para conectar Kaspersky Endpoint Security for Android a los servidores de activación de Kaspersky.

     El número de puerto predeterminado es el 17100.
4. Haga clic en **Aceptar**.

Desactivar Administración de dispositivos móviles

La desactivación de la Administración de dispositivos móviles solo está disponible en el Servidor de administración principal.

Para desactivar la Administración de dispositivos móviles:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de esta carpeta, haga clic en el enlace **Configurar componentes adicionales**.

   Se muestra la página **Componentes adicionales** del Asistente de inicio rápido del Servidor de administración.

3. Seleccione **No activar Administración de dispositivos móviles** si ya no desea administrar dispositivos móviles.

4. Haga clic en **Aceptar**.

Los dispositivos móviles anteriormente conectados no se podrán conectar al Servidor de administración. El puerto para la conexión con el dispositivo móvil y el puerto para la activación del dispositivo móvil se cerrarán automáticamente.

Las directivas que se crearon para Kaspersky Endpoint Security for Android y Kaspersky Device Management for iOS no se eliminaron. Las reglas de emisión de certificados no se modificarán. Los complementos que se instalaron no se eliminarán. La regla de movimiento de dispositivos móviles no se eliminará.

Después de que vuelve a activar la Administración de dispositivos móviles administrados, puede que deba volver a instalar aplicaciones móviles que se requieran para la administración de dispositivos móviles.

Uso de comandos para dispositivos móviles

Esta sección brinda información sobre los comandos para la administración de dispositivos móviles que admite la aplicación. Aquí se incluyen instrucciones acerca de cómo enviar comandos a dispositivos móviles y cómo consultar los estados de ejecución de comandos en el registro de comandos.

Comandos para la administración de dispositivos móviles

Kaspersky Security Center admite comandos para la administración de dispositivos móviles.

Tales comandos se utilizan para la administración remota de dispositivos móviles. Por ejemplo, si su dispositivo móvil se pierde, puede eliminar los datos corporativos del dispositivo mediante un comando.

Puede utilizar comandos con los siguientes tipos de dispositivos móviles administrados:

- Dispositivos MDM de iOS.
- Dispositivos con Kaspersky Endpoint Security (KES).
- Dispositivos EAS.

Cada tipo de dispositivo admite un conjunto de comandos concreto.

Consideraciones especiales para ciertos comandos

- Si se ejecuta correctamente el comando **Restablecer ajustes de fábrica** en cualquier tipo de dispositivo, se eliminarán todos los datos del dispositivo y se restaurarán los valores de configuración predeterminados.
- Cuando se ejecuta correctamente el comando **Eliminar datos corporativos** en un dispositivo móvil MDM con iOS, se quitan del dispositivo móvil todos los perfiles de configuración y de aprovisionamiento, el perfil de MDM para iOS y las aplicaciones cuyas casillas **Quitar junto con el perfil de MDM para iOS** se hayan seleccionado.

- Si se ejecuta correctamente el comando **Eliminar datos corporativos** en un dispositivo KES, se eliminarán todos los datos corporativos del dispositivo, como las entradas de contactos, el historial de SMS, el registro de llamadas, los datos del calendario, la configuración de conexión a Internet y las cuentas de usuario (excepto la cuenta de Google™). En el caso de un dispositivo KES, también se eliminarán todos los datos de la tarjeta de memoria.

- Antes de enviar el comando **Localizar** a un dispositivo KES, tendrá que confirmar que está usando este comando para una búsqueda autorizada de un dispositivo perdido que pertenece a su organización o a uno de sus empleados. Al usar el Kaspersky Security Center Service Pack 2 Maintenance Release 1 o versiones anteriores, un dispositivo móvil que recibe el comando **Localizar** se bloquea. Desde el inicio de Kaspersky Security Center 10 Service Pack 3, el dispositivo no se bloquea.

Lista de comandos para dispositivos móviles

En la siguiente tabla se muestran los conjuntos de comandos para dispositivos MDM con iOS.

Comandos compatibles para la administración de dispositivos móviles: dispositivo MDM con iOS.

Comandos	Resultado de la ejecución del comando
Bloquear	El dispositivo móvil se bloquea.
Desbloquear	Se deshabilita el bloqueo del dispositivo móvil mediante un código PIN. Se restablece el código PIN especificado previamente.
Restablecer ajustes de fábrica	Se eliminan todos los datos del dispositivo móvil y la configuración se restaura a los valores predeterminados.
Eliminar datos corporativos	Se quitan del dispositivo todos los perfiles de configuración y de aprovisionamiento, el perfil de MDM para iOS y las aplicaciones que se hayan instalado cuyas casillas de verificación **Quitar junto con el perfil de MDM para iOS** se hayan seleccionado.
Sincronizar dispositivo	Los datos del dispositivo móvil se sincronizan con el Servidor de administración.
Instalar perfil	Se instala el perfil de configuración en el dispositivo móvil.
Eliminar perfil	Se elimina el perfil de configuración del dispositivo móvil.
Instalar perfil de aprovisionamiento	Se instala el perfil de aprovisionamiento en el dispositivo móvil.
Eliminar perfil de aprovisionamiento	Se elimina el perfil de aprovisionamiento del dispositivo móvil.
Instalar app	La aplicación se instala en el dispositivo móvil.
Eliminar app	La aplicación se elimina del dispositivo móvil.
Introducir código de recuperación	Se introduce el código de recuperación para una aplicación de pago.
Configurar itinerancia	Se habilita o se deshabilita la itinerancia de datos y voz.

En la siguiente tabla se muestran los conjuntos de comandos para dispositivos KES.

Comandos compatibles para la administración de dispositivos móviles: dispositivos KES

Comando	Resultado de la ejecución del comando
Bloquear	El dispositivo móvil se bloquea.
Desbloquear	Se deshabilita el bloqueo del dispositivo móvil mediante un código PIN. Se restablece el código PIN especificado previamente.

Restablecer ajustes de fábrica	Se eliminan todos los datos del dispositivo móvil y la configuración se restaura a los valores predeterminados.
Eliminar datos corporativos	Se eliminan los datos corporativos, las entradas de Contactos, el historial de SMS, el registro de llamadas, el calendario, la configuración de conexión a Internet y las cuentas de usuario (excepto la cuenta de Google). Se borran los datos de la tarjeta de memoria.
Sincronizar dispositivo	Los datos del dispositivo móvil se sincronizan con el Servidor de administración.
Localizar dispositivo	Se localiza el dispositivo móvil y se muestra en Google Maps™. Los operadores de telefonía móvil cobran por enviar SMS y proporcionar conexión a Internet.
Foto de identificación	El dispositivo móvil se bloquea. Se hace una foto con la cámara delantera del dispositivo y se guarda en el Servidor de administración. Estas fotos se pueden ver en el registro de comandos. Los operadores de telefonía móvil cobran por enviar SMS y proporcionar conexión a Internet.
Alarma	El dispositivo móvil hace sonar una alarma.

En la siguiente tabla se muestran los comandos para dispositivos EAS.

Comandos compatibles para la administración de dispositivos móviles: dispositivos EAS

Comandos	Resultado de la ejecución del comando
Restablecer ajustes de fábrica	Se eliminan todos los datos del dispositivo móvil y la configuración se restaura a los valores predeterminados.

Uso de Google Cloud Firebase Messaging

Para garantizar que los comandos se envían puntualmente a los dispositivos KES administrados por el sistema operativo Android, Kaspersky Security Center utiliza las notificaciones de inserción. Las notificaciones de inserción se envían entre los dispositivos KES y el Servidor de administración mediante Google Firebase Cloud Messaging. En la Consola de administración de Kaspersky Security Center, puede especificar la configuración de Google Firebase Cloud Messaging para conectar dispositivos KES al servicio.

Para obtener la configuración de Google Cloud Firebase Messaging, debes disponer de una cuenta de Google.

Configurar Google Firebase Cloud Messaging:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.

   Se abre la ventana de propiedades de la carpeta **Dispositivos móviles**.
3. Seleccione la sección de **Configuración de Google Firebase Cloud Messaging**.
4. En el campo **ID de remitente**, indique el número de un proyecto de la API de Google que haya recibido al crear uno en la consola para desarrolladores de Google.
5. En el campo **Clave de servidor**, introduzca una clave de servidor común que haya creado en la consola para desarrolladores de Google.

En la siguiente sincronización con el Servidor de administración, los dispositivos KES administrados por sistemas operativos Android se conectarán a Google Firebase Cloud Messaging.

Puede editar la configuración de Google Firebase Cloud Messaging haciendo clic en el botón **Restablecer configuración**.

Enviar comandos

Para enviar un comando al dispositivo móvil de un usuario, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. Seleccione el dispositivo móvil del usuario al que desea enviar un comando.

3. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

4. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección con el nombre del comando que desee enviar al dispositivo móvil y haga clic en el botón **Enviar comando**.

   Dependiendo del comando que haya seleccionado, puede que al hacer clic en el botón **Enviar comando** se abra la ventana de configuración avanzada de la aplicación. Por ejemplo, cuando envía el comando para eliminar un perfil de aprovisionamiento de un dispositivo móvil, la aplicación le solicita que seleccione el perfil que se debe eliminar del dispositivo móvil. Defina la configuración avanzada del comando en esa ventana y confirme la selección. A continuación, se enviará el comando al dispositivo móvil.

   Haga clic en el botón **Reenviar** para volver a enviar el comando al dispositivo móvil del usuario.

   Haga clic en el botón **Quitar de la cola** para cancelar la ejecución de un comando enviado que todavía no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con sus respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

5. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

Visualización de estados de comandos en el registro de comandos

La aplicación guarda en el registro de comandos información sobre todos los comandos que se hayan enviado a los dispositivos móviles. El registro de comandos incluye información acerca de la hora y la fecha a las que se envió cada comando al dispositivo móvil y de sus estados, además de descripciones detalladas de los resultados de la ejecución de los comandos. Por ejemplo, en caso de que no se pueda ejecutar un comando, el registro muestra la causa del error. Los registros se guardan en el registro de comandos durante un máximo de 30 días.

Los comandos que se envían a los dispositivos móviles pueden tener los estados siguientes:

- *En ejecución*: El comando se ha enviado al dispositivo móvil.
- *Completado*: La ejecución del comando ha finalizado correctamente.
- *Completado con errores*: Se ha producido un error en la ejecución del comando.
- *Borrando*: se está quitando el comando de la cola de comandos enviados al dispositivo móvil.

- *Eliminado*: Se ha quitado el comando de la cola de comandos enviados al dispositivo móvil.
- *Error al eliminar*: el comando no se pudo quitar de la cola de comandos enviados al dispositivo móvil.

La aplicación lleva un registro de comandos de cada dispositivo móvil.

Para ver el registro de comandos enviados a un dispositivo móvil, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En la lista de dispositivos móviles, seleccione aquel cuyo registro de comandos desee ver.

3. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

   Se abre la ventana **Comandos para la administración de dispositivos móviles**. Las secciones de la ventana **Comandos para la administración de dispositivos móviles** corresponden a los comandos que se pueden enviar al dispositivo móvil.

4. Seleccione las secciones que contengan los comandos necesarios y consulte la información sobre el envío y la ejecución de comandos en la sección **Registro de comandos**.

En la sección **Registro de comandos**, puede consultar la lista de comandos que se han enviado al dispositivo móvil e información sobre esos comandos. El filtro **Mostrar comandos** permite mostrar en la lista solo comandos con el estado seleccionado.

Trabajar con certificados de dispositivos móviles

Esta sección contiene información sobre cómo trabajar con certificados de dispositivos móviles. Aquí se proporcionan instrucciones sobre cómo instalar certificados en los dispositivos móviles de los usuarios y cómo configurar reglas de emisión de certificados. También se incluyen instrucciones acerca de cómo integrar la aplicación con la infraestructura de claves públicas y cómo configurar el soporte de Kerberos.

Inicio del Asistente de instalación de certificados.

Puede instalar los siguientes tipos de certificados en el dispositivo móvil de un usuario:

- Certificados compartidos para identificar el dispositivo móvil
- Certificados de correo para configurar el correo corporativo en el dispositivo móvil
- Certificado de VPN para configurar el acceso a una red privada virtual en el dispositivo móvil

Para instalar un certificado en el dispositivo móvil de un usuario, siga estos pasos:

1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.

2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el enlace **Agregar certificado** para ejecutar el Asistente de instalación de certificados.

Siga las instrucciones del Asistente.

Cuando el Asistente finalice, se creará un certificado y se agregará a la lista de certificados del usuario. Además, se enviará una notificación al usuario con un enlace para descargar e instalar el certificado en el dispositivo móvil. Puede ver la lista de todos los certificados y exportarla a un archivo. Puede eliminar y volver a emitir certificados, así como ver sus propiedades.

Paso 1: Selección del tipo de certificado

Especifique el tipo de certificado que debe instalarse en el dispositivo móvil del usuario:

- **Certificado móvil**: para identificar el dispositivo móvil.
- **Certificado de correo**: para configurar el correo corporativo en el dispositivo móvil.
- **Certificado de VPN**: para configurar el acceso a una red privada virtual en el dispositivo móvil.

Paso 2: Selección del tipo de dispositivos

Esta ventana se muestra solo si seleccionó **Certificado de correo** o **Certificado de VPN** como el tipo de certificado.

Especifique el tipo de sistema operativo del dispositivo:

- **Dispositivo MDM con iOS**. Seleccione esta opción si tiene que instalar un certificado en un dispositivo móvil que está conectado al servidor de MDM para iOS utilizando el protocolo MDM de iOS.
- **Dispositivo KES administrado por Kaspersky Security para dispositivos móviles**. Seleccione esta opción si tiene que instalar un certificado en un dispositivo KES. En este caso, el certificado se usará para la identificación del usuario en cada conexión al Servidor de administración.
- **Dispositivo KES conectado al Servidor de administración sin autenticación del certificado de usuario**. Seleccione esta opción si tiene que instalar un certificado en un dispositivo KES sin usar una autenticación del certificado. En este caso, en el paso final del Asistente, en la ventana **Método de notificación del usuario**, el administrador debe seleccionar el tipo de autenticación de usuario utilizado en cada conexión con el Servidor de administración.

Paso 3. Selección de un usuario

En la lista, seleccione usuarios, grupos de usuarios o grupos de usuarios de Active Directory para los cuales debe instalar el certificado.

En la ventana **Selección del usuario**, puede buscar los usuarios internos de Kaspersky Security Center. Puede hacer clic en **Agregar** para añadir a un usuario interno.

Paso 4. Selección del origen del certificado

En esta ventana puede seleccionar el origen de los certificados que el Servidor de administración usará para identificar el dispositivo móvil. Puede especificar un certificado usando uno de los siguientes métodos:

- Crear un certificado automáticamente (con las herramientas del Servidor de administración) y luego entregarlo al dispositivo.
- Especifique un archivo de certificado creado anteriormente. Este método no está disponible si se seleccionó varios usuarios en el paso anterior.

Seleccione la casilla **Publicar certificado** si debe enviar a un usuario una notificación sobre la creación de un certificado para su dispositivo móvil.

Si el dispositivo móvil del usuario ya se ha autenticado previamente con un certificado y no es necesario especificar un nombre de cuenta y una contraseña para recibir un certificado nuevo, desmarque la casilla **Publicar certificado**. En este caso, la ventana **Método de notificación del usuario** no se mostrará.

Paso 5. Asignación de una etiqueta al certificado

La ventana **Etiqueta del certificado** se muestra si **Dispositivo MDM con iOS** ha sido seleccionado en el **Tipo de dispositivo**.

En la lista desplegable, puede asignar una etiqueta al certificado del dispositivo MDM con iOS del usuario. El certificado con la etiqueta asignada puede tener parámetros específicos establecidos para esta etiqueta en las propiedades de la directiva de Kaspersky Device Management for iOS.

La lista desplegable le solicita que seleccione la etiqueta *Plantilla de certificados 1*, *Plantilla de certificados 2* o *Plantilla de certificados 3*. Puede configurar las etiquetas en las siguientes secciones:

- Si se ha seleccionado **Certificado de correo** en la ventana **Tipo de certificado**, las etiquetas se pueden configurar en las propiedades de la cuenta de Exchange ActiveSync para dispositivos móviles (**Dispositivos administrados** → **Directivas** → Propiedades de la directiva de Kaspersky Device Management for iOS → sección **Exchange ActiveSync** → **Agregar** → **Avanzado**).
- Si se ha seleccionado **Certificado de VPN** en la ventana **Tipo de certificado**, las etiquetas se pueden configurar en las propiedades de VPN para dispositivos móviles (**Dispositivos administrados** → **Directivas** → Propiedades de la directiva de Kaspersky Device Management for iOS → sección **VPN** → **Agregar** → **Avanzado**). No puede configurar las etiquetas utilizadas para los certificados de VPN si selecciona el tipo de conexión L2TP, PPTP o IPSec (Cisco™) para su VPN.

Paso 6. Especificación de la configuración de publicación de certificados

En esta ventana, puede especificar la siguiente configuración de publicación de certificados:

- No notificar al usuario acerca de la existencia de un nuevo certificado

Active esta opción si no desea enviar a un usuario una notificación de la creación de un certificado para el dispositivo móvil del usuario. En este caso, la ventana **Método de notificación del usuario** no se mostrará.

Esta opción solo se aplica a dispositivos con Kaspersky Endpoint Security for Android instalado.

Es posible que desee activar esta opción, por ejemplo, si el dispositivo móvil del usuario ya se ha autenticado previamente mediante un certificado, por lo que no es necesario especificar un nombre de cuenta y una contraseña para recibir un nuevo certificado.

- **Permitir que el dispositivo reciba varias veces el mismo certificado (solo para dispositivos con Kaspersky Endpoint Security for Android instalado)**

  Active esta opción si desea que Kaspersky Security Center reenvíe automáticamente el certificado cada vez que caduque o cuando no se encuentre en el dispositivo de destino.

  El certificado se reenvía automáticamente varios días antes de la fecha de caducidad del certificado. Puede establecer el número de días en la ventana Reglas de emisión de certificados.

  En algunos casos, el certificado no se puede encontrar en el dispositivo. Por ejemplo, esto puede pasar cuando el usuario instala de nuevo la aplicación de seguridad del Laboratorio Kaspersky en el dispositivo o reinicializa la configuración del dispositivo y datos a faltas de la fábrica. En este caso, Kaspersky Security Center verifica la identificación del dispositivo en el siguiente intento del dispositivo para conectarse al Servidor de administración. Si el dispositivo tiene el mismo Id. que tenía cuando se emitió el certificado, la aplicación reenvía el certificado al dispositivo.

Paso 7. Selección del método de notificación del usuario

Esta ventana no se muestra si seleccionó **Dispositivo MDM con iOS** como el tipo de dispositivo o si seleccionó la opción **No notificar al usuario acerca de la existencia de un nuevo certificado**.

En la ventana **Método de notificación del usuario**, puede configurar la notificación que recibe el usuario sobre la instalación del certificado en el dispositivo móvil.

En el campo **Método de autenticación**, especifique el tipo de autenticación de usuario:

- **Credenciales (dominio o alias)**

  En este caso, el usuario emplea la contraseña de dominio o la contraseña de un usuario interno de Kaspersky Security Center para recibir un nuevo certificado.

- **Contraseña de un solo uso**

En este caso, el usuario recibe una contraseña de un solo uso que se enviará por correo electrónico o por SMS. Esta contraseña debe introducirse para recibir un nuevo certificado.

Esta opción cambia a **Contraseña** si activó (seleccionó) la opción **Permitir que el dispositivo reciba múltiples recibos de un solo certificado (solo para dispositivos con aplicaciones de seguridad Kaspersky para dispositivos móviles instalados)** en la ventana de **Configuración de publicación de certificados**.

- Contraseña

  En este caso, la contraseña se utiliza cada vez que el certificado se envía al usuario.

  Esta opción cambia a **Contraseña de un solo uso** si desactivó (deshabilitó) la opción **Permitir que el dispositivo reciba múltiples recibos de un solo certificado (solo para dispositivos con aplicaciones de seguridad Kaspersky para dispositivos móviles instalados)** en la ventana de **Configuración de publicación de certificados**.

Este campo se muestra si seleccionó **Certificado móvil** en la ventana **Tipo de certificado** o si seleccionó **Dispositivo KES conectado al Servidor de administración sin autenticación del certificado de usuario** como tipo de dispositivo.

Seleccione la opción de notificación de usuario:

- Mostrar la contraseña de autenticación cuando el Asistente finalice

  Si selecciona esta opción, el nombre de usuario, el nombre de usuario en el Administrador de cuentas de seguridad (SAM) y la contraseña para la recuperación de certificados para cada uno de los usuarios seleccionados se mostrarán en el paso final del Asistente de instalación de certificados. La configuración de la notificación que recibe el usuario sobre la instalación de certificados no estará disponible.

  Cuando añade certificados para varios usuarios, puede guardar las credenciales proporcionadas en un archivo haciendo clic en el botón **Exportar** en el último paso del Asistente de instalación de certificados.

  Esta opción no está disponible si seleccionó **Credenciales (dominio o alias)** en el paso del **Método de notificación del usuario** del Asistente de instalación de certificados.

- Notificar al usuario de la existencia de un nuevo certificado

  Si selecciona esta opción, puede configurar la notificación que recibe el usuario sobre un nuevo certificado.

  - Por correo electrónico

    En este grupo de configuración Por correo electrónico, puede configurar notificaciones de usuario sobre la instalación de un nuevo certificado en su dispositivo móvil mediante mensajes de correo electrónico. Este método de notificación solo está disponible si el servidor SMTP está activado.

    Haga clic en el enlace **Editar mensaje** para ver y editar el mensaje de notificación, si es necesario.

  - Por SMS

En este grupo de configuraciones, puede configurar la notificación del usuario sobre el uso de SMS para instalar un certificado en dispositivos móviles. Este método de notificación solo está disponible si la opción Notificación por SMS está activada.

Haga clic en el enlace **Editar mensaje** para ver y editar el mensaje de notificación, si es necesario.

Paso 8. Generación del certificado

En este paso, se crea el certificado.

Puede hacer clic en **Finalizar** para salir del Asistente.

El certificado se genera y se muestra en la lista de certificados en el espacio de trabajo de la carpeta **Certificados**.

Configurar reglas de emisión de certificados

Los certificados se utilizan para la autenticación del dispositivo en el Servidor de administración. Todos los dispositivos móviles administrados deben tener certificados. Puede configurar cómo se emiten los certificados.

Para configurar reglas de emisión de certificados, siga estos pasos:

1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el botón **Configurar reglas de emisión de certificados** para abrir la ventana **Reglas de emisión de certificados**.
3. Vaya a la sección con el nombre de un tipo de certificado:

   Emisión de certificados móviles: Para configurar la emisión de certificados para los dispositivos móviles.

   Emisión de certificados de correo: Para configurar la emisión de certificados de correo.

   Emisión de certificados de VPN: Para configurar la emisión de certificados de VPN.
4. En la sección **Configuración de emisión**, configure la emisión del certificado:

   - Especifique el término del certificado en días.
   - Seleccione una fuente de certificado (**Servidor de administración** o **Los certificados se especifican de forma manual**).

     Se selecciona el Servidor de administración como fuente de certificados predeterminada.
   - Especifique una plantilla de certificado (**Plantilla predeterminada**, **Otra plantilla**).

     La configuración de plantillas está disponible si la sección **Integración con la PKI** presenta la integración con la infraestructura de clave pública activada.
5. En la sección **Configuración de las actualizaciones automáticas**, configure las actualizaciones automáticas del certificado:

   - En el campo **Renovar el certificado cuando para que caduque falten (días)**, especifique cuántos días antes del vencimiento se debe renovar el certificado.

- Para habilitar las actualizaciones automáticas de certificados, seleccione la casilla de verificación **Reemitir el certificado automáticamente siempre que sea posible**.

Solo se pueden renovar manualmente los certificados móviles.

6. En la sección **Protección de contraseñas**, active y configure el uso de una contraseña al descifrar certificados.

   La protección de contraseñas solo está disponible para certificados generales.

   a. Selecciona la casilla de verificación **Solicitar contraseña durante la instalación del certificado**.

   b. Utilice el control deslizante para definir la cantidad máxima de símbolos de la contraseña de cifrado.

7. Haga clic en **Aceptar**.

Integración con la infraestructura de clave pública

Se requiere integrar la aplicación con la infraestructura de clave pública (PKI, por sus siglas en inglés) para simplificar la emisión de certificados de dominio para los usuarios. Una vez hecho esto, los certificados se emiten automáticamente.

La versión del servidor de PKI mínima admitida es Windows Server 2008.

Debe configurar la cuenta para que se integre con la PKI. La cuenta debe cumplir estos requisitos:

- Ser un usuario de dominio y administrador en un dispositivo con el Servidor de administración instalado.
- Tener el privilegio SeServiceLogonRight en el dispositivo con el Servidor de administración instalado.

Para crear un perfil de usuario permanente, inicie sesión al menos una vez con la cuenta de usuario configurada en el dispositivo en el que se aloja el Servidor de administración. En el repositorio de certificados de este usuario en el Servidor de administración, instale el certificado de agente de inscripción que le han facilitado los administradores del dominio.

Para configurar la integración con la infraestructura de claves públicas, siga estos pasos:

1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
2. En el espacio de trabajo, haga clic en el botón **Integrar con la infraestructura de clave pública** para abrir la sección **Integración con la PKI** de la ventana **Reglas de emisión de certificados**.

   La sección **Integración con la PKI** de la ventana **Reglas de emisión de certificados** se abre.
3. Selecciona la casilla de verificación **Integrar emisión de certificados con PKI**.
4. En el campo **Cuenta**, indique el nombre de la cuenta de usuario que se utilizará para integrarse con la infraestructura de clave pública.
5. En el campo **Contraseña**, introduzca la contraseña de dominio de la cuenta.

6. En la lista **El nombre de la plantilla de certificados del sistema de la PKI**, seleccione la plantilla del certificado que se utilizará para la emisión de certificados para usuarios de dominio.

   Se inicia un servicio específico en Kaspersky Security Center con la cuenta de usuario especificada. Este servicio es responsable de emitir los certificados de dominio de los usuarios. El servicio se inicia cuando se carga la lista de plantillas de certificados haciendo clic en el botón **Actualizar lista** o cuando se genera un certificado.

7. Haga clic en **Aceptar** para guardar la configuración.

Una vez hecho esto, los certificados se emiten automáticamente.

Habilitación del soporte de Kerberos Constrained Delegation

La aplicación admite el uso de Kerberos Constrained Delegation.

Para habilitarlo, siga estos pasos:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles**.
2. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.
3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.
4. En el menú contextual del servidor de MDM para iOS, seleccione **Propiedades**.
5. En la ventana de propiedades del servidor de MDM para iOS, seleccione la sección **Configuración**.
6. En la sección **Configuración**, seleccione la casilla de verificación **Garantizar la compatibilidad con la delegación limitada de Kerberos**.
7. Haga clic en **Aceptar**.

Adición de dispositivos móviles iOS a la lista de dispositivos administrados

Para añadir un dispositivo móvil iOS a la lista de dispositivos administrados, debe entregarse e instalarse un certificado compartido en el dispositivo. Los certificados compartidos se utilizan para identificar dispositivos móviles mediante el Servidor de administración. El certificado compartido para un dispositivo móvil iOS se entrega dentro de un perfil de MDM para iOS. Una vez que se entrega e instala un certificado compartido en un dispositivo móvil, este aparece en la lista de dispositivos administrados.

Kaspersky ya no admite Kaspersky Safe Browser.

Puede añadir dispositivos móviles de usuarios a la lista de dispositivos administrados mediante el Asistente para conectar un nuevo dispositivo móvil.

Para conectar un dispositivo iOS al Servidor de administración mediante un certificado compartido, haga lo siguiente:

1. Inicie el Asistente para conectar un nuevo dispositivo móvil de una de las siguientes maneras:

   - Utilice el menú contextual en la carpeta **Cuentas de usuario**:

     1. En el árbol de consola, expanda la carpeta **Avanzado** y seleccione la subcarpeta **Cuentas de usuario**.

     2. En el espacio de trabajo de la carpeta **Cuentas de usuario**, seleccione a los usuarios, grupos de usuarios o grupos de usuarios de Active Directory cuyos dispositivos móviles desea añadir a la lista de dispositivos administrados.

     3. Haga clic con el botón derecho y, en el menú contextual de la cuenta de usuario, seleccione **Agregar dispositivo móvil**.

        El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse.

   - En el espacio de trabajo de la carpeta **Dispositivos móviles**, haga clic en el botón **Agregar dispositivo móvil**:

     1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Dispositivos móviles**.

     2. En el espacio de trabajo de la subcarpeta **Dispositivos móviles**, haga clic en el botón **Agregar dispositivo móvil**.

        El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse.

2. En la página **Sistema operativo** del Asistente, seleccione **iOS** como el tipo de sistema operativo del dispositivo móvil.

3. En la página **Selección de un servidor de MDM para iOS**, seleccione el Servidor de MDM para iOS.

4. En la página **Seleccionar usuarios cuyos dispositivos móviles quiera administrar**, seleccione a los usuarios, grupos de usuarios o grupos de usuarios de Active Directory cuyos dispositivos móviles desea añadir a la lista de dispositivos administrados.

   > Este paso no se realiza si inicia el Asistente seleccionando **Agregar dispositivo móvil** en el menú contextual de la carpeta **Cuentas de usuario**.

   Si desea añadir una nueva cuenta de usuario a la lista, haga clic en el botón **Agregar** e introduzca las propiedades de la cuenta de usuario en la ventana que se abre. Si desea modificar o revisar las propiedades de la cuenta de usuario, seleccione la cuenta de usuario de la lista y haga clic en el botón **Propiedades**.

5. En la página del Asistente **Origen del certificado**, especifique el método de creación del certificado compartido que utilizará el Servidor de administración para identificar el dispositivo móvil. Puede especificar un certificado compartido usando uno de los siguientes métodos:

   - Emitir certificado a través de las herramientas del Servidor de administración

     > Seleccione esta opción para crear un nuevo certificado con las herramientas del Servidor de administración si todavía no lo ha creado.
     >
     > Si esta opción se selecciona, el perfil de MDM para iOS se firmará con un certificado generado automáticamente mediante el Servidor de administración.
     >
     > Esta opción está seleccionada de forma predeterminada.

   - Especificar archivo de certificado

Seleccione esta opción para especificar un archivo de certificado que ya se ha creado.

Este método no está disponible si se seleccionó varios usuarios en el paso anterior.

6. En la ventana **Método de notificación del usuario** del Asistente, defina la configuración para notificar al usuario del dispositivo móvil por SMS o correo electrónico sobre la creación del certificado:

   - Mostrar enlace en el Asistente

     Si selecciona esta opción, se mostrará un enlace al paquete de instalación en el paso final del Asistente de conexión de nuevo dispositivo.

     Este método no está disponible si se seleccionó varios usuarios en el paso anterior de conexión del dispositivo.

   - Enviar enlace al usuario

     La selección de esta opción le permite configurar la notificación del usuario de la conexión de un dispositivo móvil nuevo.

     Puede seleccionar el tipo de dirección de correo electrónico, especificar una dirección de correo electrónico adicional y modificar el texto del mensaje. También puede seleccionar el tipo de teléfono del usuario para enviar un mensaje del SMS, especificar un número de teléfono adicional y modificar el texto del mensaje del SMS.

     Si el Servidor del SMTP no se ha configurado, no se podrá enviar ningún mensaje de correo electrónico a los usuarios. Si no se configuró la notificación, no se enviará ningún mensajes SMS a los usuarios.

7. En la página **Resultado**, haga clic en **Finalizar** para cerrar el Asistente.

El perfil de MDM para iOS se publica automáticamente en el servidor web de Kaspersky Security Center. El usuario del dispositivo móvil recibe una notificación con un enlace para descargar el perfil de MDM para iOS desde el servidor web. El usuario hace clic en el enlace. A continuación, el sistema operativo del dispositivo móvil solicita al usuario que acepte la instalación del perfil de MDM para iOS. El usuario debe aceptar instalar el perfil de MDM para iOS antes de que el perfil de MDM para iOS se pueda descargar al dispositivo móvil. Cuando el perfil de MDM para iOS se haya descargado y el dispositivo móvil se haya sincronizado con el Servidor de administración, el dispositivo se mostrará en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de la consola.

Para permitir que el usuario prosiga con el servidor web de Kaspersky Security Center utilizando el enlace, la conexión con el Servidor de administración a través del puerto 8061 debe estar disponible en el dispositivo móvil.

Adición de dispositivos móviles Android a la lista de dispositivos administrados

Para añadir un dispositivo móvil Android a la lista de dispositivos administrados, Kaspersky Endpoint Security for Android y un certificado compartido se deben entregar e instalar en el dispositivo móvil. Los certificados compartidos se utilizan para identificar dispositivos móviles mediante el Servidor de administración. Una vez que se entrega e instala un certificado compartido en un dispositivo móvil, este aparece en la lista de dispositivos administrados.

Puede añadir dispositivos móviles de usuarios a la lista de dispositivos administrados mediante el Asistente para conectar un nuevo dispositivo móvil. El nuevo Asistente para conectar un nuevo dispositivo móvil proporciona dos opciones para entregar e instalar un certificado compartido y Kaspersky Endpoint Security for Android:

- Utilizando un enlace de Google Play
- Utilizando un enlace de Servidor web de Kaspersky Security Center

  El paquete de instalación de Kaspersky Endpoint Security for Android almacenado para la distribución en el Servidor de administración se utiliza para la instalación

Ejecución del Asistente para conectar un nuevo dispositivo móvil

Para iniciar el Asistente para conectar un nuevo dispositivo móvil, realice una de las siguientes acciones:

- Utilice el menú contextual en la carpeta **Cuentas de usuario**:

  1. En el árbol de consola, expanda la carpeta **Avanzado** y seleccione la subcarpeta **Cuentas de usuario**.
  2. En el espacio de trabajo de la carpeta **Cuentas de usuario**, seleccione a los usuarios, grupos de usuarios o grupos de usuarios de Active Directory cuyos dispositivos móviles desea añadir a la lista de dispositivos administrados.
  3. Haga clic con el botón derecho y, en el menú contextual de la cuenta de usuario, seleccione **Agregar dispositivo móvil**.

     El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse.

- En el espacio de trabajo de la carpeta **Dispositivos móviles**, haga clic en el botón **Agregar dispositivo móvil**:

  1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Dispositivos móviles**.
  2. En el espacio de trabajo de la subcarpeta **Dispositivos móviles**, haga clic en el botón **Agregar dispositivo móvil**.

     El Asistente para conectar un nuevo dispositivo móvil empieza a ejecutarse.

Agregar un dispositivo móvil Android utilizando el enlace de Google Play

Para instalar Kaspersky Endpoint Security for Android y un certificado compartido en un dispositivo móvil mediante un enlace de Google Play, realice lo siguiente:

1. Inicie el Asistente para conectar un nuevo dispositivo móvil.
2. En la página **Sistema operativo** del Asistente, seleccione **Android** como el tipo de sistema operativo del dispositivo móvil.
3. En la primera página del Asistente **Método de instalación de Kaspersky Endpoint Security for Android**, seleccione **Utilizando el enlace de Google Play**.

4. En la página del Asistente **Seleccionar usuarios cuyos dispositivos móviles quiera administrar**, seleccione a los usuarios, grupos de usuarios o grupos de usuarios de Active Directory cuyos dispositivos móviles desea añadir a la lista de dispositivos administrados.

   Este paso se omite si se inicia el Asistente al seleccionar **Agregar dispositivo móvil** en el menú contextual de la carpeta **Cuentas de usuario**.

   Si desea añadir una nueva cuenta de usuario a la lista, haga clic en el botón **Agregar** e introduzca las propiedades de la cuenta de usuario en la ventana que se abre. Si desea modificar o revisar las propiedades de la cuenta de usuario, seleccione la cuenta de usuario en la lista y haga clic en el botón **Propiedades**.

5. En la página del Asistente **Origen del certificado**, especifique el método de creación del certificado compartido que utilizará el Servidor de administración para identificar el dispositivo móvil. Puede especificar un certificado compartido usando uno de los siguientes métodos:

   - Emitir certificado a través de las herramientas del Servidor de administración

     Seleccione esta opción para crear un nuevo certificado con las herramientas del Servidor de administración si todavía no lo ha creado.

     Si selecciona esta opción, el certificado se emite automáticamente por medio de las herramientas del Servidor de administración.

     Esta opción está seleccionada de forma predeterminada.

   - Especificar archivo de certificado

     Seleccione esta opción para especificar un archivo de certificado que ya se ha creado.

     Este método no está disponible si se seleccionó varios usuarios en el paso anterior.

6. En la ventana **Método de notificación del usuario** del Asistente, defina la configuración para notificar al usuario del dispositivo móvil por SMS o correo electrónico sobre la creación del certificado:

   - Mostrar enlace en el Asistente

     Si selecciona esta opción, se mostrará un enlace al paquete de instalación en el paso final del Asistente de conexión de nuevo dispositivo.

     Este método no está disponible si se seleccionó varios usuarios en el paso anterior de conexión del dispositivo.

   - Enviar enlace al usuario

     La selección de esta opción le permite configurar la notificación del usuario de la conexión de un dispositivo móvil nuevo.

     Puede seleccionar el tipo de dirección de correo electrónico, especificar una dirección de correo electrónico adicional y modificar el texto del mensaje. También puede seleccionar el tipo de teléfono del usuario para enviar un mensaje del SMS, especificar un número de teléfono adicional y modificar el texto del mensaje del SMS.

     Si el Servidor del SMTP no se ha configurado, no se podrá enviar ningún mensaje de correo electrónico a los usuarios. Si no se configuró la notificación, no se enviará ningún mensajes SMS a los usuarios.

7. En la página **Resultado**, haga clic en **Finalizar** para cerrar el Asistente.

   Cuando el Asistente finalice, se enviarán un enlace y un código QR al dispositivo móvil del usuario, que le permitirán descargar Kaspersky Endpoint Security for Android. El usuario debe hacer clic en el enlace o analizar el código QR. A continuación, el sistema operativo del dispositivo móvil solicita al usuario que acepte la instalación de Kaspersky Endpoint Security for Android. Una vez descargado e instalado Kaspersky Endpoint Security for Android, el dispositivo móvil se conecta al Servidor de administración y descarga un certificado compartido. Una vez instalado el certificado en el dispositivo móvil, el dispositivo se muestra en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de consola.

Añadir un dispositivo móvil Android utilizando un enlace del servidor web de Kaspersky Security Center

Para la instalación, se utiliza el paquete de instalación de Kaspersky Endpoint Security for Android publicado en el Servidor de administración.

Para instalar Kaspersky Endpoint Security for Android y un certificado compartido en un dispositivo móvil utilizando un enlace del servidor web, realice lo siguiente:

1. Inicie el Asistente para conectar un nuevo dispositivo móvil.

2. En la página **Sistema operativo** del Asistente, seleccione **Android** como el tipo de sistema operativo del dispositivo móvil.

3. En la primera página del Asistente **Método de instalación de Kaspersky Endpoint Security for Android**, seleccione **Mediante un enlace de Servidor web**.

   En el campo que aparezca a continuación, seleccione un paquete de instalación o cree nuevo uno haciendo clic en **Nuevo**.

4. En la página del Asistente **Seleccionar usuarios cuyos dispositivos móviles quiera administrar**, seleccione a los usuarios, grupos de usuarios o grupos de usuarios de Active Directory cuyos dispositivos móviles desea añadir a la lista de dispositivos administrados.

   Este paso se omite si se inicia el Asistente al seleccionar **Agregar dispositivo móvil** en el menú contextual de la carpeta **Cuentas de usuario**.

   Si desea añadir una nueva cuenta de usuario a la lista, haga clic en el botón **Agregar** e introduzca las propiedades de la cuenta de usuario en la ventana que se abre. Si desea modificar o revisar las propiedades de la cuenta de usuario, seleccione la cuenta de usuario de la lista y haga clic en el botón **Propiedades**.

5. En la página del Asistente **Origen del certificado**, especifique el método de creación del certificado compartido que utilizará el Servidor de administración para identificar el dispositivo móvil. Puede especificar un certificado compartido usando uno de los siguientes métodos:

   - Emitir certificado a través de las herramientas del Servidor de administración

Seleccione esta opción para crear un nuevo certificado con las herramientas del Servidor de administración si todavía no lo ha creado.

Si selecciona esta opción, el certificado se emite automáticamente por medio de las herramientas del Servidor de administración.

Esta opción está seleccionada de forma predeterminada.

- **Especificar archivo de certificado**

  Seleccione esta opción para especificar un archivo de certificado que ya se ha creado.

  Este método no está disponible si se seleccionó varios usuarios en el paso anterior.

6. En la ventana **Método de notificación del usuario** del Asistente, defina la configuración para notificar al usuario del dispositivo móvil por SMS o correo electrónico sobre la creación del certificado:

   - **Mostrar enlace en el Asistente**

     Si selecciona esta opción, se mostrará un enlace al paquete de instalación en el paso final del Asistente de conexión de nuevo dispositivo.

     Este método no está disponible si se seleccionó varios usuarios en el paso anterior de conexión del dispositivo.

   - **Enviar enlace al usuario**

     La selección de esta opción le permite configurar la notificación del usuario de la conexión de un dispositivo móvil nuevo.

     Puede seleccionar el tipo de dirección de correo electrónico, especificar una dirección de correo electrónico adicional y modificar el texto del mensaje. También puede seleccionar el tipo de teléfono del usuario para enviar un mensaje del SMS, especificar un número de teléfono adicional y modificar el texto del mensaje del SMS.

     Si el Servidor del SMTP no se ha configurado, no se podrá enviar ningún mensaje de correo electrónico a los usuarios. Si no se configuró la notificación, no se enviará ningún mensajes SMS a los usuarios.

7. En la página **Resultado**, haga clic en **Finalizar** para cerrar el Asistente.

El paquete de aplicaciones móviles de Kaspersky Endpoint Security for Android se publica automáticamente en el servidor web de Kaspersky Security Center. El paquete de la aplicación móvil contiene la aplicación, la configuración para la conexión del dispositivo móvil al Servidor de administración y un certificado. El usuario del dispositivo móvil recibirá una notificación con un enlace para descargar el paquete desde el servidor web. El usuario hace clic en el enlace. A continuación, el sistema operativo del dispositivo solicita al usuario que acepte la instalación del paquete de aplicaciones móviles. Si el usuario acepta, el paquete se descargará en el dispositivo móvil. Cuando el paquete se haya descargado y el dispositivo móvil se haya sincronizado con el Servidor de administración, el dispositivo se mostrará en la carpeta **Dispositivos móviles**, que es una subcarpeta de la carpeta **Administración de dispositivos móviles** del árbol de la consola.

Administración de dispositivos móviles de Exchange ActiveSync

Esta sección describe las funciones avanzadas para la administración de dispositivos EAS con Kaspersky Security Center.

Además de la administración de dispositivos EAS mediante comandos, el administrador puede utilizar las opciones siguientes:

- Crear perfiles de administración para dispositivos EAS y asignarlos a buzones de correo de usuarios. El *Perfil de administración de dispositivo EAS* es una directiva de Exchange ActiveSync que se utiliza en un servidor Microsoft Exchange para administrar dispositivos EAS. En un perfil de administración de dispositivos EAS, puede configurar los grupos de configuración siguientes:
  - Configuración de administración de contraseñas de usuarios
  - Configuración de sincronización del correo
  - Restricciones sobre el uso de las características del dispositivo móvil
  - Restricciones sobre el uso de aplicaciones móviles en el dispositivo móvil

  Según el modelo del dispositivo móvil, los ajustes de un perfil de administración pueden aplicarse parcialmente. El estado de una directiva de Exchange ActiveSync que se ha aplicado puede verse en las propiedades del dispositivo móvil.
- Consultar información sobre la configuración de administración de dispositivos EAS. Por ejemplo, en las propiedades del dispositivo móvil, el administrador puede ver la hora de la última sincronización con un servidor Microsoft Exchange, la ID del dispositivo EAS, el nombre de la directiva de Exchange ActiveSync y su estado actual en el dispositivo móvil.
- Desconectar dispositivos EAS de la administración si no se encuentra en uso.
- Definir la configuración de sondeo de Active Directory mediante el servidor de dispositivos móviles de Exchange, que permite actualizar la información sobre los buzones y los dispositivos móviles de los usuarios.

Adición de un perfil de administración

Puede crear perfiles de administración de dispositivos EAS para administrar estos dispositivos y asignarlos a los buzones de Microsoft Exchange que desee.

Solo se puede asignar un perfil de administración de dispositivos EAS a un buzón de correo de Microsoft Exchange.

Para agregar un perfil de administración de dispositivos EAS a un buzón de correo de Microsoft Exchange, siga estos pasos:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles**.
2. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.
3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un servidor de dispositivos móviles Exchange.

4. Seleccione **Propiedades** en el menú contextual del Servidor de dispositivos móviles de Exchange.

   Se abre la ventana de propiedades del Servidor de dispositivos móviles.

5. En la ventana de propiedades de **Servidor de dispositivos móviles de Exchange**, seleccione la sección **Buzones de correo**.

6. Seleccione un buzón y haga clic en el botón **Asignar perfil**.

   Se abre la ventana **Perfiles de directiva**.

7. En la ventana **Perfiles de directiva**, haga clic en el botón **Agregar**.

   Se abre la ventana **Perfil nuevo**.

8. Configure el perfil en las fichas de la ventana **Perfil nuevo**.

   - Si desea especificar el nombre del perfil y el intervalo de actualización, seleccione la ficha **General**.
   - Si desea configurar la contraseña del usuario del dispositivo móvil, seleccione la ficha **Contraseña**.
   - Si desea configurar la sincronización con el servidor Microsoft Exchange, seleccione la ficha **Sincronización**.
   - Si desea configurar restricciones para las funciones del dispositivo móvil, seleccione la ficha **Restricciones de funciones**.
   - Si desea configurar restricciones para el uso de aplicaciones móviles en el dispositivo móvil, seleccione la ficha **Restricciones para las aplicaciones**.

9. Haga clic en **Aceptar**.

   El nuevo perfil se mostrará en la lista de perfiles de la ventana **Perfiles de directiva**.

   Si desea que se asigne este perfil automáticamente a nuevos buzones, así como a aquellos cuyos perfiles se han eliminado, selecciónelo en la lista de perfiles y haga clic en el botón **Definir como perfil predeterminado**.

   > El perfil predeterminado no se puede eliminar. Para eliminar el perfil predeterminado actual, debe asignar el atributo "perfil predeterminado" a un perfil diferente.

10. En la ventana **Perfiles de directiva**, haga clic en **Aceptar**.

    La configuración de perfiles de administración se aplicará al dispositivo EAS en la siguiente sincronización del dispositivo con el servidor de dispositivos móviles de Exchange.

Eliminación de un perfil de administración

Para eliminar un perfil de administración de dispositivos EAS de un buzón de correo de Microsoft Exchange, siga estos pasos:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles**.

2. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.

3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un servidor de dispositivos móviles Exchange.

4. Seleccione **Propiedades** en el menú contextual del Servidor de dispositivos móviles de Exchange.

   Se abre la ventana de propiedades del Servidor de dispositivos móviles.

5. En la ventana de propiedades del Servidor de dispositivos móviles de Exchange, seleccione la sección **Buzones de correo**.

6. Seleccione un buzón y haga clic en el botón **Cambiar perfiles**.

   Se abre la ventana **Perfiles de directiva**.

7. En la ventana **Perfiles de directiva**, seleccione el perfil que desea eliminar y haga clic en el botón rojo de eliminación.

   El perfil seleccionado se quita de la lista de perfiles de administración. El perfil predeterminado actual se aplica a los dispositivos EAS que administraba el perfil eliminado.

   > Si desea eliminar el perfil predeterminado actual, reasigne la propiedad "perfil predeterminado" a otro perfil y elimine el primero.

Administración de directivas de Exchange ActiveSync

Después de instalar el Servidor de dispositivos móviles de Exchange, en la sección **Buzones de correo** de la ventana de propiedades del Servidor puede consultar la información sobre las cuentas del servidor Exchange de Microsoft que se han recuperado al sondear el bosque de dominio o el dominio actual.

Además, en la ventana de propiedades del Servidor de dispositivos móviles de Exchange, puede usar los siguientes botones:

- **Cambiar perfiles** le permite abrir la ventana **Perfiles de directiva**, que contiene una lista de directivas recuperadas del servidor Microsoft Exchange. En esta ventana, puede crear, modificar o eliminar directivas de Exchange ActiveSync. La ventana **Perfiles de directiva** es prácticamente idéntica a la ventana de modificación de directivas en la Consola de gestión de Exchange.

- **Asignar perfiles a los dispositivos móviles** permite asignar una directiva de Exchange ActiveSync seleccionada a una o varias cuentas.

- **Activar/desactivar ActiveSync** permite activar o desactivar HTTP de Exchange ActiveSync para una o varias cuentas.

Configuración de la cobertura del análisis

En las propiedades del Servidor de dispositivos móviles de Exchange recientemente instalado, en la sección **Configuración**, puede configurar la cobertura del análisis. De forma predeterminada, la cobertura del análisis es el dominio actual en el cual está instalado el Servidor de dispositivos móviles de Exchange. La selección del valor **Todo el bosque de dominio** expande la cobertura del análisis para incluir el todo el bosque de dominio.

Uso de dispositivos EAS

Los dispositivos recuperados mediante el análisis del servidor Exchange de Microsoft se añadirán a la lista común de dispositivos, que se ubica en el nodo **Administración de dispositivos móviles**, en la carpeta **Dispositivos móviles**.

Si desea que la carpeta **Dispositivos móviles** muestre únicamente dispositivos de Exchange ActiveSync (en adelante, denominados dispositivos EAS), filtre la lista de dispositivos haciendo clic en el enlace **Exchange ActiveSync (EAS)** que se ubica anteriormente esta lista.

Puede administrar dispositivos EAS mediante comandos. Por ejemplo, el comando **Restablecer ajustes de fábrica** le permite eliminar todos los datos de un dispositivo y restablecer la configuración del dispositivo a los ajustes de fábrica. Este comando es útil si el dispositivo se pierde o es robado, cuando debe impedir que los datos personales o corporativos caigan en manos de terceros.

Si todos los datos se han eliminado del dispositivo, se eliminarán nuevamente la próxima vez que el dispositivo se conecte al servidor Exchange de Microsoft. El comando se reiterará hasta que se elimine el dispositivo de la lista de dispositivos. Este comportamiento es causado por los principios de funcionamiento del servidor Exchange de Microsoft.

Para eliminar un dispositivo EAS de la lista, en el menú contextual del dispositivo, seleccione **Eliminar**. Si la cuenta de Exchange ActiveSync no se elimina del dispositivo EAS, este reaparecerá en la lista de dispositivos después de la próxima sincronización del dispositivo con el servidor Exchange de Microsoft.

Ver información sobre un dispositivo EAS

Para ver información sobre un dispositivo EAS:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, puede filtrar los dispositivos EAS si hace clic en el enlace **Exchange ActiveSync (EAS)**.

3. Desde el menú contextual del dispositivo móvil, seleccione **Propiedades**.

   Abra la ventana de propiedades del dispositivo EAS seleccionado.

La ventana de propiedades del dispositivo móvil muestra información sobre el dispositivo EAS conectado.

Desconexión de un dispositivo EAS de la administración

Siga estos pasos para desconectar un dispositivo EAS de la administración del servidor de dispositivos móviles de Exchange:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, puede filtrar los dispositivos EAS si hace clic en el enlace **Exchange ActiveSync (EAS)**.

3. Seleccione el dispositivo móvil que desea desconectar de la administración del Servidor de dispositivos móviles de Exchange.

4. En el menú contextual del dispositivo móvil, seleccione **Eliminar**.

El dispositivo EAS se marcará con una cruz roja para indicar su eliminación. El dispositivo móvil se eliminará de la lista de dispositivos administrados después de que se elimine de la base de datos del Servidor de dispositivos móviles Exchange ActiveSync. Para ello, el administrador debe quitar la cuenta de usuario del servidor Microsoft Exchange.

Derechos de usuario para administrar dispositivos móviles de Exchange ActiveSync

Para administrar los dispositivos móviles que se ejecutan de acuerdo con el protocolo de Exchange ActiveSync con Microsoft Exchange Server 2010 o Microsoft Exchange Server 2013, asegúrese de que el usuario está incluido en un grupo de funciones para el que se pueden ejecutar los commandlets siguientes:

- Get-CASMailbox
- Set-CASMailbox
- Remove-ActiveSyncDevice
- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings
- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy

Para administrar dispositivos móviles que se ejecuten según el protocolo Exchange ActiveSync con Microsoft Exchange Server 2007, asegúrese de que el usuario posee derechos de administrador. Si no se han concedido estos derechos, ejecute los commandlets para asignar derechos de administrador al usuario (consulte la tabla siguiente).

Derechos de administrador requeridos para administrar dispositivos móviles de Exchange ActiveSync en Microsoft Exchange Server 2007

Acceso	Objeto	Cmdle
Todos	Rama "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	`Add-ADPermission -User usuario o grupo> -Ident Mailbox Policies,CN=<No organización>,CN=Micros Exchange,CN=Services,CN <Nombre del dominio>" - All -AccessRight Generi`
Lectura	Rama "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC= yourdomain"	`Add-ADPermission -User usuario o grupo> -Ident la organización>,CN=Mic Exchange,CN=Services,CN`

		`<Nombre del dominio>" -All -AccessRight Generi`
Lectura/escritura	Propiedades msExchMobileMailboxPolicyLink y msExchOmaAdminWirelessEnable para objetos de Active Directory	`Add-ADPermission -User usuario o grupo> -Ident del dominio>" -Inherita AccessRight ReadPropert Properties msExchMobile msExchOmaAdminWirelessE`
Todos	Repositorios de buzones de correo para ms-Exch-Store-Admin	`Get-MailboxDatabase | A User <nombre de usuario ExtendedRights ms-Exch-`

Para obtener más información sobre cómo utilizar los commandlets en la consola del shell de administración de Exchange, consulte el sitio web del Servicio de Soporte Técnico de Microsoft Exchange Server.

Administración de dispositivos iOS con MDM

Esta sección describe las funciones avanzadas para la administración de dispositivos iOS con MDM con Kaspersky Security Center. La aplicación admite las siguientes funciones para la administración de dispositivos iOS con MDM:

- Defina los ajustes de los dispositivos iOS con MDM administrados en modo centralizado y restrinja sus características por medio de los perfiles de configuración. Puede agregar o modificar los perfiles de configuración e instalarlos en los dispositivos móviles.
- Instale aplicaciones en dispositivos móviles por medio de perfiles de aprovisionamiento, evitando App Store. Por ejemplo, puede usar perfiles de aprovisionamiento para instalar aplicaciones corporativas internas en los dispositivos móviles del usuario. Un perfil de aprovisionamiento contiene información acerca de una app y un dispositivo móvil.
- Instale aplicaciones en un dispositivo MDM con iOS mediante App Store. Antes de instalar una aplicación en un dispositivo MDM con iOS, debe agregarla al Servidor de MDM para iOS.

Cada 24 horas se envía una notificación push a todos los dispositivos iOS con MDM conectados a fin de sincronizar los datos con el Servidor de MDM para iOS.

Para obtener información sobre el perfil de configuración y el perfil de aprovisionamiento, así como de las aplicaciones instaladas en un dispositivo MDM con iOS, consulte la ventana de propiedades del dispositivo.

Firmar un perfil de MDM para iOS mediante un certificado

Puede firmar un perfil de MDM para iOS mediante un certificado. Puede utilizar un certificado que haya emitido o puede recibir un certificado de las autoridades de certificación de confianza.

Para firmar un perfil de MDM para iOS mediante un certificado:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.

3. En la ventana de propiedades de la carpeta, seleccione la sección **Configuración de conexión para dispositivos iOS**.

4. Haga clic en el botón **Examinar** debajo del campo **Seleccionar archivo de certificado**.

   La ventana **Certificado**.

5. En el campo **Tipo de certificado**, especifique el tipo de certificado público o privado:

   - Si está seleccionado el valor **Contenedor PKCS #12**, especifique el archivo de certificado y la contraseña.
   - Si el valor **Certificado X.509** está seleccionado:

     a. Especifique el archivo clave privado (tiene la extensión *.prk o *.pem).

     b. Especifique la contraseña de la clave privada.

     c. Especifique el archivo clave público (tiene la extensión *.cer).

6. Haga clic en **Aceptar**.

Un certificado firma el perfil de MDM para iOS.

Adición de perfiles de configuración

Para crear un perfil de configuración, puede utilizar Apple Configurator 2, que está disponible en el sitio web de Apple Inc. Apple Configurator 2 solo funciona en dispositivos que ejecutan macOS; Si no tiene dichos dispositivos a su disposición, puede usar la Utilidad de configuración del iPhone en el dispositivo con la Consola de administración. Sin embargo, Apple Inc. ya no admite la Utilidad de configuración de iPhone.

Para crear un perfil de configuración usando la Utilidad de configuración de iPhone y añadirlo a un servidor de MDM para iOS:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.

2. En el espacio de trabajo de la carpeta **Administración de dispositivos móviles**, seleccione la subcarpeta **Servidores de dispositivos móviles**.

3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.

4. En el menú contextual del servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de dispositivos móviles.

5. En la ventana de propiedades del Servidor de MDM para iOS, seleccione la sección **Perfiles de configuración**.

6. En la sección **Perfiles de configuración**, haga clic en el botón **Crear**.

   Se abre la ventana **Nuevo perfil de configuración**.

7. En la ventana **Nuevo perfil de configuración**, especifique un nombre y un ID para el perfil.

   El identificador del perfil de configuración debe ser único; el valor se debe especificar en formato de DNS inverso, por ejemplo, *com.companyname.identifier*.

8. Haga clic en **Aceptar**.

   La utilidad de configuración de iPhone se inicia si la tiene instalada.

9. Vuelva a configurar el perfil en la utilidad de configuración de iPhone.

   Para obtener una descripción de la configuración del perfil e instrucciones sobre cómo configurar el perfil, consulte la documentación incluida con la utilidad de configuración de iPhone.

Una vez que haya configurado el perfil con la utilidad de configuración de iPhone, el nuevo perfil de configuración se muestra en la sección **Perfiles de configuración** de la ventana de propiedades del Servidor de MDM para iOS.

Haga clic en el botón **Modificar** para modificar el perfil de configuración.

Haga clic en el botón **Importar** para cargar el perfil de configuración en un programa.

Haga clic en el botón **Exportar** para guardar el perfil de configuración en un archivo.

El perfil que ha creado debe estar instalado en dispositivos MDM con iOS.

Instalación de un perfil de configuración en un dispositivo

Para instalar un perfil de configuración en un dispositivo móvil, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos con MDM de iOS por tipo de protocolo (*MDM de iOS*).

3. Seleccione el dispositivo móvil del usuario en el que desea instalar un perfil de configuración.

   Puede seleccionar varios dispositivos móviles en los que instalar a la vez el perfil.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Instalar perfil** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** en el menú contextual del dispositivo móvil y, a continuación **Instalar perfil**.

   Se abre la ventana **Seleccionar perfiles** y muestra una lista de perfiles. Seleccione en la lista el perfil que tiene que instalar en el dispositivo móvil. Puede seleccionar varios perfiles para instalarlos a la vez en el dispositivo móvil. Para seleccionar el intervalo de perfiles, utilice la tecla **Mayús**. Para combinar varios perfiles en un grupo, utilice la tecla **Ctrl**.

6. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando se ejecuta el comando, se instala en el dispositivo móvil del usuario el perfil de configuración seleccionado. Si se ejecuta correctamente el comando, el estado actual del comando se mostrará como *Listo* en el registro de comandos.

   Haga clic en el botón **Reenviar** para volver a enviar el comando al dispositivo móvil del usuario.

   Haga clic en el botón **Quitar de la cola** para cancelar la ejecución de un comando enviado que todavía no se ha ejecutado.

La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con sus respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

7. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

Puede ver el perfil que ha instalado y eliminarlo, si es necesario.

Eliminación de un perfil de configuración de un dispositivo

Para quitar un perfil de configuración de un dispositivo móvil, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, puede filtrar los dispositivos con MDM de iOS haciendo clic en el enlace **MDM de iOS**.

3. Seleccione el dispositivo móvil del usuario del que tiene que quitar el perfil de configuración.

   Puede seleccionar varios dispositivos móviles de los que quitar a la vez el perfil.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Eliminar perfil** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** en el menú contextual del dispositivo y, a continuación, **Eliminar perfil**.

   Se abre la ventana **Eliminar perfiles** y muestra una lista de perfiles.

6. Seleccione en la lista el perfil que tiene que quitar del dispositivo móvil. Puede seleccionar varios perfiles para quitarlos a la vez del dispositivo móvil. Para seleccionar el intervalo de perfiles, utilice la tecla **Mayús**. Para combinar varios perfiles en un grupo, utilice la tecla **Ctrl**.

7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando se ejecuta el comando, se quita del dispositivo móvil del usuario el perfil de configuración seleccionado. Si se ejecuta correctamente el comando, el estado actual del comando se mostrará como *Completado*.

   Haga clic en el botón **Reenviar** para volver a enviar el comando al dispositivo móvil del usuario.

   Haga clic en el botón **Quitar de la cola** para cancelar la ejecución de un comando enviado que todavía no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con sus respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

Adición de un nuevo dispositivo mediante la publicación de un enlace en un perfil

En la Consola de administración, el administrador crea un nuevo perfil de MDM para iOS usando el Asistente para conectar un nuevo dispositivo móvil. El Asistente realiza las siguientes acciones:

- El perfil de MDM para iOS se publica automáticamente en el Servidor Web.
- El usuario recibe un enlace al perfil de MDM para iOS por SMS o por correo electrónico. Después de recibir el enlace, el usuario instala el perfil de MDM para iOS en el dispositivo móvil.
- El dispositivo móvil se conecta al Servidor de MDM para iOS.

Debido a una directiva de seguridad más estricta introducida por Apple, debe configurar las versiones del protocolo TLS 1.1 y TLS 1.2 al conectar un dispositivo móvil que ejecute iOS 11 a un Servidor de administración que tenga la integración con la Infraestructura de clave pública (PKI) habilitada.

Agregar un nuevo dispositivo mediante la instalación del perfil por el administrador

Para conectar un dispositivo móvil a un Servidor de MDM para iOS mediante la instalación de un perfil de MDM para iOS en ese dispositivo móvil, el administrador debe realizar las siguientes acciones:

1. En Consola de administración, abra el Asistente de Conexión de nuevo dispositivo.
2. Cree un nuevo perfil de MDM para iOS al seleccionar la casilla **Mostrar el certificado cuando el Asistente finalice** en la ventana del Asistente para nuevo perfil.
3. Guarde el perfil de MDM para iOS.
4. Instale el perfil de MDM para iOS en el dispositivo móvil del usuario mediante la utilidad Apple Configurator.

   El dispositivo móvil se conecta al Servidor de MDM para iOS.

Debido a una directiva de seguridad más estricta introducida por Apple, debe configurar las versiones del protocolo TLS 1.1 y TLS 1.2 al conectar un dispositivo móvil que ejecute iOS 11 a un Servidor de administración que tenga la integración con la Infraestructura de clave pública (PKI) habilitada.

Adición de un perfil de aprovisionamiento

Para añadir un perfil de aprovisionamiento a un Servidor de MDM para iOS:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles**.
2. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.
3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.
4. En el menú contextual del servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de dispositivos móviles.
5. En la ventana de propiedades del **Servidor de MDM para iOS**, vaya a la sección **Perfiles de aprovisionamiento**.

6. En la sección **Perfiles de aprovisionamiento**, haga clic en el botón **Importar** e indique la ruta de un archivo de perfil de aprovisionamiento.

   Se agregará el perfil a la configuración del Servidor de MDM para iOS.

   Haga clic en el botón **Exportar** para guardar el perfil de aprovisionamiento en un archivo.

Puede instalar el perfil de aprovisionamiento que importó en dispositivos iOS MDM.

Instalación de un perfil de aprovisionamiento en un dispositivo

Para instalar un perfil de aprovisionamiento en un dispositivo móvil, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos con MDM de iOS por tipo de protocolo (*MDM de iOS*).

3. Seleccione el dispositivo móvil del usuario en el que desea instalar el perfil de aprovisionamiento.

   Puede seleccionar varios dispositivos móviles en los que instalar a la vez el perfil de aprovisionamiento.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Instalar perfil de aprovisionamiento** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** en el menú contextual del dispositivo móvil y, a continuación, **Instalar perfil de aprovisionamiento**.

   Se abre la ventana **Seleccionar perfiles de aprovisionamiento** y muestra una lista de perfiles de aprovisionamiento. Seleccione en la lista el perfil de aprovisionamiento que desea instalar en el dispositivo móvil. Puede seleccionar varios perfiles de aprovisionamiento para instalarlos a la vez en el dispositivo móvil. Para seleccionar el intervalo de perfiles de aprovisionamiento, utilice la tecla **Mayús**. Para combinar varios perfiles de aprovisionamiento en un grupo, utilice la tecla **Ctrl**.

6. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando se ejecuta el comando, se instala el perfil de aprovisionamiento seleccionado en el dispositivo móvil del usuario. Si se ejecuta correctamente el comando, el estado actual del comando aparece como *Completado* en el registro.

   Haga clic en el botón **Reenviar** para volver a enviar el comando al dispositivo móvil del usuario.

   Haga clic en el botón **Quitar de la cola** para cancelar la ejecución de un comando enviado que todavía no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con sus respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

7. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

Puede ver el perfil que ha instalado y eliminarlo, si es necesario.

Eliminación de un perfil de aprovisionamiento del dispositivo

Para quitar un perfil de aprovisionamiento de un dispositivo móvil:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos con MDM de iOS por tipo de protocolo (*MDM de iOS*).

3. Seleccione el dispositivo móvil del usuario del que tiene que quitar el perfil de aprovisionamiento.

   Puede seleccionar varios dispositivos móviles de los que quitar a la vez el perfil de aprovisionamiento.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Eliminar perfil de aprovisionamiento** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** en el menú contextual del dispositivo móvil y, a continuación, **Eliminar perfil de aprovisionamiento**.

   Se abre la ventana **Eliminar perfiles de aprovisionamiento** y muestra una lista de perfiles.

6. Seleccione en la lista el perfil de aprovisionamiento que desea quitar del dispositivo móvil. Puede seleccionar varios perfiles de aprovisionamiento para quitarlos a la vez en el dispositivo móvil. Para seleccionar el intervalo de perfiles de aprovisionamiento, utilice la tecla **Mayús**. Para combinar varios perfiles de aprovisionamiento en un grupo, utilice la tecla **Ctrl**.

7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando se ejecuta el comando, se quita del dispositivo móvil del usuario el perfil de aprovisionamiento seleccionado. No se podrán utilizar las aplicaciones relacionadas con el perfil de aprovisionamiento eliminado. Si se ejecuta correctamente el comando, el estado actual del comando se mostrará como *Completado*.

   Haga clic en el botón **Reenviar** para volver a enviar el comando al dispositivo móvil del usuario.

   Haga clic en el botón **Quitar de la cola** para cancelar la ejecución de un comando enviado que todavía no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con sus respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

Adición de una aplicación administrada

Antes de instalar una aplicación en un dispositivo MDM con iOS, debe agregarla al Servidor de MDM para iOS. Se considera que una aplicación es administrada si se ha instalado en un dispositivo mediante Kaspersky Security Center. Una aplicación administrada se puede controlar de forma remota mediante Kaspersky Security Center.

Para agregar una aplicación administrada a un Servidor de MDM para iOS:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles**.

2. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Servidores de dispositivos móviles**.

3. En el espacio de trabajo de la carpeta **Servidores de dispositivos móviles**, seleccione un Servidor de MDM para iOS.

4. En el menú contextual del servidor de MDM para iOS, seleccione **Propiedades**.

   Se abre la ventana de propiedades del Servidor de MDM para iOS.

5. En la ventana de propiedades del servidor de MDM para iOS, seleccione la sección **Aplicaciones administradas**.

6. Haga clic en el botón **Agregar** de la sección **Aplicaciones administradas**.

   Se abre la ventana **Agregar una aplicación**.

7. En la ventana **Agregar una aplicación**, en el campo **Nombre de la aplicación** especifique el nombre de la aplicación que se va a agregar.

8. En el campo **ID de Apple o enlace a App Store**, especifique el ID de Apple de la aplicación que se va a agregar o un enlace al archivo de manifiesto que se pueda usar para descargar la aplicación.

9. Si desea quitar una aplicación administrada del dispositivo móvil del usuario junto con el perfil de MDM para iOS, al desinstalar este último, seleccione la casilla **Quitar junto con el perfil de MDM para iOS**.

10. Si desea bloquear la creación de copias de seguridad de los datos de la aplicación a través de iTunes, seleccione la casilla **Bloquear copia de seguridad de datos**.

11. Haga clic en **Aceptar**.

La aplicación agregada aparece en la sección **Aplicaciones administradas** de la ventana de propiedades del Servidor de MDM para iOS.

Instalación de una aplicación en un dispositivo móvil

Para instalar una aplicación en un dispositivo con MDM de iOS, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. Seleccione el dispositivo MDM con iOS en el que desee instalar una aplicación.

   Puede seleccionar varios dispositivos móviles en los que instalar a la vez la aplicación.

3. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

4. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Instalar app** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** en el menú contextual del dispositivo móvil y, a continuación, **Instalar app**.

Se abre la ventana **Seleccionar aplicaciones** y muestra una lista de perfiles. Seleccione en la lista la aplicación que desea instalar en el dispositivo móvil. Puede seleccionar varias aplicaciones para instalarlos a la vez en el dispositivo móvil. Para seleccionar un intervalo de aplicaciones, utilice la tecla **Mayús**. Para combinar aplicaciones en un grupo, utilice la tecla **Ctrl**.

5. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando se ejecuta el comando, se instala en el dispositivo móvil del usuario la aplicación seleccionada. Si se ejecuta correctamente el comando, el estado actual del comando se mostrará como *Completado* en el registro.

   Haga clic en el botón **Reenviar** para volver a enviar el comando al dispositivo móvil del usuario. Haga clic en el botón **Quitar de la cola** para cancelar la ejecución de un comando enviado que todavía no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con sus respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

6. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

En las propiedades del dispositivo con MDM de iOS se muestra información sobre la aplicación instalada. Puede quitar la aplicación del dispositivo móvil mediante el registro de comandos o desde el menú contextual del dispositivo móvil.

Eliminación de una aplicación del dispositivo

Para quitar una aplicación de un dispositivo móvil, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos con MDM de iOS por tipo de protocolo (*MDM de iOS*).

3. Seleccione el dispositivo móvil del usuario del que desea quitar la aplicación.

   Puede seleccionar varios dispositivos móviles de los que quitar a la vez la aplicación.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Eliminar app** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** en el menú contextual del dispositivo móvil y, a continuación **Eliminar app**.

   De este modo, se abre la ventana **Quitar aplicaciones** y se muestra una lista de aplicaciones.

6. Seleccione en la lista la aplicación que desea quitar del dispositivo móvil. Puede seleccionar varias aplicaciones para quitarlas simultáneamente. Para seleccionar un intervalo de aplicaciones, utilice la tecla **Mayús**. Para combinar aplicaciones en un grupo, utilice la tecla **Ctrl**.

7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando se ejecuta el comando, se quita del dispositivo móvil del usuario la aplicación seleccionada. Si se ejecuta correctamente el comando, el estado actual del comando se mostrará como *Completado*.

   Haga clic en el botón **Reenviar** para volver a enviar el comando al dispositivo móvil del usuario.

Haga clic en el botón **Quitar de la cola** para cancelar la ejecución de un comando enviado que todavía no se ha ejecutado.

La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo móvil, con sus respectivos estados de ejecución. Haga clic en **Actualizar** para actualizar la lista de comandos.

8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para la administración de dispositivos móviles**.

Configuración de itinerancia en un dispositivo móvil con MDM de iOS

Para configurar la itinerancia:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles**.
2. En la carpeta **Administración de dispositivos móviles**, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
3. Seleccione el dispositivo MDM con iOS del usuario para quien tiene que configurar la itinerancia.

   Puede seleccionar varios dispositivos móviles en los que configurar la itinerancia a la vez.
4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.
5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Configurar itinerancia** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos → Configurar itinerancia** en el menú contextual del dispositivo.
6. En la ventana **Configuración de itinerancia**, especifique la siguiente configuración:

   - Activar itinerancia de voz

     Si se selecciona esta opción, se habilita la itinerancia de voz en el dispositivo con MDM de iOS. El usuario del dispositivo móvil con MDM de iOS puede efectuar y contestar llamadas mientras esté activada la itinerancia.

     Esta opción está activada de forma predeterminada.

   - Activar itinerancia de datos

     Si esta opción está seleccionada, se habilita la itinerancia de voz en el dispositivo con MDM de iOS. El usuario del dispositivo móvil con MDM de iOS puede navegar por Internet mientras está en itinerancia.

     Esta opción está desactivada de forma predeterminada.

La itinerancia se configura para los dispositivos seleccionados.

Visualización de la información de un dispositivo MDM con iOS

Para consultar la información de un dispositivo MDM con iOS, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, puede filtrar los dispositivos con MDM de iOS haciendo clic en el enlace **MDM de iOS**.

3. Seleccione el dispositivo móvil cuya información necesite consultar.

4. Desde el menú contextual del dispositivo móvil, seleccione **Propiedades**.

   De esa forma, se abrirá la ventana de propiedades del dispositivo MDM con iOS.

La ventana de propiedades del dispositivo móvil muestra información acerca del dispositivo MDM con iOS conectado.

Desvinculación un dispositivo MDM con iOS de la administración

Para desvincular un dispositivo MDM con iOS del Servidor de MDM para iOS, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, puede filtrar los dispositivos con MDM de iOS haciendo clic en el enlace **MDM de iOS**.

3. Seleccione el dispositivo móvil que desee desvincular.

4. En el menú contextual del dispositivo móvil, seleccione **Eliminar**.

   Se seleccionará el dispositivo MDM con iOS en la lista para que se desinstale. El dispositivo móvil se quitará automáticamente de la lista de dispositivos administrados cuando este se quite de la base de datos del Servidor de MDM para iOS. El dispositivo móvil se eliminará desde la base de datos del Servidor de MDM para iOS en un plazo de un minuto.

Cuando se desvincula el dispositivo MDM con iOS de la administración, se quitan del dispositivo móvil todos los perfiles de configuración, el perfil de MDM para iOS y las aplicaciones que tengan activada la opción **Quitar junto con el perfil de MDM para iOS**.

Envío de comandos a un dispositivo

Para enviar un comando a un dispositivo MDM con iOS:

1. En la Consola de administración, abra el nodo **Administración de dispositivos móviles**.

2. Seleccione la carpeta **Dispositivos móviles**.

3. En la carpeta **Dispositivos móviles**, seleccione el dispositivo móvil al cual se deben enviar los comandos.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la lista que aparece, seleccione el comando que se enviará al dispositivo móvil.

Comprobación del estado de ejecución de los comandos enviados

Para verificar el estado de ejecución de un comando enviado a un dispositivo móvil:

1. En la Consola de administración, abra el nodo **Administración de dispositivos móviles**.
2. Seleccione la carpeta **Dispositivos móviles**.
3. En la carpeta **Dispositivos móviles**, seleccione el dispositivo móvil en el cual debe comprobarse el estado de ejecución para los comandos seleccionados.
4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

Administración de dispositivos KES

En Kaspersky Security Center, puede administrar dispositivos móviles KES de las siguientes maneras:

- Administre los dispositivos KES de forma centralizada utilizando comandos.
- Ver información sobre la configuración para la administración de dispositivos KES.
- Instalar aplicaciones mediante paquetes de aplicaciones para dispositivos móviles.
- Desvincular dispositivos KES de la administración.

Creación de un paquete de apps para dispositivos KES

Se requiere una licencia de Kaspersky Endpoint Security for Android para crear un paquete de aplicaciones para dispositivos KES.

Siga estos pasos para crear un paquete de aplicaciones móviles:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.

   La carpeta **Instalación remota** es una subcarpeta de la carpeta predeterminada **Avanzado**.
2. Haga clic en el botón **Acciones adicionales** y seleccione **Administrar paquetes de aplicaciones móviles** en la lista desplegable.
3. En la ventana **Administración de paquetes de aplicaciones móviles**, haga clic en el botón **Nuevo**.
4. Se iniciará el Asistente para la creación de paquetes de aplicaciones móviles. Siga las instrucciones del Asistente.

El paquete de aplicaciones para dispositivos móviles recientemente creado se muestra en la ventana **Administración de paquetes de aplicaciones móviles**.

Activación de la verificación en dos pasos de dispositivos KES

Para permitir la verificación en dos pasos de un dispositivo KES:

1. Abra el Registro del dispositivo cliente que tenga instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).
2. Vaya al siguiente subárbol:
   - Para un sistema de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - Para un sistema de 32 bits:

     HKLM\Software\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Cree una clave con el nombre LP_MobileMustUseTwoWayAuthOnPort13292.
4. Especifique REG_DWORD como tipo de clave.
5. Configure el valor de clave en 1.
6. Reinicie el servicio del Servidor de administración.

   Se activará la verificación en dos pasos del dispositivo KES utilizando un certificado compartido después de ejecutar el servicio del Servidor de administración.

> La primera conexión del dispositivo KES con el Servidor de administración no requiere ningún certificado.

De forma predeterminada, la verificación en dos pasos de dispositivos KES está desactivada.

Consulta de información de un dispositivo KES

Para consultar información sobre un dispositivo KES, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el espacio de trabajo, filtre los dispositivos KES por tipo de protocolo *(KES)*.
3. Seleccione el dispositivo móvil cuya información desee consultar.
4. Desde el menú contextual del dispositivo móvil, seleccione **Propiedades**.

   Abra la ventana de propiedades del dispositivo KES seleccionado.

La ventana de propiedades del dispositivo móvil muestra información sobre el dispositivo KES conectado.

Desvinculación de dispositivos KES de la administración

Para desvincular un dispositivo KES de la administración, el usuario debe quitar el Agente de red del dispositivo móvil. Una vez que el usuario ha eliminado el Agente de red, los detalles del dispositivo móvil se eliminan de la base de datos del Servidor de administración, por tanto el administrador puede eliminar el dispositivo móvil de la lista de dispositivos administrados.

Para quitar un dispositivo KES de la lista de dispositivos administrados, siga estos pasos:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el espacio de trabajo, filtre los dispositivos KES por tipo de protocolo *(KES)*.

3. Seleccione el dispositivo móvil que desee desvincular de la administración.

4. En el menú contextual del dispositivo móvil, seleccione **Eliminar**.

   El dispositivo móvil se quita de la lista de dispositivos administrados.

   Si no se ha quitado Kaspersky Endpoint Security for Android del dispositivo móvil, este volverá a aparecer en la lista de dispositivos administrados tras la sincronización con el Servidor de administración.

Protección y cifrado de datos

El cifrado de datos reduce el riesgo de pérdida involuntaria de datos en caso de que le roben o pierda su ordenador portátil, su unidad extraíble o su disco duro, o en caso de que usuarios no autorizados y aplicaciones accedan a ellos.

Kaspersky Endpoint Security para Windows proporciona funcionalidad de cifrado. Kaspersky Endpoint Security para Windows le permite cifrar archivos almacenados en unidades locales de dispositivos y unidades extraíbles, así como cifrar unidades extraíbles y unidades de disco duro en su totalidad.

Las reglas de cifrado se configuran mediante Kaspersky Security Center definiendo directivas. El cifrado y descifrado basado en reglas existentes se realiza cuando se aplica una directiva.

La disponibilidad de la función de administración de cifrado determina la configuración de la interfaz de usuario.

El administrador puede realizar las siguientes acciones:

- Configurar y realizar el cifrado o descifrado de archivos en los discos locales del dispositivo.
- Configurar y cifrar los archivos en unidades extraíbles.
- Crear reglas de acceso de la aplicación a archivos cifrados.

- Crear y entregar al usuario un archivo clave para acceder a archivos cifrados si el cifrado de archivos está restringido en el dispositivo del usuario.
- Configurar y realizar el cifrado de la unidad de disco duro.
- Administrar el acceso de usuario a discos duros y unidades extraíbles cifradas (administrar cuentas de agente de autenticación, crear y entregar a los usuarios información sobre la solicitud para la restauración del nombre de la cuenta y la contraseña, así como claves de acceso para dispositivos cifrados).
- Ver estados de cifrado e informes sobre el cifrado de archivos.

Estas operaciones se realizan mediante las herramientas integradas en Kaspersky Endpoint Security para Windows. Si desea obtener instrucciones detalladas sobre cómo realizar cifrados, así como una descripción de las funciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows.

Kaspersky Security Center admite la funcionalidad de administración de cifrado para dispositivos que usan sistemas operativos MAC. El cifrado se configura usando herramientas de Kaspersky Endpoint Security for Mac para versiones de aplicación que admitan la funcionalidad de cifrado. Si desea obtener instrucciones detalladas sobre cómo realizar cifrados, así como una descripción de las funciones, consulte la *Guía del administrador de Kaspersky Endpoint Security for Mac*.

Visualización de la lista de dispositivos cifrados

Siga estos pasos para ver la lista de dispositivos que almacenan información cifrada:

1. En el árbol del Servidor de administración, seleccione la carpeta **Protección y cifrado de datos**.
2. Abra la lista de dispositivos cifrados usando uno de los siguientes métodos:
   - Haga clic en el enlace **Ir a la lista de dispositivos cifrados** en la sección **Administrar dispositivos cifrados**.
   - Seleccione la carpeta **Dispositivos cifrados** en el árbol de consola.

El espacio de trabajo muestra información acerca de los dispositivos en la red que almacenan archivos cifrados, así como acerca de dispositivos cifrados en el nivel de la unidad. Una vez que se descifre la información de un dispositivo, este se elimina automáticamente de la lista.

Puede clasificar la información en la lista de dispositivos en orden ascendente o descendente en cualquier columna.

Los parámetros de la interfaz de usuario determinan si aparece en el árbol de consola la carpeta **Protección y cifrado de datos**.

Visualización de la lista de eventos de cifrado

Al ejecutar tareas de cifrado y descifrado de datos en los dispositivos cliente, Kaspersky Endpoint Security para Windows envía a Kaspersky Security Center información sobre los siguientes tipos de eventos:

- No se puede cifrar o descifrar un archivo, o crear un archivo cifrado debido a que falta espacio en disco.

- No se puede cifrar o descifrar un archivo, o crear un archivo cifrado debido a problemas de licencia.
- No se puede cifrar o descifrar un archivo, o crear un archivo cifrado debido a que faltan derechos de acceso.
- Se ha prohibido a la aplicación acceder a un archivo cifrado.
- Errores desconocidos.

Para ver una lista de eventos que se han producido al cifrar datos en dispositivos:

1. En el árbol del Servidor de administración, seleccione la carpeta **Protección y cifrado de datos**.
2. Vaya a la lista de eventos que se produjeron durante el cifrado usando uno de los siguientes métodos:
   - Haga clic en el enlace **Ir a la lista de errores** en la sección **Errores de cifrado de datos**.
   - Seleccione la carpeta **Dispositivos cifrados** en el árbol de consola.

El espacio de trabajo muestra información acerca de los problemas que se han producido al cifrar datos en dispositivos.

Puede realizar las siguientes acciones en la lista de eventos de cifrado:

- Ordenar registros de datos en orden ascendente o descendente en cualquiera de las columnas.
- Realizar búsquedas rápidas de registros (por la coincidencia de texto con una subsecuencia en cualquier campo de la lista).
- Exportar listas de eventos a un archivo de texto.

Los parámetros de la interfaz de usuario determinan si aparece en el árbol de consola la carpeta **Protección y cifrado de datos**.

Exportación de una lista de eventos de cifrado a un archivo de texto

Siga estos pasos para exportar la lista de eventos de cifrado a un archivo de texto:

1. Cree una lista de eventos de cifrado.
2. En el menú contextual de la lista de eventos, seleccione **Exportar lista**.

   Se abre la ventana **Exportar lista**.
3. En la ventana **Exportar lista**, especifique el nombre del archivo de texto con la lista de eventos, seleccione una carpeta en la que guardarla y haga clic en el botón **Guardar**.

   La lista de eventos de cifrado se guardará en el archivo especificado.

Creación y visualización de informes sobre el cifrado

Puede generar los siguientes informes:

- Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo. Este informe contiene información sobre el estado de cifrado del dispositivo para todos los grupos de dispositivos.
- Informe sobre los derechos de acceso a dispositivos cifrados. Este informe contiene información sobre el estado de las cuentas de usuarios que han otorgado acceso a los dispositivos cifrados.
- Informe sobre errores en el cifrado de archivos. Este informe contiene información sobre errores que han ocurrido durante tareas de cifrado o descifrado de datos en dispositivos.
- Informe sobre el estado del cifrado de los dispositivos administrados. Este informe contiene información sobre si el estado del cifrado del dispositivo cumple con la directiva de cifrado.
- Informe sobre el bloqueo del acceso a archivos cifrados. Este informe contiene información sobre el bloqueo del acceso de la aplicación a archivos encriptados.

Para generar el informe de cifrado de dispositivos:

1. En el árbol de consola, seleccione la carpeta **Protección y cifrado de datos**.
2. Realice una de las siguientes acciones:
   - Para generar el informe sobre el estado de cifrado de los dispositivos administrados, haga clic en el enlace **Ver Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo**.

     Si aún no ha configurado este informe, se iniciará el Asistente de nueva plantilla de informe. Siga los pasos del Asistente.
   - Para generar el informe sobre el estado de cifrado de los dispositivos de almacenamiento masivo, en el árbol de la consola, seleccione la subcarpeta **Dispositivos cifrados** y luego haga clic en el botón **Ver Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo**.

Se inicia la generación de informes. El informe aparece en la ficha **Informes** en el nodo **Servidor de administración**.

Para generar el informe sobre derechos de acceso a dispositivos cifrados:

1. En el árbol de consola, seleccione la carpeta **Protección y cifrado de datos**.
2. Realice una de las siguientes acciones:
   - Haga clic en el enlace **Informe sobre los derechos de acceso a dispositivos cifrados** en la sección **Administrar dispositivos cifrados** para iniciar el Asistente de nueva plantilla de informe.
   - Seleccione la subcarpeta **Dispositivos cifrados**, después haga clic en el botón **Informe sobre los derechos de acceso a dispositivos cifrados** para iniciar el Asistente de nueva plantilla de informe.
3. Siga los pasos del Asistente de nueva plantilla de informe.

Se inicia la generación de informes. El informe aparece en la ficha **Informes** en el nodo **Servidor de administración**.

Para generar el informe sobre errores en el cifrado de archivos:

1. En el árbol de consola, seleccione la carpeta **Protección y cifrado de datos**.
2. Realice una de las siguientes acciones:

- Haga clic en el enlace **Ver informe sobre errores en el cifrado de archivos** en la sección **Errores de cifrado de datos** para iniciar el Asistente de nueva plantilla de informe.

- Seleccione la subcarpeta **Eventos de cifrado** y luego haga clic en el enlace **Informe sobre errores en el cifrado de archivos** para iniciar el Asistente de nueva plantilla de informe.

3. Siga los pasos del Asistente de nueva plantilla de informe.

Se inicia la generación de informes. El informe aparece en la ficha **Informes** en el nodo **Servidor de administración**.

Para generar el informe sobre el estado del cifrado de dispositivos administrados:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.

2. En el espacio de trabajo del nodo, abra la ficha **Informes**.

3. Haga clic en el botón **Nueva plantilla de informe** para ejecutar el Asistente de nueva plantilla de informe.

4. Siga las instrucciones del Asistente de nueva plantilla de informe. En la ventana **Selección del tipo de plantilla de informe**, en la sección **Otro**, seleccione **Informar sobre el estado de cifrado de los dispositivos administrados**.

   Cuando finaliza el Asistente de nueva plantilla de informe, aparece una nueva plantilla de informe en el nodo del Servidor de administración en la ficha **Informes**.

5. En el nodo del Servidor de administración correspondiente, en la ficha **Informes**, seleccione la plantilla de informe creada durante los pasos anteriores de las instrucciones.

Se inicia la generación de informes. El informe aparece en la ficha **Informes** en el nodo **Servidor de administración**.

También puede obtener información acerca de si los estados del cifrado de los dispositivos y de las unidades extraíbles cumplen con la directiva de cifrado en los paneles de información de la ficha **Estadísticas** del nodo Servidor de administración.

Para generar el informe sobre el bloqueo de acceso a archivos cifrados:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.

2. En el espacio de trabajo del nodo, abra la ficha **Informes**.

3. Haga clic en el botón **Nueva plantilla de informe** para iniciar el Asistente de nueva plantilla de informe.

4. Siga las instrucciones del Asistente de nueva plantilla de informe. En la **Selección del tipo de plantilla de informe** ventana, en la sección **Otro**, seleccione **Informe sobre el bloqueo del acceso a archivos cifrados**.

   Después de que finalice el Asistente de nueva plantilla de informe, aparece una nueva plantilla de informe en el nodo del **Servidor de administración** en la ficha **Informes**.

5. En el nodo del **Servidor de administración** en la ficha **Informes**, seleccione la plantilla de informe creada durante los pasos anteriores de las instrucciones.

Se inicia la generación de informes. El informe aparece en la ficha **Informes** en el nodo **Servidor de administración**.

Transmisión de claves de cifrado entre Servidores de administración

Si se activa la función de cifrado de datos en un dispositivo administrado, la clave de cifrado se almacena en el Servidor de administración. La clave de cifrado se utiliza para acceder a los datos cifrados y para gestionar la directiva de cifrado.

La clave de cifrado debe transmitirse a otro Servidor de administración en los siguientes casos:

- Se reconfigura el Agente de red en un dispositivo administrado para asignar el dispositivo a otro Servidor de administración. Si este dispositivo contiene datos cifrados, la clave de cifrado debe transmitirse al Servidor de administración de destino. De lo contrario, los datos no podrán descifrarse.

- Se cifra una unidad extraíble conectada a un dispositivo D1 administrado por el Servidor de administración S1 y luego se conecta esta unidad extraíble a un dispositivo D2 administrado por el Servidor de administración S2. Para acceder a los datos en la unidad extraíble, la clave de cifrado debe transmitirse desde el Servidor de administración S1 al Servidor de administración S2.

- Se cifra un archivo en un dispositivo D1 administrado por el Servidor de administración S1 y luego se intenta acceder al archivo en un dispositivo D2 administrado por el Servidor de administración S2. Para acceder al archivo, la clave de cifrado debe transmitirse desde el Servidor de administración S1 al Servidor de administración S2.

Puede transmitir claves de cifrado de las siguientes maneras:

- Automáticamente, al habilitar la opción **Usar la jerarquía de Servidores de administración para obtener claves de cifrado** en las propiedades de dos Servidores de administración entre los cuales se debe transmitir una clave de cifrado. Si esta opción está deshabilitada para uno de los Servidores de administración, la transmisión automática de claves de cifrado no es posible.

  Cuando activa la opción **Usar la jerarquía de Servidores de administración para obtener claves de cifrado** en las propiedades de un Servidor de administración, el Servidor de administración envía todas las claves de cifrado almacenadas en su repositorio al Servidor de administración principal (si hubiera) un nivel hacia arriba en la jerarquía.

  Cuando trata de acceder a los datos cifrados, el Servidor de administración primero busca la clave de cifrado en su propio repositorio. Si la opción **Usar la jerarquía de Servidores de administración para obtener claves de cifrado** está activada y la clave de cifrado requerida no se ha encontrado en el repositorio, el Servidor de administración también envía una solicitud a los Servidores de administración principales (si hubiera) para proporcionar la clave de cifrado requerida. La solicitud se enviará a todos los Servidores de administración principales hasta el servidor de nivel más alto en la jerarquía.

- Manualmente desde un Servidor de administración hasta otro al exportar e importar el archivo que contiene las claves de cifrado.

Para habilitar la transmisión automática de las claves de cifrado entre los Servidores de administración dentro de la jerarquía, realice lo siguiente:

1. En el árbol de la consola, seleccione el Servidor de administración para el que desea habilitar la transmisión automática de las claves de cifrado.

2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.

3. En la ventana propiedades, seleccione la sección **Algoritmo de cifrado**.

4. Active la opción **Usar la jerarquía de Servidores de administración para obtener claves de cifrado**.

5. Haga clic en **Aceptar** para aplicar los cambios.

Las claves de cifrado se transmitirán a los Servidores de administración principales (si hubiera) en la próxima sincronización (latido). Este Servidor de administración también proporcionará mediante solicitud una clave de cifrado desde su repositorio a un Servidor de administración secundario.

Para transmitir manualmente las claves de cifrado entre Servidores de administración, realice lo siguiente:

1. En el árbol de la consola del Servidor de administración, seleccione el Servidor de administración secundario desde el que desea transmitir las claves de cifrado.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana propiedades, seleccione la sección **Algoritmo de cifrado**.
4. Haga clic en **Exportar claves de cifrado del Servidor de administración**.
5. En la ventana **Exportar claves de cifrado**, realice lo siguiente:
   - Haga clic en el botón **Examinar** y especifique dónde desea guardar el archivo.
   - Especifique la contraseña para proteger el archivo contra el acceso no autorizado.

     Recuerde la contraseña. Una contraseña perdida no puede recuperarse. Si pierde la contraseña, debe repetir el procedimiento de exportación. Por lo tanto, escriba la contraseña en un papel y téngalo a mano.
6. Transmita el archivo a otro Servidor de administración, por ejemplo, a través de una carpeta compartida o unidad extraíble.
7. En el Servidor de administración de destino, asegúrese de que se esté ejecutando la Consola de administración de Kaspersky Security Center.
8. En el árbol de la consola del Servidor de administración, seleccione el Servidor de administración de destino donde desea transmitir las claves de cifrado.
9. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
10. En la ventana propiedades, seleccione la sección **Algoritmo de cifrado**.
11. Haga clic en **Importar claves de cifrado al Servidor de administración**.
12. En la ventana **Importar claves de cifrado**, realice lo siguiente:
    - Haga clic en el botón **Examinar** y seleccione el archivo que contiene las claves de cifrado.
    - Especifica la contraseña.
13. Haga clic en **Aceptar**.

Las claves de cifrado se transmiten al Servidor de administración de destino.

Repositorios de datos

Esta sección proporciona información sobre los datos almacenados en el Servidor de administración y se utiliza para realizar un seguimiento de la condición de los dispositivos cliente y ofrecerles un servicio de soporte.

La carpeta **Repositorios** del árbol de la consola muestra los datos usados para hacer un seguimiento de los estados de los dispositivos cliente.

La carpeta **Repositorios** contiene los siguientes objetos:

- Actualizaciones descargadas por el Servidor de administración que se distribuyen a los dispositivos cliente.
- Lista de equipos detectados en la red.
- Claves de licencia detectadas en dispositivos cliente.
- Archivos puestos por las aplicaciones de seguridad en las carpetas de Cuarentena de dispositivos.
- Archivos puestos en Copias de seguridad en dispositivos cliente.
- Los archivos cuyo análisis ha sido pospuesto por las aplicaciones de seguridad.

Exportación de una lista de objetos del repositorio a un archivo de texto

Se puede exportar una lista de objetos desde el repositorio a un archivo de texto.

Para exportar la lista de objetos desde el repositorio a un archivo de texto:

1. En el árbol de la consola, en la carpeta **Repositorios** seleccione la subcarpeta del repositorio correspondiente.
2. En la subcarpeta del repositorio, seleccione **Exportar lista** en el menú contextual.

   Se abrirá la ventana **Exportar lista**, donde podrá especificar el nombre del archivo de texto y la ruta de la carpeta donde esté ubicado.

Paquetes de instalación

Kaspersky Security Center traslada los paquetes de instalación de las aplicaciones de Kaspersky y de otros proveedores a los repositorios de datos.

Un *paquete de instalación* es un conjunto de archivos necesarios para instalar una aplicación. Un paquete de instalación contiene los parámetros de instalación y la configuración inicial de la aplicación que se está instalando.

Si desea instalar una aplicación en un dispositivo cliente, debe crear un paquete de instalación para la aplicación o utilizar uno existente. La lista de paquetes de instalación creados se almacena en la carpeta **Instalación remota** del árbol de consola, en la subcarpeta **Paquetes de instalación**.

Estados principales de los archivos del repositorio

Las aplicaciones de seguridad analizan archivos en dispositivos en busca de virus conocidos y otros programas que pueden plantear una amenaza, asignan estados a archivos y mueven algunos de ellos al repositorio.

Por ejemplo, las aplicaciones de seguridad pueden hacer lo siguiente:

- Guardar una copia de un archivo en el repositorio antes de eliminarlo
- Aislar archivos posiblemente infectados en el repositorio

Los estados principales de los archivos se presentan en la siguiente tabla. Puede obtener información más detallada sobre las medidas que debe tomar con los archivos en la Ayuda de las aplicaciones de seguridad correspondientes.

Estados de los archivos del repositorio

Nombre del estado	Descripción del estado
Infectado	El archivo tiene una sección de código de un virus conocido u otro malware cuya información se encuentra en las bases de datos antivirus de Kaspersky.
No infectado	No se ha detectado ningún virus conocido ni otro malware en el archivo.
Advertencia	El archivo contiene un fragmento de código que coincide parcialmente con un fragmento del código de una amenaza conocida.
Probablemente infectado	El archivo contiene código modificado de un virus conocido o código parecido a un virus que Kaspersky todavía desconoce.
Colocado en carpeta por el usuario	El usuario colocó manualmente el archivo en el repositorio porque el comportamiento del archivo dio lugar a sospechas de que contiene algunas amenazas. El usuario puede analizar el archivo en busca de amenazas usando bases de datos actualizadas.
Falso positivo	Una aplicación de Kaspersky asignó el estado Infectado a un archivo no infectado porque su código es parecido al de un virus. Después de un análisis con base de datos actualizadas, el archivo se identifica como no infectado.
Desinfectado	El archivo se desinfectó correctamente.
Eliminado	El archivo se eliminó durante el proceso.
Protegido con contraseña	El archivo no se puede procesar porque está protegido con una contraseña.

Activación de reglas en el modo Aprendizaje inteligente

Esta sección proporciona información sobre las detecciones realizadas por las reglas de Control de anomalías adaptativo en Kaspersky Endpoint Security para Windows en dispositivos cliente.

Las reglas detectan un comportamiento anómalo en los dispositivos cliente y pueden bloquearlo. Si las reglas funcionan en el modo Aprendizaje inteligente, detectan un comportamiento anómalo y envían informes sobre cada incidente al Servidor de administración de Kaspersky Security Center. Esta información se almacena como una lista en la subcarpeta **Activación de reglas en el estado Aprendizaje inteligente** de la carpeta **Repositorios**. Puede confirmar las detecciones como correctas o añadirlas como exclusiones, para que este tipo de comportamiento ya no se considere anómalo.

La información sobre las detecciones se almacena en el registro de eventos en el Servidor de administración (junto con otros eventos) y en el informe de Control de anomalías adaptativo.

Para obtener más información acerca del Control de anomalías adaptativo, las reglas, sus modos y estados, consulte la Ayuda de Kaspersky Endpoint Security para Windows.

Visualización de la lista de detecciones realizadas mediante las reglas de Control de anomalías adaptativo

Para ver la lista de detecciones realizadas por las reglas de Control de anomalías adaptativo:

1. En el árbol de la consola, seleccione el nodo del Servidor de administración que necesite.
2. Seleccione la subcarpeta **Activación de reglas en el estado Aprendizaje inteligente** (por defecto, esta es una subcarpeta de **Avanzado** → **Repositorios**).

   La lista muestra la siguiente información sobre las detecciones realizadas con las reglas de Control de anomalías adaptativo:

   - **Grupo de administración**

     El nombre del grupo de administración al que pertenece el dispositivo.

   - **Nombre del dispositivo**

     El nombre del dispositivo cliente donde se aplicó la regla.

   - **Nombre**

     El nombre de la regla que se aplicó.

   - **Estado**

     Exclusión: el nombre del dispositivo cliente donde se aplica la regla. Este estado permanece hasta la próxima sincronización del dispositivo cliente con el Servidor de administración; después de la sincronización, el elemento desaparece de la lista.

     Confirmación: si el Administrador procesara este elemento y lo confirmara. Este estado permanece hasta la próxima sincronización del dispositivo cliente con el Servidor de administración; después de la sincronización, el elemento desaparece de la lista.

     Vacío: si el administrador no procesó este elemento.

   - **Número de veces que fueron activadas las reglas**

     El número de detecciones dentro de una regla heurística, un proceso y un dispositivo cliente. Kaspersky Endpoint Security cuenta este número.

   - **Nombre de usuario**

El nombre del usuario del dispositivo cliente que ejecuta el proceso que generó la detección.

- **Ruta del proceso de origen**

  Ruta al proceso de origen, es decir, al proceso que realiza la acción (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del proceso de origen**

  SHA-256 hash del archivo de proceso de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de origen**

  Ruta al objeto que inició el proceso (para obtener más información, haga referencia a la ayuda de la Seguridad de Endpoint de Kaspersky).

- **Hash del objeto de origen**

  SHA-256 hash del archivo de origen (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del proceso de destino**

  Ruta al proceso de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del proceso de destino**

  SHA-256 hash del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Ruta del objeto de destino**

  Ruta al objeto de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Hash del objeto de destino**

  SHA-256 hash del archivo de destino (para obtener más información, consulte la ayuda de Kaspersky Endpoint Security).

- **Procesado**

  Fecha en la que se detectó la anomalía.

Para ver las propiedades de cada elemento de información:

1. En el árbol de la consola, seleccione el nodo del Servidor de administración que necesite.
2. Seleccione la subcarpeta **Activación de reglas en el estado Aprendizaje inteligente** (por defecto, esta es una subcarpeta de **Avanzado** → **Repositorios**).
3. En el espacio de trabajo **Activación de reglas en el estado Aprendizaje inteligente**, seleccione el objeto que desee.
4. Realice una de las siguientes acciones:
   - Haga clic en el enlace **Propiedades** en el cuadro de información que aparece en el lado derecho de la pantalla.
   - Haga clic derecho y en el menú contextual seleccione **Propiedades**.

   Se abre la ventana de propiedades del objeto, que muestra información sobre el elemento seleccionado.

Puede confirmar o añadir a las exclusiones cualquier elemento en la lista de detecciones de las reglas de Control de anomalías adaptativo

Para confirmar un elemento,

Seleccione un elemento (o varios elementos) en la lista de detecciones y haga clic en el botón **Confirmar**.

El estado de los elementos se cambiará a **Confirmando**.

Su confirmación contribuirá a las estadísticas utilizadas por las reglas (para obtener más información, consulte la Ayuda de Kaspersky Endpoint Security 11 para Windows).

Para añadir un elemento como una exclusión,

Haga clic con el botón derecho en un elemento (o varios elementos) en la lista de detecciones y seleccione **Añadir a exclusiones** en el menú contextual.

Se inicia el Asistente para añadir exclusiones. Siga las instrucciones del Asistente.

Si rechaza o confirma un elemento, será excluido de la lista de detecciones después de la próxima sincronización del dispositivo cliente con el Servidor de administración y ya no aparecerá en la lista.

Adición de exclusiones en las reglas de Control de anomalías adaptativo

El Asistente para añadir exclusiones le permite agregar exclusiones de las reglas de Control de anomalías adaptativo para Kaspersky Endpoint Security.

Puede iniciar el Asistente a través de uno de los tres siguientes procedimientos.

Para iniciar el Asistente para añadir exclusiones a través del nodo Control de anomalías adaptativo:

1. En el árbol de consola, seleccione el nodo del Servidor de administración requerido.

2. Seleccione **Activación de reglas en el estado Aprendizaje inteligente** (por defecto, esta es una subcarpeta de **Avanzado → Repositorios**).

3. En el espacio de trabajo, haga clic con el botón derecho en un elemento (o varios elementos) en la lista de detecciones y seleccione **Añadir a exclusiones** en el menú contextual.

   Puede añadir hasta 1000 exclusiones a la vez. Si selecciona más elementos e intenta añadirlos a exclusiones, se mostrará un mensaje de error.

Se inicia el Asistente para añadir exclusiones.

Puede iniciar el Asistente para añadir exclusiones desde otros nodos en el árbol de la consola:

- La ficha **Eventos** de la ventana principal del Servidor de administración (a continuación la opción **Solicitudes de los usuarios** o la opción **Eventos recientes**).
- **Informe sobre el estado de las reglas de Control de anomalías adaptativo**, columna **Recuento de detecciones**.

Paso 1. Selección de la aplicación

Este paso se puede omitir si solo tiene una versión de Kaspersky Endpoint Security para Windows y no tiene otras aplicaciones que admitan las reglas de Control de anomalías adaptativo.

El Asistente para añadir exclusiones muestra la lista de aplicaciones de Kaspersky cuyos complementos de administración le permiten agregar exclusiones a las directivas para estas aplicaciones. Seleccione una aplicación de esta lista y haga clic en **Siguiente** para proceder a seleccionar la directiva a la que se añadirá la exclusión.

Paso 2. La selección de la directiva (directivas)

El Asistente muestra la lista de directivas (con perfiles de directivas) para la Kaspersky Endpoint Security.

Seleccione todas las directivas y perfiles a los cuales desea agregar exclusiones y haga clic en **Siguiente**.

Paso 3. Procesamiento de la directiva (directivas)

El Asistente muestra una barra de progreso según se procesan las directivas. Puede interrumpir el procesamiento de las directivas haciendo clic en **Cancelar**.

Las directivas heredadas no se pueden actualizar. Si no tiene los derechos para modificar una directiva, esta directiva tampoco se actualizará.

Cuando todas las directivas se procesan (o si interrumpe el procesamiento), aparecerá un informe. Muestra qué directivas se actualizaron correctamente (icono verde) y qué directivas no se actualizaron (icono rojo).

Este es el último paso del Asistente. Haga clic **en Finalizar** para cerrar el Asistente.

Cuarentena y Copia de seguridad

Las aplicaciones antivirus de Kaspersky instaladas en dispositivos cliente pueden poner archivos en Cuarentena o Copia de seguridad durante el análisis del dispositivo.

Cuarentena es un repositorio especial que almacena archivos que probablemente están infectados con virus, así como los que no se pueden desinfectar en el momento de su detección.

El propósito de las *copias de seguridad* es almacenar copias de seguridad de los archivos que se han eliminado o modificado durante el proceso de desinfección.

Kaspersky Security Center crea una lista resumida de los archivos puestos en Cuarentena o en Copia de seguridad por la aplicación Kaspersky en los dispositivos. Los Agentes de red de los dispositivos cliente transfieren información acerca de los archivos en Cuarentena y Copia de seguridad al Servidor de administración. Puede usar la Consola de administración para ver las propiedades de los archivos en los repositorios de dispositivos cliente, ejecutar el análisis antivirus de estos repositorios y eliminar los archivos almacenados en ellos. Los iconos de los estados del archivo se describen en el apéndice.

Las funciones Cuarentena y Copia de seguridad son compatibles con las versiones 6.0 o posteriores de Kaspersky Anti-Virus for Windows Workstation y Kaspersky Anti-Virus for Windows Servers, así como con Kaspersky Endpoint Security 10 para Windows o versiones posteriores.

Kaspersky Security Center no copia archivos de los repositorios al Servidor de administración. Todos los archivos se guardan en los repositorios de los dispositivos. Puede restaurar un archivo solo en el dispositivo con la aplicación antivirus que colocó ese archivo en el repositorio.

Habilitación de la administración remota de archivos en los repositorios

De forma predeterminada, no se pueden administrar archivos ubicados en los repositorios de los dispositivos cliente.

Para habilitar la administración remota de los archivos almacenado en los repositorios de los dispositivos cliente:

1. En el árbol de consola, seleccione el grupo de administración para el que quiera habilitar la administración remota de archivos en el repositorio.
2. En el espacio de trabajo del grupo, abra la ficha **Directivas**.
3. En la ficha **Directivas** seleccione la directiva de la aplicación de seguridad que puso los archivos en los repositorios de los dispositivos cliente.
4. En la ventana de parámetros de las directivas, dentro del grupo de parámetros **Transferencia de datos al Servidor de administración**, seleccione las casillas de verificación correspondientes a los repositorios para los que se quiere habilitar la administración remota.

   La ubicación del grupo de parámetros **Transferencia de datos al Servidor de administración** dentro de la ventana de propiedades de directiva y los nombres de las casillas de verificación dependerán de la aplicación de seguridad que se esté usando.

Visualización de las propiedades de un archivo colocado en el repositorio

Para ver las propiedades de un archivo en Cuarentena o en Copia de seguridad:

1. En el árbol de consola, seleccione la carpeta **Repositorios**, la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**), seleccione el archivo del que quiera ver las propiedades.

3. Seleccionando **Propiedades** en el menú contextual del archivo.

Eliminar archivos de repositorios

Para eliminar un archivo de Cuarentena o Copia de seguridad:

1. En el árbol de la consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (o **Copia de seguridad**), seleccione los archivos que quiera eliminar con las teclas **Shift** y **Ctrl**.
3. Elimine los archivos por alguno de los siguientes medios:
   - Seleccionando **Eliminar** en el menú contextual de los archivos.
   - Haga clic en el enlace **Eliminar** (**Eliminar**) si quiere eliminar un archivo) en el cuadro de información de los archivos seleccionados.

Las aplicaciones de seguridad que pusieron los archivos en los repositorios de los dispositivos cliente los eliminarán.

Restauración de archivos desde los repositorios

Para restaurar un archivo de Cuarentena o Copia de seguridad:

1. En el árbol de consola, seleccione la carpeta **Repositorios**, la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**), seleccione los archivos que quiera restaurar con las teclas **Mayús** y **Ctrl**.
3. Inicie la restauración de los archivos por alguno de los medios siguientes:
   - Seleccionando **Restaurar** en el menú contextual de los archivos.
   - Haga clic en el enlace **Restaurar** en el cuadro de información de los archivos seleccionados.

Las aplicaciones de seguridad que pusieron los archivos en los repositorios de los dispositivos cliente los restaurarán a las carpetas de origen.

Almacenamiento de un archivo desde los repositorios al disco

Kaspersky Security Center le permite guardar en disco las copias de los archivos que la aplicación de seguridad puso en Cuarentena o en Copia de seguridad en un dispositivo cliente. Los archivos se copian en la carpeta especificada del dispositivo cliente que tenga instalado Kaspersky Security Center.

Para guardar en el disco duro una copia del archivo Cuarentena o Copia de seguridad:

1. En el árbol de consola, seleccione la carpeta **Repositorios**, la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**), seleccione el archivo que quiera copiar en el disco duro.

3. Inicie la copia por alguno de los medios siguientes:

   - Seleccionando **Guardar en disco** en el menú contextual del archivo.
   - Haga clic en el enlace **Guardar en disco** en el cuadro de información del archivo seleccionado.

La aplicación de seguridad que puso el archivo en Cuarentena en el dispositivo cliente guardará una copia del archivo en el disco duro.

Análisis de los archivos en Cuarentena

Para analizar los archivos en cuarentena:

1. En el árbol de consola, seleccione la carpeta **Repositorios**, la subcarpeta **Cuarentena**.
2. En el espacio de trabajo de la carpeta **Cuarentena**, seleccione los archivos que quiera analizar con las teclas **`Mayús`** y **`Ctrl`**.
3. Inicie el análisis de los archivos de una de las siguientes formas:

   - Seleccionando **Analizar** en el menú contextual del archivo.
   - Haga clic en el enlace **Analizar** en el cuadro de información de los archivos seleccionados.

   La aplicación ejecuta la tarea de análisis a petición para las aplicaciones de seguridad que han puesto los archivos seleccionados en cuarentena en los dispositivos cliente donde están almacenados esos archivos.

Amenazas activas

La información sobre los archivos no procesados encontrados en los dispositivos cliente se almacena en la carpeta **Repositorios**, en la subcarpeta **Amenazas activas**.

El procesamiento pospuesto y la desinfección son realizados por la aplicación de seguridad a petición o después de que un evento especificado ocurre. Se pueden configurar los procesos aplazados.

Desinfección de un archivo no procesado

Para iniciar la desinfección del archivo no procesado:

1. En el árbol de consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Amenazas activas**.
2. En el espacio de trabajo de la carpeta **Amenazas activas**, seleccione el archivo que quiera desinfectar.
3. Inicie la desinfección del archivo por alguno de los medios siguientes:

   - Seleccionando **Desinfectar** en el menú contextual del archivo.
   - Haga clic en el enlace **Desinfectar** en el cuadro de información del archivo seleccionado.

   A continuación, se realiza el intento de desinfección del archivo.

Si el archivo se ha desinfectado, la aplicación de seguridad instalada en el dispositivo cliente lo restaura a su carpeta de origen. El registro acerca del archivo se elimina de la lista de la carpeta **Amenazas activas**. Si el archivo no se puede desinfectar, la aplicación de seguridad instalada en el dispositivo lo elimina de ese dispositivo. El registro acerca del archivo se elimina de la lista de la carpeta **Amenazas activas**.

Almacenamiento en disco de un archivo no procesado

Kaspersky Security Center le permite guardar en disco las copias de los archivos no procesados encontrados en los dispositivos cliente. Los archivos se copian en la carpeta especificada del dispositivo cliente que tenga instalado Kaspersky Security Center. Puede descargar un archivo solo si está almacenado en el almacenamiento de copias de seguridad del dispositivo gestionado.

Para guardar en disco la copia de un archivo no procesado:

1. En el árbol de consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Amenazas activas**.
2. En el espacio de trabajo de la carpeta **Amenazas activas**, seleccione el archivo que quiera copiar al disco.
3. Inicie la copia por alguno de los medios siguientes:
   - Seleccionando **Guardar en disco** en el menú contextual del archivo.
   - Haga clic en el enlace **Guardar en disco** en el cuadro de información del archivo seleccionado.

La aplicación de seguridad instalada en el dispositivo cliente donde se encontró el archivo no procesado guardará una copia el archivo en la carpeta especificada.

Eliminación de archivos de la carpeta "Amenazas activas"

*Para eliminar un archivo de la carpeta **Amenazas activas**:*

1. En el árbol de consola, en la carpeta **Repositorios**, seleccione la subcarpeta **Amenazas activas**.
2. En el espacio de trabajo de la carpeta **Amenazas activas**, seleccione los archivos que quiera eliminar con las teclas **Mayús** y **Ctrl**.
3. Elimine los archivos por alguno de los siguientes medios:
   - Seleccionando **Eliminar** en el menú contextual de los archivos.
   - Haga clic en el enlace **Eliminar** (**Eliminar** si quiere eliminar un archivo) en el cuadro de información de los archivos seleccionados.

Las aplicaciones de seguridad que pusieron los archivos en los repositorios de los dispositivos cliente eliminarán los mismo archivos en aquellos repositorios. Los registros de los archivos se eliminan de la lista de la carpeta **Amenazas activas**.

Kaspersky Security Network (KSN)

Esta sección describe cómo utilizar la infraestructura de servicios en línea denominada Kaspersky Security Network (KSN). La sección proporciona información sobre KSN, así como instrucciones acerca de cómo habilitar KSN, configurar el acceso a KSN y consultar estadísticas de uso de KSN.

Acerca de KSN

Kaspersky Security Network (KSN) es una infraestructura de servicios en línea que proporciona acceso a la Base de conocimientos en línea de Kaspersky, donde hay información disponible sobre la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas de las aplicaciones Kaspersky a las amenazas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos. KSN permite utilizar las bases de datos de reputación de Kaspersky para obtener información sobre las aplicaciones instaladas en los dispositivos administrados.

Al participar en el programa KSN, acepta enviar automáticamente a Kaspersky información sobre el funcionamiento de las aplicaciones Kaspersky instaladas en los dispositivos cliente administrados por Kaspersky Security Center. La información se transfiere de acuerdo con la configuración de acceso de KSN actual.

La aplicación le solicita que se una a KSN durante la ejecución del Asistente de inicio rápido. Puede comenzar a utilizar KSN o dejar de hacerlo en cualquier momento que se encuentre utilizando la aplicación.

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si la Declaración de KSN se ha actualizado, se la muestra cuando actualiza o el Servidor de administración o pasa a una versión más nueva. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si la rechaza, seguirá usando KSN de acuerdo con la versión anterior de la Declaración de KSN que aceptó anteriormente.

Cuando KSN está activado, Kaspersky Security Center comprueba si se puede acceder a los servidores de KSN. Si no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza el DNS público. Esto es necesario para garantizar que se mantenga el nivel de seguridad de los dispositivos administrados.

Los dispositivos cliente administrados por el Servidor de administración interactúan con KSN mediante el proxy de KSN. El proxy KSN proporciona las funciones siguientes:

- Los dispositivos cliente pueden enviar consultas a KSN y transferir información a KSN aunque no dispongan de acceso directo a Internet.
- El Servidor proxy de KSN coloca en la memoria caché los datos procesados, de manera que se reduce la carga en el canal de salida, así como el tiempo de espera en las consultas de información realizadas por un dispositivo cliente.

Puede configurar el Servidor proxy de KSN en la sección **Proxy de KSN** de la ventana de propiedades del Servidor de administración.

Configuración del acceso a Kaspersky Security Network

Puede configurar el acceso a Kaspersky Security Network (KSN) en el Servidor de administración y en un punto de distribución.

Para configurar el acceso del Servidor de administración a Kaspersky Security Network (KSN):

1. En el árbol de consola, seleccione el Servidor de administración en el que deba configurar el acceso a KSN.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, en el panel **Secciones**, seleccione **Proxy de KSN → Configuración del proxy de KSN**.

4. En el espacio de trabajo, active la opción **Utilizar el Servidor de administración como servidor proxy** para usar el servicio de proxy de KSN.

   El Dato se envía desde dispositivos cliente a KSN de acuerdo con la directiva de seguridad de Kaspersky Endpoint que esté activa en esos dispositivos cliente. Si esta casilla está vacía, no se enviará ningún dato a KSN desde el Servidor de administración y los dispositivos cliente mediante Kaspersky Security Center. Sin embargo, los dispositivos cliente pueden enviar datos directamente a KSN (omitiendo Kaspersky Security Center), de conformidad con sus respectivas configuraciones. La directiva de Kaspersky Endpoint Security para Windows, que está activa en los dispositivos cliente determina qué datos enviarán directamente (omitiendo Kaspersky Security Center) dichos dispositivos a KSN.

5. Active la opción **Acepto usar Kaspersky Security Network**.

   Si activa esta opción, los dispositivos cliente enviarán resultados sobre la instalación de parches a Kaspersky. Antes de activar esta opción, asegúrese de leer y aceptar las condiciones de la Declaración de KSN.

   Si está utilizando KSN privada, active la opción **Configurar KSN privada** y haga clic en el botón **Seleccionar archivo con Proxy de KSN** para descargar la configuración de KSN privada (archivos con las extensiones pkcs7 y pem). Tras descargar la configuración, la interfaz muestra el nombre y los contactos del proveedor, así como la fecha de creación del archivo de configuración de la KSN privada.

   > Cuando habilite KSN privada, preste atención a los puntos de distribución configurados para enviar solicitudes de KSN directamente a Cloud KSN. Los puntos de distribución que tengan instalado el Agente de red versión 11 (o versiones anteriores) continuarán enviando solicitudes KSN a Cloud KSN. Para reconfigurar los puntos de distribución para enviar solicitudes KSN a KSN privada, active la opción **Reenviar solicitudes de KSN al Servidor de administración** para cada punto de distribución. Puede activar esta opción en las propiedades del punto de distribución o en la directiva del Agente de red.

   Cuando selecciona la casilla de verificación **Configurar KSN privada**, aparece un mensaje con los detalles sobre la KSN privada.

   Las siguientes aplicaciones Kaspersky admiten KSN privada:

   - Kaspersky Security Center 10 Service Pack 1 o posterior
   - Kaspersky Endpoint Security 10 Service Pack 1 para Windows o posterior
   - Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
   - Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

   Si activa la opción **Configurar KSN privada** en Kaspersky Security Center, estas aplicaciones reciben información sobre la admisión de la KSN privada. En la ventana de configuración de la aplicación, en la subsección **Kaspersky Security Network** de la sección **Protección contra amenazas avanzada**, se muestra **proveedor de KSN: KSN privada**. De lo contrario, se muestra **proveedor de KSN: KSN Global**.

   > Si utiliza versiones de aplicaciones anteriores a Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 o una anteriores a Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent cuando ejecuta KSN privada, le recomendamos que utilice Servidores de administración secundarios que no tengan habilitado el uso de KSN privada.

   > Kaspersky Security Center no envía ningún dato estadístico a Kaspersky Security Network si se configura la KSN privada en la sección **Proxy de KSN → Configuración del proxy de KSN** de la ventana de propiedades del Servidor de administración.

Si tiene la configuración del servidor proxy configurada en las propiedades del Servidor de administración pero su arquitectura de red requiere que su KSN privada active directamente la opción **Ignorar la configuración del servidor proxy al conectarse a KSN privada**. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a la KSN privada.

6. Configure la conexión del Servidor de administración al servicio de proxy de KSN:

   - Bajo **Configuración de la conexión**, para el **Puerto TCP**, especifique el número de puerto TCP que se debe usar para conectarse al Servidor proxy de KSN. El puerto predeterminado de conexión al Servidor proxy de KSN es 13111.

   - Si desea que el Servidor de administración se conecte al Servidor proxy de KSN mediante un puerto UDP, active la opción **Utilizar puerto UDP** y especifique un número de puerto para el **Puerto UDP**. De forma predeterminada, esta opción está desactivada y se utiliza el puerto TCP. Si esta opción está habilitada, el puerto UDP predeterminado de conexión al Servidor proxy de KSN será 15111.

7. Active la opción **Conectar Servidores de administración secundarios a KSN mediante el Servidor de administración principal**.

   Si se activa esta opción, los Servidores de administración secundarios usarán el Servidor de administración principal como Servidor proxy de KSN. Si se desactiva esta opción, los Servidores de administración secundarios se conectarán a KSN por su propia cuenta. En este caso, los dispositivos administrados usarán los Servidores de administración secundarios como Servidores proxy de KSN.

   > Los Servidores de administración secundarios usarán el Servidor de administración principal como servidor proxy si en el panel derecho de la sección **Configuración del proxy de KSN** en las propiedades de los Servidores de administración secundarios tiene seleccionada la casilla **Utilizar el Servidor de administración como servidor proxy**.

8. Haga clic en **Aceptar**.

Se guarda la configuración de acceso a KSN.

También puede configurar el acceso de puntos de distribución a KSN, por ejemplo, si desea reducir la carga sobre el Servidor de administración. El punto de distribución que actúa como Servidor proxy de KSN envía las solicitudes de KSN directamente a Kaspersky desde los dispositivos administrados, sin utilizar el Servidor de administración.

Para configurar el acceso del punto de distribución a Kaspersky Security Network (KSN):

1. Asegúrese que el punto de distribución se asigne manualmente.

2. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.

3. Seleccione **Propiedades** en el menú contextual del Servidor de administración.

4. En la ventana de propiedades del Servidor de administración, seleccione la sección **Puntos de distribución**.

5. Seleccione el punto de distribución en la lista y haga clic en el botón **Propiedades** para abrir su ventana de propiedades.

6. En la ventana de propiedades del punto de distribución, en la sección **KSN Proxy**, seleccione **Acceder a la nube de KSN directamente a través de Internet**.

7. Haga clic en **Aceptar**.

El punto de distribución actuará como un Servidor proxy de KSN.

Habilitación y deshabilitación de KSN

Para habilitar KSN, siga estos pasos:

1. En el árbol de consola, seleccione el Servidor de administración para el que debe habilitar KSN.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, en la sección **Proxy de KSN**, seleccione la subsección **Configuración del proxy de KSN**.
4. Seleccione el **Utilizar el Servidor de administración como servidor proxy**.

   Se habilita el Servidor proxy de KSN.
5. Selecciona la casilla de verificación **Acepto usar Kaspersky Security Network**.

   Se habilita KSN.

   Si se selecciona esta casilla, los dispositivos cliente enviarán resultados sobre la instalación de parches a Kaspersky. Antes de seleccionar esta casilla, debe leer y aceptar las condiciones de la Declaración de KSN.
6. Haga clic en **Aceptar**.

Para deshabilitar KSN, siga estos pasos:

1. En el árbol de consola, seleccione el Servidor de administración para el que debe habilitar KSN.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana de propiedades del Servidor de administración, en la sección **Proxy de KSN**, seleccione la subsección **Configuración del proxy de KSN**.
4. Desmarque las casillas de verificación **Utilizar el Servidor de administración como servidor proxy** o **Acepto usar Kaspersky Security Network** para deshabilitar el proxy de KSN.

   Si esta casilla está vacía, los dispositivos cliente no enviarán resultados de la instalación de parches a Kaspersky.

   Si está utilizando KSN privada, desmarque la casilla de verificación **Configurar KSN privada**.

   Se deshabilita KSN.
5. Haga clic en **Aceptar**.

Ver la declaración de KSN aceptada

Cuando habilita Kaspersky Security Network (KSN), debe leer y aceptar la Declaración de KSN. Puede ver la declaración de KSN aceptada en cualquier momento.

Para ver la declaración de KSN aceptada:

1. En el árbol de consola, seleccione el Servidor de administración para el que ha habilitado KSN.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.

3. En la ventana de propiedades del Servidor de administración, en la sección **Proxy de KSN**, seleccione la subsección **Configuración del proxy de KSN**.

4. Haga clic en el enlace **Ver Declaración de KSN aceptada**.

   En la ventana que se abre, puede ver el texto de la Declaración de KSN aceptada.

Visualización de estadísticas del Servidor proxy de KSN

El *Servidor proxy de KSN* es un servicio que asegura la interacción entre la infraestructura de Kaspersky Security Network y los dispositivos cliente administrados por un Servidor de administración.

Usar un Servidor proxy de KSN proporciona las funciones siguientes:

- Los dispositivos cliente pueden enviar consultas a KSN y transferir información a KSN aunque no dispongan de acceso directo a Internet.
- El Servidor proxy de KSN coloca en la memoria caché los datos procesados, de manera que se reduce la carga en el canal de salida, así como el tiempo de espera en las consultas de información realizadas por un dispositivo cliente.

En la ventana de propiedades del Servidor de administración, puede configurar el Servidor proxy de KSN y ver estadísticas sobre su uso.

Para ver las estadísticas del Servidor proxy de KSN, siga estos pasos:

1. En el árbol de consola, seleccione el Servidor de administración del que desee consultar las estadísticas de KSN.

2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.

3. En la ventana de propiedades del Servidor de administración, en la sección **Proxy de KSN**, seleccione la subsección **Estadísticas del proxy de KSN**.

   Esta sección muestra las estadísticas del funcionamiento del Servidor proxy de KSN. Si es necesario, realice estas acciones adicionales:

   - Haga clic en **Actualizar** para actualizar las estadísticas sobre el uso del Servidor proxy de KSN.
   - Haga clic en el botón **Exportar a archivo** para exportar las estadísticas a un archivo CSV.
   - Haga clic en el botón **Comprobar conexión de KSN** para comprobar si el Servidor de administración está conectado a KSN.

4. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

Aceptación de una declaración de KSN actualizada

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si la Declaración de KSN se ha actualizado, se la muestra cuando actualiza o el Servidor de administración o pasa a una versión más nueva. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si lo rechaza, sigue utilizando KSN de acuerdo con la versión de la declaración de KSN que aceptó anteriormente.

Después de actualizar o pasar a una nueva versión del Servidor de Administración, la Declaración de KSN actualizada se muestra automáticamente. Si rechaza la Declaración de KSN actualizada, aún puede verla y aceptarla más tarde.

Para ver y luego aceptar o rechazar una Declaración de KSN actualizada:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. En la pestaña **Supervisión**, en la sección **Supervisión**, haga clic en el enlace **La Declaración de Kaspersky Security Network es obsoleta**.

   Se abre la ventana de la **Declaración de KSN**.
3. Lea atentamente la Declaración de KSN y luego tome una decisión. Si acepta la declaración de KSN actualizada, haga clic en el botón **Acepto los términos del Contrato de licencia**. Si rechaza la Declaración de KSN actualizada, haga clic en el botón **Cancelar**.

Dependiendo de su elección, KSN sigue funcionando de acuerdo con los términos de la Declaración de KSN actual o actualizada. Usted puede ver el texto de la declaración de KSN aceptada en las propiedades del Servidor de administración en cualquier momento.

Protección mejorada con Kaspersky Security Network

Kaspersky ofrece a los usuarios una capa adicional de protección a través de Kaspersky Security Network. Este método de la protección está diseñado para combatir amenazas persistentes avanzadas y ataques de día cero. Las tecnologías en la nube integradas y los conocimientos de los analistas de virus de Kaspersky convierten Kaspersky Endpoint Security en la opción sin paralelos para la protección contra las amenazas de red más sofisticadas.

Los detalles sobre la protección mejorada de Kaspersky Endpoint Security están disponibles en el sitio web de Kaspersky.

Comprobar si el punto de distribución funciona como KSN Proxy

En un dispositivo administrado asignado para funcionar como punto de distribución, puede habilitar KSN Proxy. Un dispositivo administrado funciona como KSN Proxy cuando el servicio ksnproxy se está ejecutando en el dispositivo. Puede verificar, activar o desactivar este servicio de forma local en el dispositivo.

Para comprobar si el punto de distribución funciona como proxy KSN:

1. En el dispositivo que funciona como punto de distribución, en Windows, abra **Servicios** (**Todos los programas** → **Herramientas administrativas** → **Servicios**).
2. En la lista de servicios, verifique si el servicio ksnproxy se está ejecutando.

   Si el servicio ksnproxy se está ejecutando, entonces el Agente de red en el dispositivo participa en Kaspersky Security Network y funciona como KSN Proxy para los dispositivos administrados incluidos en el alcance del punto de distribución.

Si lo desea, puede desactivar el servicio ksnproxy. En este caso, el Agente de red en el punto de distribución deja de participar en Kaspersky Security Network. Esto requiere derechos de administrador local.

Alternar entre la Ayuda en línea y la Ayuda sin conexión

Si no tiene acceso a Internet, puede utilizar la Ayuda sin conexión.

Para cambiar entre la Ayuda en línea y la Ayuda sin conexión:

1. En la ventana principal de Kaspersky Security Center, en el árbol de la consola, seleccione **Kaspersky Security Center 14**.
2. Haga clic en el enlace **Configuración de interfaz global**.

   Se abre la ventana de configuración.
3. En la ventana de configuración, haga clic en **Usar la Ayuda sin conexión**.
4. Haga clic en **Aceptar**.

La configuración se aplica y se guarda. Si lo desea, puede volver a cambiar la configuración en cualquier momento y comenzar a utilizar la Ayuda en línea en cualquier momento.

Exportación de eventos a sistemas SIEM

Esta sección explica cómo exportar eventos registrados por Kaspersky Security Center a sistemas de Security Information and Event Management (SIEM) externos.

Configuración de la exportación de eventos a sistemas SIEM

Kaspersky Security Center permite la configuración mediante uno de los siguientes métodos: exportar a cualquier sistema SIEM que utilice formato Syslog, exportar a QRadar, Splunk, ArcSight sistemas SIEM que utilizan formatos LEEF y CEF o exportar eventos a sistemas SIEM directamente desde la base de datos de Kaspersky Security Center. Cuando completa este escenario, el Servidor de administración envía automáticamente eventos al sistema SIEM.

Requisitos previos

Antes de iniciar la exportación de la configuración de eventos en Kaspersky Security Center:

- Obtenga más información sobre los métodos de exportación de eventos.
- Asegúrese de contar con los valores de la configuración del sistema.

Puede realizar los pasos de este escenario en cualquier orden.

El proceso de exportación de eventos al sistema SIEM consta de las siguientes etapas:

- **Configuración del sistema SIEM para recibir eventos de Kaspersky Security Center**

  Instrucciones prácticas: Configurar la exportación de eventos en un sistema SIEM

- **Seleccionar eventos que desea exportar al sistema SIEM:**

  Instrucciones:

  - Consola de administración: Marcar eventos de una aplicación de Kaspersky para exportar en formato Syslog, Marcar eventos generales para exportar en formato Syslog
  - Kaspersky Security Center 14 Web Console: Marcado de eventos de una aplicación de Kaspersky para exportar en formato Syslog, Marcado de eventos generales para exportar en formato Syslog

- **Configuración de la exportación de eventos al sistema SIEM utilizando uno de los siguientes métodos:**

  - Utilizando los protocolos TCP/IP, UDP o TLS sobre TCP.

    Instrucciones:

    - Consola de administración: Configurar la exportación de eventos a sistemas SIEM
    - Kaspersky Security Center 14 Web Console: Configuración de la exportación de eventos a sistemas SIEM

  - Usando la exportación de eventos directamente desde la base de datos de Kaspersky Security Center (Se proporciona un conjunto de vistas públicas en la base de datos de Kaspersky Security Center; puede encontrar la descripción de estas vistas públicas en el documento klakdb.chm).

Resultados

Después de configurar la exportación de eventos al sistema SIEM, puede ver los resultados de la exportación si seleccionó los eventos que desea exportar.

Antes de empezar

Al configurar la exportación automática de eventos en Kaspersky Security Center, debe especificar ciertos parámetros de la configuración del sistema SIEM. Se recomienda que compruebe esta configuración de antemano a fin de prepararse para configurar Kaspersky Security Center.

Para configurar correctamente el envío automático de eventos a un sistema SIEM, debe conocer los siguientes ajustes:

- **Dirección del servidor del sistema SIEM**

  La dirección IP del servidor en el que está instalado el sistema SIEM actualmente en uso. Compruebe este valor en su configuración del sistema SIEM.

- **Puerto del servidor del sistema SIEM**

  El número de puerto usado para establecer una conexión entre Kaspersky Security Center y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del receptor de su sistema SIEM.

- **Protocolo**

Protocolo usado para transferir mensajes desde Kaspersky Security Center a su sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del receptor de su sistema SIEM.

Acerca de los eventos en Kaspersky Security Center

Kaspersky Security Center le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre eventos se guarda en la base de datos del Servidor de administración. Puede exportar esta información a sistemas SIEM externos. La exportación de la información de eventos a sistemas SIEM externos permite a los administradores de sistemas SIEM responder lo antes posible a eventos del sistema de seguridad que ocurren en dispositivos administrados o grupos de dispositivos.

En Kaspersky Security Center existen los siguientes tipos de eventos:

- Eventos generales. Estos eventos ocurren en todas las aplicaciones de Kaspersky administradas. Por ejemplo, FBrote de virus es un evento general. Los eventos generales tienen una sintaxis y semántica definidas estrictamente. Los eventos generales se utilizan, por ejemplo, en informes y paneles.

- Eventos específicos de aplicaciones de Kaspersky administradas. Cada aplicación de Kaspersky administrada tiene su propio conjunto de eventos.

Cada evento tiene su propio nivel de importancia. Según las condiciones en que se produzca, un evento se puede asignar varios niveles de importancia. Existen cuatro niveles de importancia de eventos:

- Un *evento crítico* es un evento que indica que se ha producido un problema crítico que puede llevar a la pérdida de datos, un funcionamiento defectuoso o un error crítico.

- Un *fallo operativo* es un evento que indica que se ha producido un grave problema, un error o un funcionamiento defectuoso que ocurrió durante el funcionamiento de la aplicación o al realizar un procedimiento.

- Una *advertencia* es un evento que no es necesariamente grave, pero también indica un problema posible en el futuro. La mayor parte de los eventos se designan como advertencias si la aplicación se puede restaurar sin la pérdida de datos o capacidades funcionales después de que tales eventos ocurran.

- Un evento *de información* es un evento que se produce para informar sobre la finalización correcta de una operación, el correcto funcionamiento de la aplicación o la finalización de un procedimiento.

Cada evento tiene un plazo de almacenamiento definido, durante el cual puede verlo o modificarlo en Kaspersky Security Center. Algunos eventos no se guardan en la base de datos del Servidor de administración de forma predeterminada porque su plazo de almacenamiento definido es el cero. Solo los eventos que se almacenarán en la base de datos del Servidor de administración durante al menos un día se pueden exportar a sistemas externos.

Sobre exportación de eventos

Puede utilizar la exportación de eventos en sistemas centralizados que tratan con problemas de seguridad a un nivel organizativo y técnico, proporcionan servicios de supervisión de la seguridad y unifican la información de soluciones diferentes. Estos son sistemas de SIEM, que proporcionan análisis en tiempo real de alertas de seguridad y eventos generados por el hardware de la red y las aplicaciones o Centros operativos de seguridad (SOCs).

Estos sistemas reciben datos desde muchas fuentes, redes incluidas, seguridad, servidores, bases de datos y aplicaciones. Los sistemas SIEM también proporcionan funcionalidad para consolidar datos supervisados a fin de ayudarle a evitar omitir eventos críticos. Además, los sistemas realizan análisis automatizados de eventos correlacionados y alertas a fin de notificar a los administradores sobre problemas de seguridad inmediatos. La generación de alertas se puede implementar a través de un panel o se puede enviar a través de canales de terceros, como el correo electrónico.

El proceso de exportar eventos desde Kaspersky Security Center a sistemas SIEM externos involucra a dos partes: un remitente del evento, Kaspersky Security Center, y un destinatario del evento, un sistema SIEM. Para exportar eventos correctamente, debe configurar estos parámetros en su sistema de SIEM y en la Consola de administración de Kaspersky Security Center. No importa qué componente configura primero. Puede configurar la transmisión de eventos desde Kaspersky Security Center y, a continuación, configurar la recepción de eventos por parte del sistema SIEM o viceversa.

Métodos para enviar eventos desde Kaspersky Security Center

Hay tres métodos para enviar eventos desde Kaspersky Security Center a sistemas externos:

- El envío de eventos con el protocolo de Syslog a cualquier sistema SIEM

  Usando el protocolo de Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración de Kaspersky Security Center y las aplicaciones de Kaspersky instaladas en dispositivos administrados. El protocolo Syslog es un protocolo de registros de mensajes estándar. Puede utilizarlo para exportar eventos a cualquier sistema SIEM.

  Para ello, debe marcar los eventos que desea transmitir al sistema SIEM. Puede marcar los eventos en la Consola de administración o en Kaspersky Security Center 14 Web Console. Solo los eventos marcados se transmitirán al sistema SIEM. Si no marcó nada, no se retransmitirá ningún evento.

- Enviando eventos sobre protocolos CEF y LEEF a sistemas QRadar, Splunk y ArcSight

  Puede utilizar los protocolos CEF y LEEF para exportar eventos generales. Al exportar eventos en protocolos CEF y LEEF, no tiene la capacidad de seleccionar eventos específicos que exportar. En cambio, todos los eventos generales se exportan. A diferencia del protocolo Syslog, los protocolos CEF y LEEF no son universales. CEF y LEEF están diseñados para los sistemas SIEM apropiados (QRadar, Splunk y ArcSight). Por lo tanto, cuando elige exportar eventos sobre uno de estos protocolos, usa el analizador requerido en el sistema SIEM.

  > Para exportar eventos a través de los protocolos CEF y LEEF, la función Integración con los sistemas SIEM debe activarse en el Servidor de administración utilizando una clave de licencia activa o un código de activación válido.

- Directamente desde la base de datos de Kaspersky Security Center a cualquier sistema SIEM.

  Este método de exportar eventos puede utilizarse para recibir eventos directamente de vistas públicas de la base de datos mediante consultas de SQL. Los resultados de una consulta se guardan a un archivo XML que se puede utilizar como datos de entrada para un sistema externo. Solo los eventos disponibles en vistas públicas se pueden exportar directamente desde la base de datos.

Recepción de eventos por el sistema SIEM

El sistema SIEM debe recibir y analizar correctamente los eventos recibidos desde Kaspersky Security Center. Con estos objetivos, debe configurar correctamente el sistema SIEM. La configuración depende del sistema SIEM específico utilizado. No obstante, hay varios pasos generales en la configuración de todos los sistemas SIEM, por ejemplo, configurando el receptor y el analizador.

Acerca de la configuración de la exportación de eventos en un sistema SIEM

El proceso de exportar eventos desde Kaspersky Security Center a sistemas SIEM externos involucra a dos partes: un remitente del evento – Kaspersky Security Center y un destinatario del evento – sistema SIEM. Debe configurar la exportación de eventos en su sistema SIEM y en Kaspersky Security Center.

La configuración que especifica en el sistema SIEM dependerá del sistema que usted esté usando. Generalmente, para todos los sistemas SIEM debe configurar un receptor y, opcionalmente, un analizador sintáctico del mensaje para analizar los eventos recibidos.

Configuración del receptor

Para poder recibir los eventos enviados por Kaspersky Security Center, debe configurar el receptor en su sistema SIEM. En general, la configuración siguiente se debe especificar en el sistema SIEM:

- **Protocolo de exportación o tipo de entrada**

  Es el protocolo de transferencia del mensaje, TCP/IP o UDP. Este protocolo debe ser el mismo que el protocolo que especificó en Kaspersky Security Center.

- **Puerto**

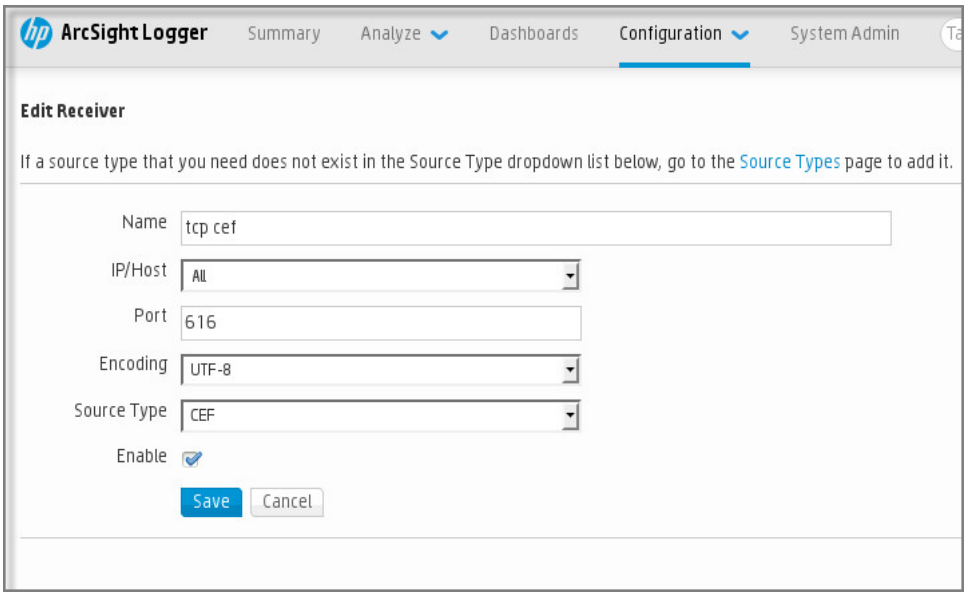
  Número de puerto para conectar con Kaspersky Security Center. Este puerto debe ser igual que el puerto que especificó en Kaspersky Security Center.

- **Protocolo del mensaje o tipo de la fuente**

  El protocolo utilizado para exportar eventos al sistema SIEM. Puede ser uno de los protocolos estándar: Syslog, CEF o LEEF. El sistema SIEM selecciona el analizador sintáctico del mensaje según el protocolo que especifica.

Según el sistema SIEM que utilice, es posible que deba especificar la configuración del receptor adicional.

La cifra siguiente muestra la pantalla de instalación del receptor en ArcSight.



Instalación del receptor en ArcSight

Analizador sintáctico del mensaje

Los eventos de Exportar se transfieren a sistemas SIEM como mensajes. Estos mensajes se deben analizar correctamente de modo que la información sobre los eventos se pueda utilizar por el sistema SIEM. Los analizadores sintácticos de los mensajes son una parte del sistema SIEM; se utilizan para dividir los contenidos del mensaje en los campos relevantes, como ID del evento, gravedad, descripción, parámetros, etc. Esto permite al sistema SIEM procesar eventos recibidos de Kaspersky Security Center de modo que se puedan almacenar en la base de datos del sistema SIEM.

Cada sistema SIEM tiene un conjunto de analizadores de mensajes estándar. Kaspersky también proporciona analizadores de mensajes para algunos sistemas SIEM, por ejemplo, para QRadar y ArcSight. Puede descargar estos analizadores de mensajes de los sitios web de los sistemas SIEM correspondientes. Al configurar el receptor, puede seleccionar utilizar uno de los analizadores de mensajes estándar o un analizador de mensajes de Kaspersky.

Marcado de eventos para exportar a sistemas SIEM en formato Syslog

Esta sección describe cómo marcar eventos para su posterior exportación a sistemas SIEM en formato Syslog.

Acerca del marcado de eventos para exportar al sistema SIEM en formato Syslog

Después de activar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM externo.

Puede configurar la exportación de eventos en formato Syslog a un sistema externo según una de las condiciones siguientes:

- Marcado de eventos generales. Si marca los eventos para exportar en una directiva, en la configuración de un evento, o en la configuración del Servidor de administración, el sistema SIEM recibirá los eventos marcados que se produjeron en todas las aplicaciones administradas por la directiva específica. Si los eventos exportados se seleccionaran en la directiva, no podrá redefinirlos para una aplicación particular administrada por esta directiva.

- Marcado de eventos para una aplicación administrada. Si marca eventos para exportar para una aplicación administrada instalada en un dispositivo administrado, el sistema SIEM solo recibirá los eventos que hayan ocurrido en esta aplicación.

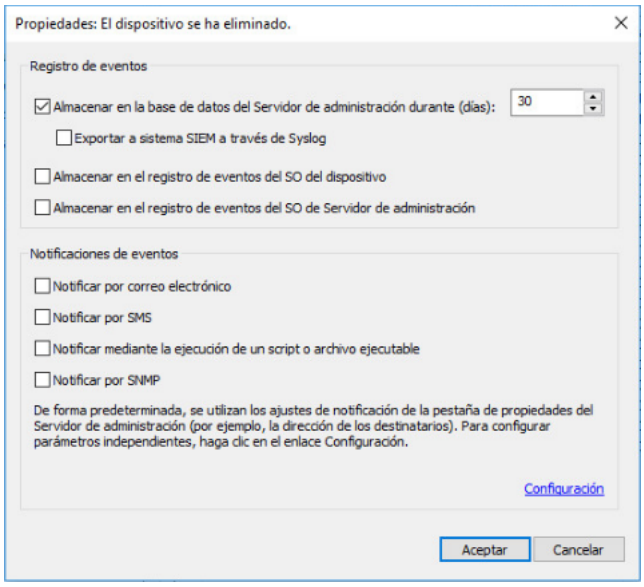
Marcar eventos de una aplicación de Kaspersky para exportar en formato Syslog

Si desea exportar los eventos que hayan ocurrido en una aplicación administrada individual y que estén instalados en un dispositivo administrado, márquelos en la aplicación. Si los eventos anteriormente exportados estaban marcados en la directiva, no podrá redefinir los eventos marcados para una aplicación particular administrada por esta directiva.

Para marcar los eventos que desea exportar para una aplicación individual:

1. En el árbol de consola de Kaspersky Security Center, seleccione el nodo **Dispositivos administrados** y vaya a la ficha **Dispositivos**.
2. Haga clic con el botón derecho del ratón para abrir el menú contextual del dispositivo relevante y seleccione **Propiedades**.
3. En la ventana de propiedades del dispositivo que se abre, seleccione la sección **Aplicaciones**.
4. En la lista de aplicaciones que aparece, seleccione la aplicación cuyos eventos tiene que exportar y haga clic en el botón **Propiedades**.
5. En la ventana propiedades de la aplicación, seleccione la sección **Configuración de eventos**.
6. En la lista de eventos que aparece, seleccione uno o varios eventos que se tienen que exportar al sistema SIEM, y haga clic en el botón **Propiedades**.
7. En la ventana de propiedades del evento que aparece, seleccione la casilla de verificación **Exportar a sistema SIEM a través de Syslog** para marcar los eventos seleccionados para exportarlos en formato Syslog. Limpie la casilla de verificación **Exportar a sistema SIEM a través de Syslog** para desmarcar los eventos seleccionados para exportar en formato Syslog.

   Si las propiedades del evento están definidas en una directiva, los campos de esta ventana no se pueden modificar.



Ventana de Propiedades de eventos

8. Haga clic en **Aceptar** para guardar los cambios.

9. Haga clic **Aceptar** en la ventana de propiedades de la aplicación y en la ventana de propiedades del dispositivo.

Los eventos marcados se enviarán al sistema SIEM con el protocolo de Syslog. Los eventos cuyas en casillas de verificación haya desactivado **Exportar a sistema SIEM a través de Syslog**, no se exportarán a un sistema SIEM. La exportación comenzará inmediatamente después de que active la exportación automática y seleccione los eventos que exportar. Configure el sistema SIEM para asegurarse de que pueda recibir eventos de Kaspersky Security Center.

Marcar eventos generales para exportar en formato Syslog

Si desea exportar eventos que ocurrieron en todas las aplicaciones administradas por una directiva específica, marque los eventos para exportar en la directiva. En este caso, no puede marcar eventos para una aplicación administrada individual.

Para marcar eventos generales para exportar a un sistema SIEM:

1. En el árbol de consola de Kaspersky Security Center, seleccione el nodo **Directivas**.

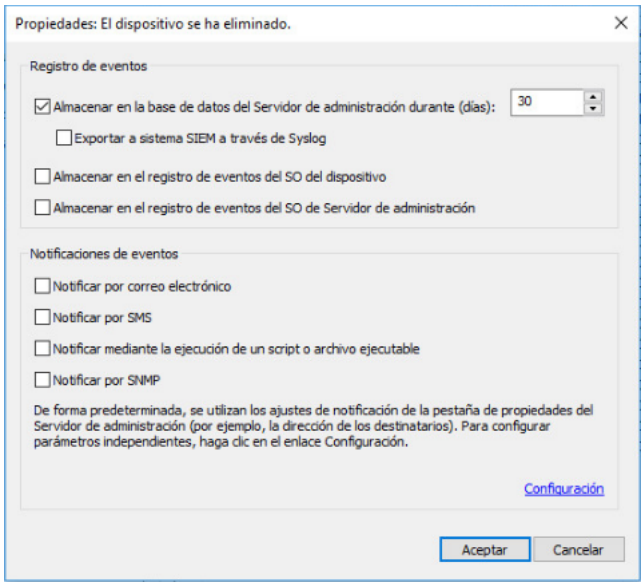
2. Haga clic con el botón derecho del ratón para abrir el menú contextual de la directiva relevante y seleccione **Propiedades**.

3. En la ventana de propiedades de la directiva abierta, seleccione la sección **Configuración de eventos**.

4. En la lista de eventos que aparece, seleccione uno o varios eventos que se tienen que exportar al sistema SIEM, y haga clic en el botón **Propiedades**.

   Si tiene que seleccionar todos los eventos, haga clic en el botón **Seleccionar todo**.

5. En la ventana de propiedades del evento que aparece, seleccione la casilla de verificación **Exportar a sistema SIEM a través de Syslog** para marcar los eventos seleccionados para exportarlos en formato Syslog. Limpie la casilla de verificación **Exportar a sistema SIEM a través de Syslog** para desmarcar los eventos seleccionados para exportar en formato Syslog.



Ventana de propiedades de eventos del Servidor de administración

6. Haga clic en **Aceptar** para guardar los cambios.

7. En la ventana de propiedades de la directiva, haga clic en **Aceptar**.

Los eventos marcados se enviarán al sistema SIEM con el protocolo de Syslog. Los eventos cuyas en casillas de verificación haya desactivado **Exportar a sistema SIEM a través de Syslog**, no se exportarán a un sistema SIEM. La exportación comenzará inmediatamente después de que active la exportación automática y seleccione los eventos que exportar. Configure el sistema SIEM para asegurarse de que pueda recibir eventos de Kaspersky Security Center.

Acerca de la exportación de eventos mediante el formato Syslog

Puede utilizar el formato Syslog para exportar a sistemas SIEM los eventos que se producen en el Servidor de administración y otras aplicaciones de Kaspersky instaladas en dispositivos administrados.

Syslog es un estándar para el protocolo de registro de mensajes. Permite la separación del software que genera mensajes, el sistema que los almacena y el software que los notifica y los analiza. Cada mensaje se etiqueta mediante un código, indicando el tipo del software que genera el mensaje y se le asigna un nivel de gravedad.

El formato Syslog se define por los documentos Request for Comments (RFC) publicados por el Internet Engineering Task Force (estándares de Internet). El estándar RFC 5424 se utiliza para exportar los eventos desde Kaspersky Security Center a sistemas externos.

En Kaspersky Security Center, puede usar el protocolo de Syslog para configurar la exportación de los eventos a sistemas externos.

El proceso de exportación consiste en dos pasos:

1. La activación de la exportación de evento automática. En este paso, Kaspersky Security Center se configura de modo que envíe eventos al sistema SIEM. Kaspersky Security Center empieza a enviar eventos inmediatamente después de que usted active la exportación automática.

2. La selección de los eventos que exportar al sistema externo. En este paso, usted selecciona qué evento exportar al sistema SIEM.

Acerca de la exportación de mediante los protocolos CEF y LEEF

Puede utilizar los formatos CEF y LEEF para exportar eventos generales a los sistemas SIEM, como así también eventos que las aplicaciones de Kaspersky transfieren al Servidor de administración. El conjunto de eventos de exportación está predefinido, y no puede seleccionar los eventos que exportarse.

Para exportar eventos a través de los protocolos CEF y LEEF, la función Integración con los sistemas SIEM debe activarse en el Servidor de administración utilizando una clave de licencia activa o un código de activación válido.

Seleccione el formato de exportación que corresponda al sistema SIEM utilizado. La tabla a continuación muestra sistemas SIEM y los formatos de exportación correspondientes.

Formatos de exportación de eventos a un sistema SIEM

Sistema SIEM	Formato de exportación
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - es un formato de evento personalizado para IBM Security QRadar SIEM. QRadar puede integrar, identificar y procesar eventos LEEF. Los eventos LEEF deben usar la codificación de caracteres UTF-8. Puede encontrar información detallada sobre el protocolo LEEF en IBM Knowledge Center.

- CEF (Common Event Format): un estándar de administración de registros abierto que mejora el interoperabilidad de la información relacionada con la seguridad desde dispositivos y aplicaciones de seguridad y red diferentes. CEF le permite usar un formato de registros de eventos común de modo que los datos se puedan integrar y añadir fácilmente para que un sistema de administración de la empresa los analice.

La exportación automática significa que Kaspersky Security Center envía eventos generales al sistema SIEM. La exportación automática de eventos comienza inmediatamente después de que se activa. Esta sección explica detalladamente cómo activar la exportación automática de eventos.

Configuración de Kaspersky Security Center para la exportación de eventos a un sistema SIEM

Puede activar la exportación automática de eventos en Kaspersky Security Center.

Solo se pueden exportar eventos generales desde las aplicaciones administradas mediante los formatos CEF y LEEF. Los eventos específicos de la aplicación no se pueden exportar desde las aplicaciones administradas mediante los formatos CEF y LEEF. Si necesita exportar eventos de aplicaciones administradas o un conjunto personalizado de eventos que se haya configurado utilizando las directivas de aplicaciones administradas, exporte los eventos mediante el formato Syslog.

Para activar la exportación automática de eventos:

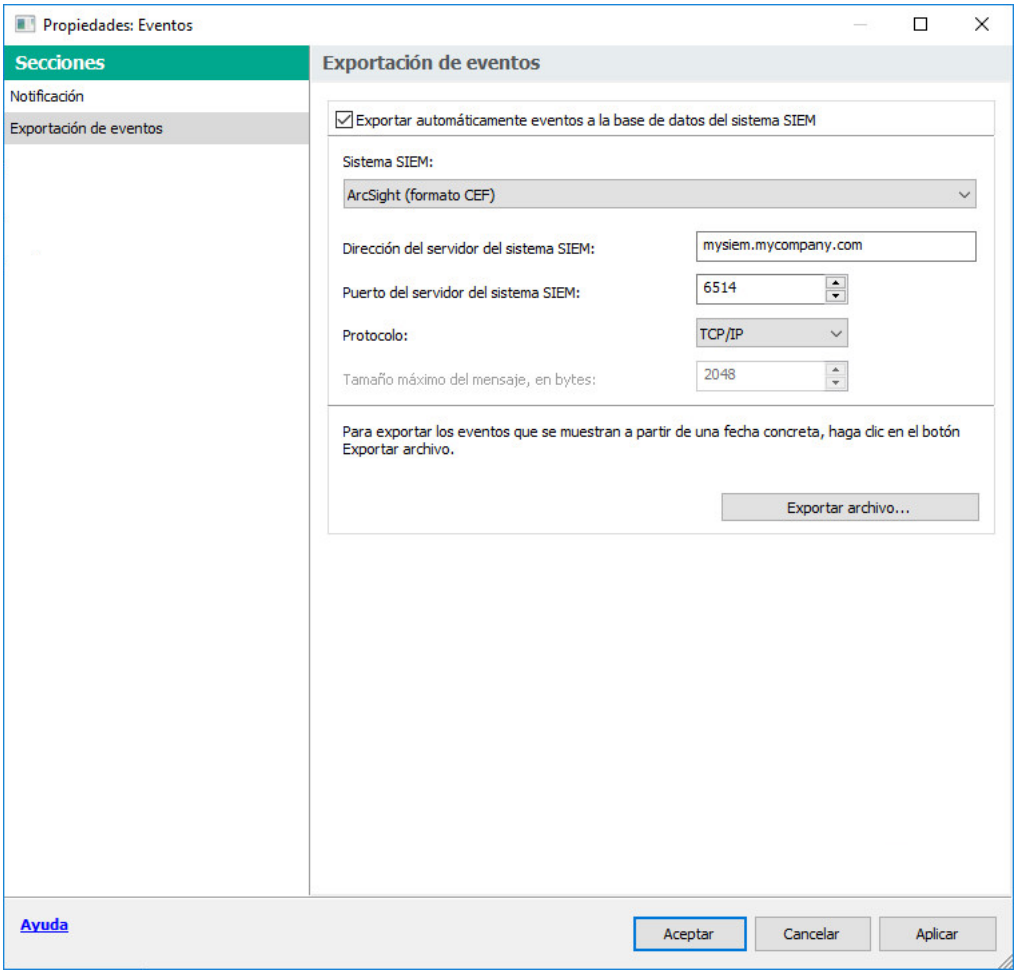
1. En el árbol de consola de Kaspersky Security Center, seleccione el Servidor de administración cuyos eventos desea exportar.

2. En el espacio de trabajo del Servidor de administración seleccionado, seleccione la pestaña **Eventos**.

3. Haga clic en la flecha desplegable junto al enlace **Configurar las notificaciones y la exportación de eventos** y seleccione **Configurar exportación a sistema SIEM** en la lista desplegable.

   Se abre la ventana de propiedades de eventos y muestra la sección **Exportación de eventos**.

4. En la sección **Exportación de eventos**, especifique la configuración de exportación siguiente:



Sección de exportación de evento de la ventana de propiedades de eventos

- **Exportar automáticamente eventos a la base de datos del sistema SIEM**

  Seleccione esta casilla para permitir la exportación automática de eventos a sistemas SIEM. Seleccionar esta casilla activa todos los campos en la sección **Exportando eventos**.

- **Sistema SIEM**

  Seleccione el sistema SIEM al cual exportar los eventos: QRadar® (formato LEEF), ArcSight (formato CEF), Splunk® (formato CEF) y formato Syslog (RFC 5424).

- **Dirección del servidor del sistema SIEM**

  Especifique la dirección del servidor del sistema SIEM. La dirección se puede especificar como un nombre de DNS o NetBIOS o como una dirección IP.

- **Puerto del servidor del sistema SIEM**

Indique el número del puerto para conectarse al servidor del sistema SIEM. Este número de puerto debe ser igual al que su sistema SIEM utiliza para recibir los eventos (ver la sección Configuración de un sistema SIEM).

- **Protocolo**

Seleccione el protocolo para transferir mensajes al sistema SIEM. Puede seleccionar el protocolo TCP/IP, UDP o TLS sobre TCP.

Puede ajustar la configuración de TLS si selecciona TLS sobre el protocolo TCP:

- **Autenticación del servidor**

  En el campo **Autenticación del servidor**, puede seleccionar los valores **Certificados de confianza** o **Huellas digitales SHA**:

  - **Certificados de confianza**. Puede recibir un archivo con la lista de certificados de una autoridad de certificados (CA) de confianza y cargar el archivo en Kaspersky Security Center. Kaspersky Security Center verifica si el certificado del servidor del sistema SIEM también está firmado por una CA de confianza o no.

    Para agregar un certificado de confianza, haga clic en el botón **Busque archivo de certificados de CA** y, a continuación, cargue el certificado.

  - **Huellas digitales SHA**. Puede especificar huellas digitales SHA-1 de certificados del sistema SIEM en Kaspersky Security Center. Para agregar una huella digital SHA-1, introdúzcala en el campo **Huellas digitales** y, a continuación, haga clic en el botón **Añadir**.

  Al usar el ajuste **Añadir autenticación del cliente**, puede generar un certificado para autenticar Kaspersky Security Center. Por lo tanto, utilizará un certificado autofirmado emitido por Kaspersky Security Center. En este caso, puede usar un certificado de confianza y una huella digital SHA para autenticar el servidor del sistema SIEM.

- **Añadir Nombre del sujeto/Nombre alternativo del sujeto**

  El nombre del sujeto es un nombre de dominio para el que se recibe el certificado. Kaspersky Security Center no puede conectarse al servidor del sistema SIEM si el nombre de dominio del servidor del sistema SIEM no coincide con el nombre del sujeto del certificado del servidor del sistema SIEM. Sin embargo, el servidor del sistema SIEM puede cambiar su nombre de dominio si el nombre ha cambiado en el certificado. En este caso, se pueden especificar los nombres de sujeto en el campo **Añadir Nombre del sujeto/Nombre alternativo del sujeto**. Si alguno de los nombres de sujeto especificados coincide con el nombre de sujeto del certificado del sistema SIEM, Kaspersky Security Center validará el certificado del servidor del sistema SIEM.

- **Añadir autenticación del cliente**

  Para la autenticación del cliente, puede insertar su certificado o generarlo en Kaspersky Security Center.

  - **Ingresar certificado**. Puede utilizar un certificado que haya recibido de cualquier fuente; por ejemplo, de cualquier CA de confianza. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

    - **PEM certificado X.509**. Cargue un archivo con un certificado en el campo **Archivo con certificado** y un archivo con una clave privada en el campo **Archivo con clave**. Ninguno de estos archivos dependen el uno del otro y, por tanto, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, especifique la contraseña para descodificar la clave privada en el campo **Verificación de certificado o contraseña**. La contraseña puede tener un valor vacío si la clave privada no está codificada.

    - **PKCS12 certificado X.509**. Cargue un único archivo que contenga un certificado y su clave privada en el campo **Archivo con certificado**. Cuando se cargue el archivo, especifique la contraseña para descodificar la clave privada en el campo **Verificación de certificado o contraseña**. La contraseña puede tener un valor vacío si la clave privada no está codificada.

- **Generar clave**. Puede generar un certificado autofirmado en Kaspersky Security Center. Como resultado, Kaspersky Security Center almacena el certificado autofirmado generado y puede pasar la parte pública del certificado o huella digital SHA1 al sistema SIEM.

Si selecciona el formato Syslog, debe especificar:

- **Tamaño máximo del mensaje, en bytes**

  Especifique el tamaño máximo (en bytes) de un mensaje transmitido al sistema SIEM. Cada evento se transmite en un mensaje. Si la longitud real de un mensaje supera el valor especificado, el mensaje se trunca y los datos se pueden perder. El tamaño predeterminado es 2048 bytes. Este campo solo está disponible si seleccionó el formato de Syslog en el campo **Sistema SIEM**.

5. Si desea exportar a la base de datos del sistema SIEM los eventos que ocurrieron después de una fecha especificada en el pasado, haga clic en el botón **Exportar archivo** y especifique la fecha de inicio para la exportación del evento. De forma predeterminada, la exportación del evento comienza inmediatamente después de que la activa.

6. Haga clic en **Aceptar**.

La exportación automática de eventos se activa.

Después de activar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM.

Exportar eventos directamente desde la base de datos

Puede recuperar eventos directamente desde la base de datos de Kaspersky Security Center sin necesidad de usar la interfaz de Kaspersky Security Center. Puede consultar las vistas públicas directamente y recuperar los datos del evento o crear sus propias vistas sobre la base de las vistas públicas existentes y dirigirse a ellas para conseguir los datos que necesita.

Vistas públicas

Para su comodidad, se proporciona un conjunto de vistas públicas en la base de datos de Kaspersky Security Center. Puede encontrar la descripción de estas vistas públicas en el documento klakdb.chm.

La vista pública v_akpub_ev_event contiene un conjunto de campos que representan los parámetros del evento en la base de datos. En el documento klakdb.chm también puede encontrar información sobre vistas públicas correspondiente a otras entidades de Kaspersky Security Center, por ejemplo, dispositivos, aplicaciones o usuarios. Puede usar esta información en sus consultas.

Esta sección contiene instrucciones para crear una consulta SQL mediante la utilidad klsql2 y un ejemplo de consulta.

Para crear consultas SQL o vistas de bases de datos, también puede utilizar cualquier otro programa para trabajar con bases de datos. En la sección correspondiente, se proporciona información sobre cómo ver los parámetros para conectar a la base de datos de Kaspersky Security Center, como el nombre de la instancia y nombre de la base de datos.

Creación de una consulta SQL usando la herramienta klsql2

Esta sección describe cómo descargar y usar la utilidad klsql2, y cómo crear una consulta SQL usando esta utilidad. Cuando crea una consulta SQL por medio de la utilidad klsql2, no tiene que proporcionar el nombre de la base de datos ni parámetros de acceso, porque la consulta aborda las vistas públicas de Kaspersky Security Center directamente.

Para descargar y usar la utilidad klsql2:

1. Descargar la utilidad klsql2 desde el sitio web de Kaspersky.
2. Copie y extraiga el archivo klsql2.zip descargado en cualquier carpeta en el dispositivo con el Servidor de administración de Kaspersky Security Center instalado.

   El paquete klsql2.zip incluye los archivos siguientes:

   - klsql2.exe
   - src.sql
   - start.cmd
3. Abra el archivo src.sql en cualquier editor de texto.
4. En el archivo src.sql, escriba la consulta SQL que desee y guarde el archivo.
5. En el dispositivo con el Servidor de administración de Kaspersky Security Center instalado, en la línea de comandos, escriba el comando siguiente para ejecutar la consulta SQL desde el archivo src.sql y guarde los resultados en el archivo result.xml:
   ```
   klsql2 -i src.sql -o result.xml
   ```
6. Abra el archivo result.xml recién creado para ver los resultados de la consulta.

Puede modificar el archivo src.sql y crear cualquier consulta en las vistas públicas. A continuación, desde la línea de comandos, ejecute su pregunta y guarde los resultados en un archivo.

Ejemplo de una consulta SQL en la utilidad klsql2

Esta sección muestra un ejemplo de una consulta SQL, creada por medio de la utilidad klsql2.

El ejemplo siguiente ilustra la recuperación de los eventos que ocurrieron en dispositivos durante los últimos siete días, y muestra los eventos solicitados cuando ocurren; los eventos más recientes se muestran primero.

Ejemplo:

```
SELECT
e.nId, /* identificador de eventos */
e.tmRiseTime, /* hora, cuando se produjo el evento */
e.strEventType, /* nombre interno del tipo de evento */
e.wstrEventTypeDisplayName, /* nombre del evento mostrado */
e.wstrDescription, /* descripción del evento mostrada */
e.wstrGroupName, /* nombre del grupo, donde se encuentra el dispositivo */
```

```
h.wstrDisplayName, /* nombre del dispositivo mostrado, en el que se produjo el
evento */
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 /* IP-address del dispositivo, donde se
produjo el evento */
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
```

La visualización del nombre de la base de datos de Kaspersky Security Center

Si desea acceder a la base de datos de Kaspersky Security Center por medio de las herramientas de administración de bases de datos SQL Server, MySQL o MariaDB, debe conocer el nombre de la base de datos a fin de conectarse desde su editor de scripts de SQL.

Ver el nombre de la base de datos de Kaspersky Security Center:

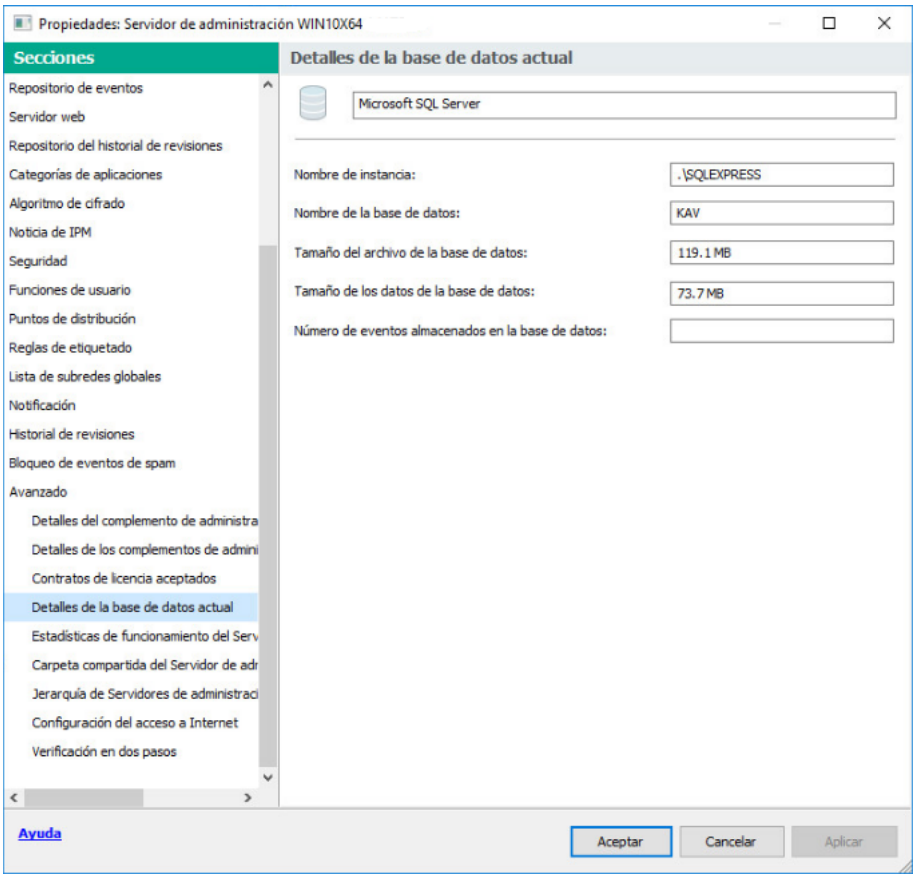
1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, en el panel **Avanzado**, seleccione **Detalles de la base de datos actual**.
3. En la sección **Detalles de la base de datos actual**, tenga en cuenta las propiedades de la base de datos siguientes (consulte la siguiente figura):

   - **Nombre de instancia**

     Nombre de la instancia de base de datos de Kaspersky Security Center actual. El valor predeterminado es *.\KAV_CS_ADMIN_KIT*.

   - **Nombre de la base de datos**

     Nombre de la base de datos de Kaspersky Security Center SQL. El valor predeterminado es *KAV*.



Sección con información sobre la base de datos del Servidor de administración actual

4. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

Use el nombre de la base de datos para dirigirse a la base de datos en sus consultas SQL.

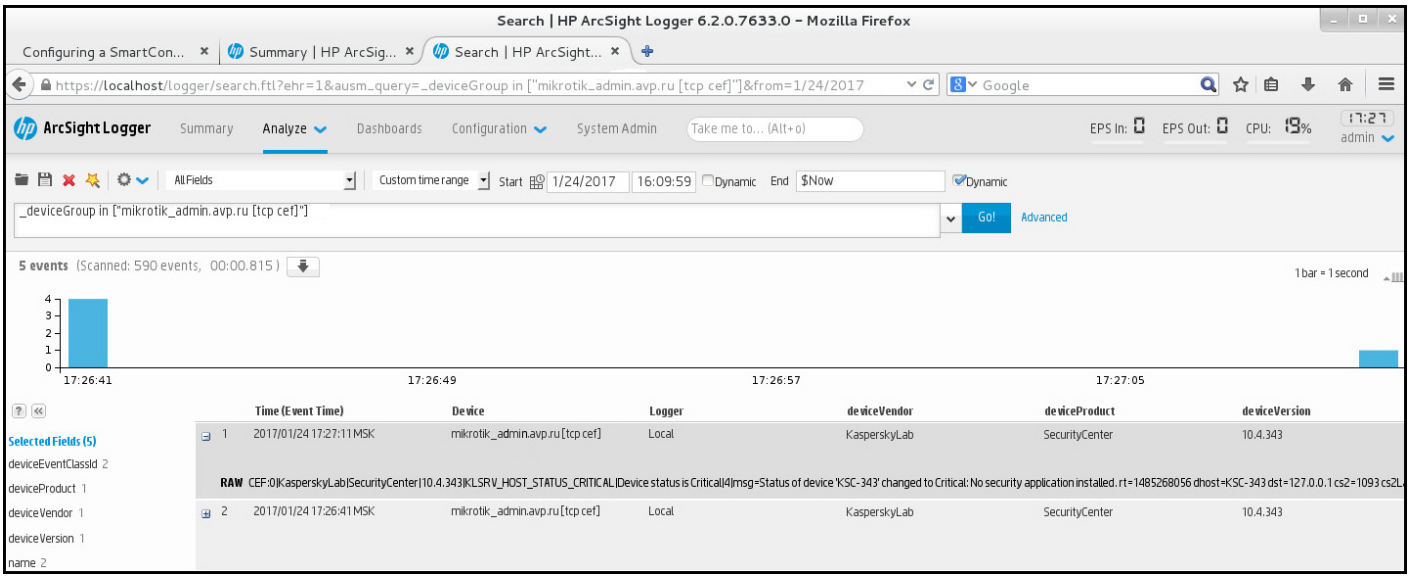
Visualización de resultados de exportación

Puede controlar la finalización correcta del procedimiento de exportación del evento. Para hacerlo, compruebe si los mensajes con eventos de exportación se reciben por su sistema SIEM.

Si los eventos enviados desde Kaspersky Security Center se reciben y analizan correctamente por su sistema SIEM, la configuración en ambos lados se realiza correctamente. De otra forma, compruebe la configuración que especificó en Kaspersky Security Center con respecto a la configuración en su sistema SIEM.

La figura a continuación muestra los eventos exportados a ArcSight. Por ejemplo, el primer evento es un evento crítico del Servidor de administración: "*El estado del dispositivo es crítico*".

La representación de eventos de exportación en el sistema SIEM varía según el sistema SIEM que use.



Ejemplo de eventos

Usar SNMP para enviar estadísticas a aplicaciones de terceros

Esta sección describe cómo obtener información del Servidor de administración mediante el Protocolo simple de administración de redes (SNMP) en Windows. Kaspersky Security Center contiene un agente SNMP, que transfiere estadísticas del rendimiento del Servidor de administración a las aplicaciones secundarias que utilizan OID.

Esta sección también contiene información sobre cómo resolver problemas que puede encontrar al usar SNMP para Kaspersky Security Center.

El agente SNMP y los identificadores de objetos

Para Kaspersky Security Center, el agente SNMP se implementa como una biblioteca dinámica `klsnmpag.dll`, que el instalador registra durante la instalación del Servidor de administración. El agente SNMP funciona dentro del proceso `snmp.exe` (que es un servicio de Windows). Las aplicaciones de terceros usan SNMP para recibir estadísticas (que vienen en forma de contadores) sobre el rendimiento del Servidor de administración.

Cada contador tiene un identificador de *objeto único* (también denominado OID). Un identificador de objeto es una secuencia de números dividida por puntos. Los identificadores de objeto del Servidor de administración comienzan con el prefijo 1.3.6.1.4.1.23668.1093. El OID del contador es una concatenación de ese prefijo con un sufijo que describe el contador. Por ejemplo, el contador con el valor OID de 1.3.6.1.4.1.23668.1093.1.1.4 tiene un sufijo con el valor 1.1.4.

Puede usar un cliente de SNMP (como Zabbix) para monitorizar el estado del sistema. Para obtener la información, puede buscar un valor de OID que corresponda a la información e ingresar ese valor en su cliente de SNMP. Entonces su cliente SNMP le devolverá otro valor, que caracteriza el estado de su sistema.

La lista de contadores y tipos de contadores se encuentra en el archivo `adminkit.mib` en el Servidor de administración. *MIB* son las siglas de Management Information Base. Puede importar y analizar archivos `.mib` a través de la aplicación MIB Viewer que está diseñada para solicitar y mostrar los valores del contador.

Obtener un nombre de contador de cadena a partir de un identificador de objeto

Para utilizar un identificador de objeto (OID) para transferir información a aplicaciones de terceros, puede que deba obtener un nombre de contador de cadena de ese OID.

Para obtener un nombre de contador de cadena de un OID:

1. Abra el archivo `adminkit.mib`, que se encuentra en el Servidor de administración, en un editor de texto.
2. Busque el espacio de nombres que describe el primer valor (de izquierda a derecha).

   Por ejemplo, para el sufijo OID 1.1.4, sería `"counters" (::= { kladminkit 1 })`.
3. Busque el espacio de nombres que describe el segundo valor.

   Por ejemplo, para el sufijo OID 1.1.4 sería `counters 1`, que significa `deployment`.
4. Busque el espacio de nombres que describe el tercer valor.

   Por ejemplo, para el sufijo OID 1.1.4 sería `deployment 4`, que significa `hostsWithAntivirus`.

El nombre del contador de cadenas es la concatenación de esos valores, por ejemplo `<espacio de nombres de la base MIB>.counters.deployment.hostsWithAntivirus`, y corresponde al OID con el valor 1.3.6.1.4.1.23668.1093.1.1.4.

Valores de identificadores de objetos para SNMP

La siguiente tabla muestra los valores y descripciones de los identificadores de objetos (también llamados OID) que se utilizan para transferir información sobre el rendimiento del Servidor de administración a aplicaciones de terceros.

Valores y descripciones de identificadores de objeto para SNMP

Valor del identificador de objeto	Tipo de datos numéricos	OID	Descripción
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Estado de despliegue. El estado puede ser uno de los siguientes: • **Información**. La licencia ya no es válida para N dispositivos. • **Advertencia**. Uno de los siguientes: Hay M máquinas con aplicaciones de Kaspersky instaladas en un total de N dispositivos en grupos del Servidor de administración (> M). La licencia L caduca en N dispositivos en M días.

			La tarea T de instalar aplicaciones se ha completado correctamente en N dispositivos, es necesario reiniciar M dispositivos. • **Crítico**. La licencia de N dispositivos ha caducado. • **OK**. Ninguna de las anteriores.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	El motivo `deploymentStatus` muestra que el grupo del Servidor de administración contiene demasiados dispositivos sin software antivirus. El valor es igual a 1 en caso de que se encuentren algunos dispositivos sin aplicaciones administradas y 0 en caso contrario.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	El motivo `deploymentStatus` muestra que la tarea de la instalación remota ha fallado en algunos dispositivos. El número de esos dispositivos se puede obtener a través de `hostsRemoteInstallFailed`
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	El motivo `deploymentStatus` muestra que hay algunos dispositivos con una licencia que caduca en los próximos siete días. El número de esos dispositivos se puede obtener a través de `hostsLicenseExpiring`.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	El motivo `deploymentStatus` muestra que hay algunos dispositivos con una licencia caducada. Puede obtener el número de esos dispositivos a través de `hostsLicenseExpired`.
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	Número de dispositivos en los grupos del Servidor de administración.
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	Número de dispositivos en los grupos del Servidor de administración con aplicaciones administradas instaladas.
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	Número de dispositivos en los

			que ha fallado la tarea de instalación remota.
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	ID de una clave de licencia que caduca pronto (en menos de 7 días).
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	ID de la clave de licencia caducada.
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	Número de días antes de que caduque una licencia.
`hostsLicenceExpiring`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.9	Número de dispositivos con una licencia que caduca pronto (en menos de siete días).
`hostsLicenceExpired`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.10	Número de dispositivos con una licencia caducada.
`updatesStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.2.1	Estado actual de las bases antivirus. El estado puede ser uno de los siguientes: • **Información**. Hace más de 1 día que no se actualiza el Servidor de administración y ha pasado menos de 1 día desde la instalación de la aplicación. • **Advertencia**. Hace más de 1 día que no se actualiza el Servidor de administración. • **Crítico**. Hace más de 2 días que no se actualiza el Servidor de administración. • **OK**. Ninguna de las anteriores.
`serverNotUpdated`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.1	Este motivo muestra que el Servidor de administración no s ha actualizado durante mucho tiempo. La cantidad de tiempo que se considera larga se especifica en `updatesStatus`.
`notUpdatedHosts`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.2.2.2	Esta razón muestra que algunos dispositivos no se actualizaron durante mucho tiempo (7 días o más para **Crítico** y 3 días para **Advertencia**). Puede obtener e número de esos dispositivos a través de `hostsNotUpdated`.
`lastServerUpdateTime`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.2.3	La última vez que se actualizaro las bases antivirus en el Servido de administración.
`hostsNotUpdated`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.2.4	El número de dispositivos que

			contienen bases antivirus que n están actualizadas.
protectionStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.3.1	Estado de la protección en tiempo real. Uno de los siguientes: • **Advertencia**. Uno de los siguientes: Se ha detectado una brecha de seguridad en un host que pertenece al grupo del Servidor de administración. Errores de cifrado hicieron que algunos dispositivos cambiaran el estado de la protección. No se ha realizado ningún análisis completo desde hac mucho tiempo. • **Crítico**. La protección antivirus no funciona en algunos dispositivos de los grupos del Servidor de administración. • **OK**. Ninguna de las anteriores.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Esta razón muestra que en algunos dispositivos no se está ejecutando una aplicación de seguridad. Puede obtener el número de esos dispositivos a través de `hostsAntivirusNotRunning`
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Esto muestra que no se está ejecutando la protección en tiempo real en algunos dispositivos. Puede obtener el número de esos dispositivos a través de `hostsRealtimeNotRunning`.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Esto muestra que hay dispositivos que contienen objetos no desinfectados. Puede obtener el número de esos dispositivos a través de `hostsNotCuredObject`.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Esto muestra que se encontraron amenazas en algunos dispositivos. Puede obtener el número de esos dispositivos a través de `hostsTooManyThreats`.
virusOutbreak	INTEGER {	.1.3.6.1.4.1.23668.1093.1.3.2.6	Esto muestra el estado del brot

	`off(0), on(1) }`		de virus del sistema. El valor es igual a 1 si se encontr una cierta cantidad de virus durante un cierto período de tiempo y 0 en caso contrario. La cantidad de virus y la cantidad de tiempo se especifican en el Servidor de administración mediante la configuración de `Virus attack`.
`hostsAntivirusNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.3	Número de dispositivos con aplicaciones de seguridad que no se están ejecutando.
`hostsRealtimeNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.4	Número de dispositivos con protección en tiempo real que no se están ejecutando.
`hostsRealtimeLevelChanged`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.5	Número de dispositivos con niv de protección en tiempo real no aceptable.
`hostsNotCuredObject`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.6	Número de dispositivos que contienen objetos no desinfectados.
`hostsTooManyThreats`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.7	Número de dispositivos que contienen amenazas.
`fullscanStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.4.1	Estado del análisis antivirus completo. Uno de los siguientes • **Información**. Han pasado menos de 7 días desde el momento de la instalación d la aplicación. • **Advertencia**. No se ha realizado un análisis antivirus completo durante más de 7 días desde el momento de la instalación de la aplicación. • **Crítico**. No se ha realizado u análisis antivirus completo durante más de 14 días desd el momento de la instalación de la aplicación. • **OK**. Ninguna de las anteriores.
`notScannedLately`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.4.2.1	Esta razón muestra que algunos dispositivos no se han escaneado durante un cierto período de tiempo. Puede obtener el número de esos dispositivos a través de `hostsNotScannedLately`. La

			cantidad de tiempo se especifica en `fullScanStatus`
`hostsNotScannedLately`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.4.3	Número de dispositivos que no se han analizado durante un tiempo determinado. La cantidad de tiempo se especifica en `fullScanStatus`
`logicalNetworkStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.5.1	Estado de la red lógica del Servidor de administración. Uno de los siguientes: • **Advertencia**. Si hay dispositivos con un estado de advertencia a los que no se puede acceder o si hay dispositivos que no pertenecen a ningún grupo del Servidor de administración. • **Crítico**. Si hay dispositivos cuyo control ha sido perdido por el Servidor de administración, o si hay dispositivos con un estado crítico y no se puede acceder. • **OK**. Ninguna de las anteriores.
`notConnectedLongTime`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.1	Este motivo muestra que algunos dispositivos no han estado conectados al Servidor de administración durante mucho tiempo (7 días o más para un dispositivo en estado de **Advertencia** y 4 días para un dispositivo en estado **crítico**). Puede obtener el número de esos dispositivos mediante `hostsNotConnectedLongTime`
`controlLost`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.2	Esto muestra que hay dispositivos sobre los que el Servidor de administración ha perdido el control. Puede obtener el número de esos dispositivos a través de `hostsControlLost`.
`hostsFound`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.3	Número de dispositivos encontrados por el Servidor de administración que no pertenecen a ningún grupo del Servidor administración.
`groupsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.4	Número de grupos en el Servidor de administración.

hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Número de dispositivos que no se han conectado al Servidor d administración durante mucho tiempo. La cantidad de tiempo considerada larga se especifica en notConnectedLongTime.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Número de dispositivos que no están controlados por el Servidor de administración.
eventsStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.6.1	Subsistema de estado de eventos. Uno de los siguientes: • **Advertencia**. Uno de los siguientes: Los dispositivos del grupo d Servidor de administración no han estado buscando actualizaciones de Windows durante mucho tiempo. Hay dispositivos con problemas de estado. • **Crítico**. Uno de los siguientes: Hay un evento de importancia "Crítico" en al menos un host. Hay un evento de importancia de "Error" en al menos un host. Hay un evento de tarea que se está completando sin éxito en al menos un dispositivo. Los dispositivos del grupo d Servidor de administración no han estado buscando actualizaciones de Windows durante mucho tiempo. Hay dispositivos con problemas de estado. • **OK**. Ninguna de las anteriores.
criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	El motivo eventsStatus muestra que hay algunos eventos críticos en el Servidor de administración. Puede obtener el número de esos eventos a través de criticalEventsCount. El valor es igual a 1 si hay al menos un evento crítico en cualquier dispositivo, y 0, en caso contrario.
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	Número de eventos críticos en

			Servidor de administración.

Solución de problemas

Esta sección enumera las soluciones para algunos problemas típicos que puede encontrar al utilizar el servicio SNMP.

La aplicación de terceros no se puede conectar al servicio SNMP

Asegúrese de haber instalado la compatibilidad con SNMP en Windows. La compatibilidad con SNMP está desactivada de forma predeterminada.

Para permitir la compatibilidad con SNMP en Windows 10:

1. Navegue al **Panel de control**.
2. Abra el menú **Añadir o eliminar programas**.
3. Haga clic en **Activar o desactivar las funciones de Windows**.
4. En la Lista de funciones de Windows, navegue hasta la función SNMP y luego haga clic en **Aceptar**.
5. Vaya a **Panel de control** → **Herramientas administrativas** → **Servicios**.
6. Elija el servicio SNMP y ejecútelo.
7. Compruebe si la escucha funciona probándola con `netstat`, para un puerto UPD estándar.

La compatibilidad con SNMP está permitida en Windows 10.

El servicio SNMP está funcionando, pero la aplicación de terceros no puede obtener ningún valor.

Permita el seguimiento del agente SNMP y asegúrese de que se crea un archivo no vacío. Esto significa que el agente SNMP está registrado y funcionando correctamente. Después de esto, permita las conexiones desde el servicio SNMP en la configuración del servicio lateral. Si un servicio secundario funciona en el mismo host que el agente SNMP, la lista de direcciones IP debe contener la dirección IP de ese host o el `loopback 127.0.0.1`.

Debe ejecutarse en Windows un servicio SNMP que se comunica con los agentes. Puede especificar las rutas a los agentes SNMP en el Registro de Windows a través de regedit.

- Microsoft Windows 10:
  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents]
- Para Windows Vista y Windows Server 2008:
  [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents]

También puede permitir el rastreo de agentes SNMP a través de regedit.

- Para x86:

[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug]

- Para x64:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\De

  "TraceLevel"=dword:00000004

  "TraceDir"="C:\\"

Los valores no coinciden con los estados de la Consola de administración

Para reducir la carga en el Servidor de administración, se implementa el almacenamiento en caché de valores para el agente SNMP. La latencia entre la caché que se actualiza y los valores que se cambian en el Servidor de administración puede causar discrepancias entre los valores devueltos por el agente SNMP y los reales. Cuando trabaje con aplicaciones de terceros, debe tener en cuenta esa posible latencia.

Trabajo en un entorno de nube

Esta sección proporciona información sobre el despliegue y el mantenimiento de Kaspersky Security Center en entornos de nube, como Amazon Web Services, Microsoft Azure o Google Cloud.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Acerca del trabajo en un entorno de nube

Kaspersky Security Center 14 no solo funciona con dispositivos locales, sino que también proporciona características especiales para trabajar en un entorno de nube. Kaspersky Security Center funciona con las siguientes máquinas virtuales:

- Instancias de Amazon EC2 (en adelante, también denominadas *instancias*). Una instancia de Amazon EC2 es una máquina virtual que se crea sobre la base de la plataforma de servicios web de Amazon (AWS). Kaspersky Security Center utiliza la *API* de AWS (interfaz de programación de aplicaciones).
- Máquinas virtuales de Microsoft Azure. Kaspersky Security Center utiliza la API de Azure.
- Instancias de máquinas virtuales de Google Cloud. Kaspersky Security Center utiliza la API de Google.

Puede desplegar Kaspersky Security Center en una instancia o en una máquina virtual para administrar la protección de dispositivos en un entorno de nube y usar las características especiales de Kaspersky Security Center para trabajar en un entorno de nube. Estas funciones incluyen:

- La utilización de herramientas API para sondear dispositivos en un entorno de nube
- Uso de herramientas API para instalar el Agente de red y aplicaciones de seguridad en dispositivos en un entorno de nube
- La búsqueda de dispositivos según si pertenecen a un segmento de la nube específico

También puede usar una instancia o una máquina virtual en la que se despliega un Servidor de administración de Kaspersky Security Center para proteger los dispositivos locales (por ejemplo, si un servidor en la nube resulta ser más fácil para usted de revisar y mantener que uno físico). Si este es el caso, trabajará con el Servidor de administración de la misma manera que lo haría si el Servidor de administración se instalara en un dispositivo local.

En un Kaspersky Security Center que se ha desplegado desde una imagen de máquina de Amazon (AMI) pagada (en AWS) o una SKU facturada mensualmente basada en el uso (en Azure), la administración de vulnerabilidades y parches (incluida la integración con los sistemas SIEM) se activa automáticamente; la Administración de dispositivos móviles no se puede activar.

El Servidor de administración se instala junto con la Consola de administración. Kaspersky Security for Windows Server también se instala automáticamente en el dispositivo en el que está instalado el Servidor de administración.

Puede utilizar el Asistente de configuración del entorno de nube para configurar Kaspersky Security Center, teniendo en cuenta los aspectos específicos del trabajo en un entorno de nube.

Escenario: Despliegue para el escenario de entorno de nube

Esta sección describe el despliegue de Kaspersky Security Center para trabajar en entornos de nube como Amazon Web Services, Microsoft Azure y Google Cloud.

Una vez que finalice el escenario de despliegue, el Servidor de administración de Kaspersky Security Center y la Consola de administración se iniciarán y se configurarán con los ajustes predeterminados. La protección antivirus administrada por Kaspersky Security Center se desplegará en las instancias seleccionadas de Amazon EC2 o máquinas virtuales de Microsoft Azure. Puede poner a punto a continuación la configuración de Kaspersky Security Center, crear una estructura compleja de grupos de administración y crear varias directivas y tareas para grupos.

El despliegue de Kaspersky Security Center para su funcionamiento en entornos de nube consta de las siguientes partes:

1. Tareas preliminares.
2. Despliegue del Servidor de administración.
3. La instalación de aplicaciones del antivirus de Kaspersky en dispositivos virtuales que se tienen que proteger.
4. Configuración de los parámetros de descarga de las actualizaciones.
5. Configuración de los ajustes para administrar informes sobre el estado de la protección de los dispositivos.

El Asistente de configuración del entorno de nube está pensado para realizar la configuración inicial. Se inicia automáticamente la primera vez que Kaspersky Security Center se despliega desde una imagen lista para usar. También puede iniciar manualmente el Asistente en cualquier momento. Además, puede optar por realizar manualmente todas las acciones que realiza el Asistente.

Le recomendamos que planifique un mínimo de una hora para el despliegue del Servidor de administración de Kaspersky Security Center en el entorno de nube y al menos un día hábil para el despliegue de la protección en el entorno de nube.

El despliegue de Kaspersky Security Center en el entorno de nube se lleva a cabo en etapas:

1. **Planificación de la configuración de los segmentos de la nube**

Aprenda cómo Kaspersky Security Center funciona en un entorno de nube. Planifique dónde se desplegará el Servidor de administración (dentro o fuera del entorno de nube) y especifique cuántos segmentos de la nube planea proteger. Si planea desplegar el Servidor de administración fuera del entorno de nube o si planea proteger más de 5000 dispositivos, necesitará instalar manualmente el Servidor de administración.

Para trabajar con Google Cloud, solo puede instalar el Servidor de administración de forma manual.

2. **Planificación de los recursos**

   Asegúrese de que tiene todo lo que se requiere para el despliegue.

3. **Suscripción a Kaspersky Security Center como imagen lista para usar**

   Seleccione una de las AMI listas para usar en AWS Marketplace, o seleccione una SKU facturada mensualmente en Azure Marketplace, pague según las reglas del mercado si es necesario (o use el modelo BYOL), y use la imagen para desplegar una instancia de Amazon EC2 o máquina virtual de Microsoft Azure con Kaspersky Security Center instalado.

   Esta etapa solo es necesaria si planea desplegar el Servidor de administración en una instancia o máquina virtual dentro de un entorno de nube y también planea desplegar protección para no más de 5000 dispositivos. De lo contrario, esta etapa no es necesaria y, en su lugar, debe instalar manualmente el Servidor de administración, la Consola de administración y el DBMS.

   Este paso no está disponible para Google Cloud.

4. **Determinación de la ubicación del DBMS**

   Determine dónde estará su DBMS.

   Si planea utilizar una base de datos fuera del entorno de nube, asegúrese de tener una base de datos que esté en funcionamiento.

   Si planea utilizar Amazon Relational Database Service (RDS), cree una base de datos con RDS en el entorno de nube de AWS.

   Si planea utilizar Microsoft Azure SQL DBMS, cree una base de datos con el servicio Azure Database en el entorno de nube de Microsoft Azure.

   Si planea utilizar Google MySQL, cree una base de datos en Google Cloud (consulte https://cloud.google.com/sql/docs/mysql para obtener más detalles).

5. **Instalación manual del Servidor de administración y la Consola de administración (basada en Microsoft Management Console o en la consola web) en dispositivos seleccionados**

   Instale el Servidor de administración, la Consola de administración y el DBMS en los dispositivos seleccionados según lo descrito en el escenario principal de despliegue para Kaspersky Security Center.

   Esta etapa es necesaria si planea desplegar el Servidor de administración fuera de un entorno de nube o si planea desplegar protección para más de 5.000 dispositivos. Después, asegúrese de que su Servidor de administración cumple con los requisitos de hardware. De lo contrario, esta etapa no es necesaria y basta con una suscripción a Kaspersky Security Center como una imagen lista para usar en AWS Marketplace, Azure Marketplace o Google Cloud.

6. **Asegurar que el Servidor de administración tenga los permisos para trabajar con las API de la nube**

   En AWS, vaya a la Consola de administración de AWS y cree una función de IAM o una cuenta de usuario de IAM. La función de IAM creada (o la cuenta de usuario de IAM) permitirá que Kaspersky Security Center funcione con API AWS para sondear segmentos de la nube y desplegar la protección.

   En Azure, cree una suscripción y un Id. de la aplicación con una contraseña. Kaspersky Security Center usa estas credenciales para trabajar con la API de Azure: sondear los segmentos de la nube y desplegar la protección.

   En Google Cloud, registre un proyecto, obtenga su Id. de proyecto y una clave privada. Kaspersky Security Center utiliza estas credenciales para sondear segmentos de la nube utilizando la API de Google.

7. **Creación de una función de IAM para instancias protegidas (solo para AWS)**

En la consola de administración de AWS, cree una función de IAM que defina el conjunto de permisos para ejecutar solicitudes a AWS. Esta función recién creada se asignará posteriormente a nuevas instancias. La función de IAM es necesaria para usar Kaspersky Security Center con intención de instalar aplicaciones en instancias.

8. **Preparación de una base de datos utilizando el Servicio de base de datos relacional de Amazon o Microsoft Azure SQL**

   Si planea utilizar el Servicio de base de datos relacional (RDS) de Amazon, cree una instancia de base de datos de Amazon RDS y un S3 bucket en el que se almacenará la copia de seguridad de la base de datos. Puede omitir esta etapa si desea una base de datos en la misma instancia de EC2 donde está instalado el Servidor de administración o si desea que su base de datos se encuentre en otro lugar.

   Si planea usar Microsoft Azure SQL, cree una cuenta de almacenamiento y una base de datos en Microsoft Azure.

   Si planea utilizar Google MySQL, configure su base de datos en Google Cloud. (Consulte https://cloud.google.com/sql/docs/mysql para obtener más detalles).

9. **Licencias de Kaspersky Security Center para trabajar en entorno de nube**

   Asegúrese de tener la licencia de Kaspersky Security Center para trabajar en el entorno de nube y proporcione un código de activación o un archivo clave para que la aplicación pueda añadirlo al almacenamiento de licencias. Esta etapa se puede completar en el Asistente de configuración del entorno de nube.

   Esta etapa es obligatoria si está utilizando Kaspersky Security Center instalado a partir de una AMI gratuita y lista para usar basada en el modelo BYOL o si va a instalar manualmente Kaspersky Security Center sin usar ninguna AMI. En ambos casos, necesitará una licencia para Kaspersky Security for Virtualization, o una licencia para seguridad de la nube del híbrido de Kaspersky, para activar Kaspersky Security Center.

   Si está usando Kaspersky Security Center instalado desde una imagen, esta etapa no es necesaria y la ventana correspondiente del Asistente de configuración del entorno de nube no se muestra.

10. **Autorización en el entorno de nube**

    Proporcione a Kaspersky Security Center sus credenciales de AWS, Azure o Google Cloud para que Kaspersky Security Center pueda operar con los permisos necesarios. Esta etapa se puede completar en el Asistente de configuración del entorno de nube.

11. **Sondeo del segmento de la nube para que el Servidor de administración pueda recibir información sobre los dispositivos en el segmento de la nube**

    Inicie el sondeo del segmento de la nube. En el entorno de AWS, Kaspersky Security Center recibirá las direcciones y los nombres de todas las instancias a las que se puede acceder en función de los permisos de la función de IAM o del usuario de IAM. En el entorno de Microsoft Azure, Kaspersky Security Center recibirá las direcciones y los nombres de todas las máquinas virtuales a las que se puede acceder según los permisos de la función de lector.

    Luego puede usar Kaspersky Security Center para instalar aplicaciones y software de Kaspersky de otros proveedores en las instancias o máquinas virtuales detectadas.

    Kaspersky Security Center inicia regularmente un sondeo, lo que significa que las nuevas instancias o máquinas virtuales se detectan automáticamente.

12. **Combinación de todos los dispositivos de red en el grupo de administración de la nube**

    Mueva las instancias o máquinas virtuales descubiertas al grupo de administración **Dispositivos administrados\Cloud** para que puedan estar disponibles para la administración centralizada. Si desea asignar dispositivos a subgrupos, por ejemplo, dependiendo de qué sistema operativo está instalado, puede crear varios grupos de administración en el grupo de **dispositivos administrados\Cloud**. Puede activar el traslado automático de todos los dispositivos que se detectarán durante los sondeos de rutina al grupo **Dispositivos administrados\Cloud**.

13. **Utilización del Agente de red para conectar dispositivos en red al Servidor de administración**

Instale el Agente de red en dispositivos en el entorno de nube. El Agente de red es el componente de Kaspersky Security Center que proporciona la comunicación entre los dispositivos y el Servidor de administración. Los ajustes del Agente de red se configuran automáticamente de forma predeterminada.

Puede instalar el Agente de red en cada dispositivo localmente. También puede instalar remotamente el Agente de red en dispositivos usando Kaspersky Security Center. O bien, puede omitir esta etapa e instalar el Agente de red junto con las últimas versiones de las aplicaciones de seguridad.

14. **Instalación de las versiones más recientes de aplicaciones de seguridad en dispositivos en red**

    Seleccione los dispositivos donde desea instalar las aplicaciones de seguridad y después instale las versiones más recientes de las aplicaciones de seguridad en esos dispositivos. Puede realizar la instalación de forma remota utilizando Kaspersky Security Center en el Servidor de administración o localmente.

    Puede que tengas que crear manualmente paquetes de instalación para estos programas.

    Kaspersky Endpoint Security para Linux está destinado a instancias y máquinas virtuales que ejecutan Linux.

    Kaspersky Security for Windows Server está destinado a instancias y máquinas virtuales que ejecutan Windows.

15. **Configuración de los parámetros de actualización**

    La tarea **Buscar vulnerabilidades y actualizaciones requeridas** se crea automáticamente cuando se ejecuta el Asistente de configuración del entorno de nube. También puede crear la tarea manualmente. Esta tarea encuentra y descarga automáticamente actualizaciones de aplicaciones requeridas para la instalación posterior en dispositivos de red usando herramientas de Kaspersky Security Center.

    Se recomienda completar las siguientes etapas después de que el Asistente de configuración del entorno de nube termine:

16. **Configuración de la administración de informes**

    Puede ver informes en la ficha **Supervisión** en el espacio de trabajo del nodo **Servidor de administración**. También puede recibir informes por correo electrónico. Los informes en la ficha **Supervisión** están disponibles de forma predeterminada. Para configurar la recepción de informes por correo electrónico, especifique las direcciones de correo electrónico que deberían recibir informes y después configure el formato de los informes.

Resultados

Al completar el escenario, puede asegurarse de que la configuración inicial terminó correctamente:

- Puede conectarse al Servidor de administración a través de la Consola de administración o Kaspersky Security Center 14 Web Console.
- Las últimas versiones de las aplicaciones de seguridad de Kaspersky están instaladas y se ejecutan en los dispositivos administrados.
- Kaspersky Security Center ha creado las directivas y tareas predeterminadas para todos los dispositivos administrados.

Requisitos previos para desplegar Kaspersky Security Center en un entorno de nube

Antes de comenzar el despliegue de Kaspersky Security Center en los servicios web de Amazon o en el entorno de nube de Microsoft Azure, asegúrese de que dispone de lo siguiente:

- Acceso a Internet

- Una de las siguientes cuentas:
  - Cuenta de Amazon Web Services (para trabajar con AWS)
  - Cuenta de Microsoft (para trabajar con Azure)
  - Cuenta de Google (para trabajar con Google Cloud)
- Uno de los siguientes:
  - Licencia para Kaspersky Security for Virtualization
  - Licencia para seguridad de la nube del híbrido de Kaspersky
  - Fondos para comprar dicha licencia (Kaspersky Security for Virtualization o Kaspersky Hybrid Cloud Security)
  - Fondos para pagar una imagen lista para usar en Azure Marketplace
- Guías para las últimas versiones de Kaspersky Endpoint Security for Linux y Kaspersky Security for Windows Server

Requisitos de hardware para el Servidor de administración en un entorno de nube

Para la implementación en entornos de nube, los requisitos para el Servidor de administración y el servidor de base de datos son los mismos que los del Servidor de administración físico (según el número de dispositivos que desee administrar). Consulte la documentación del entorno de nube para más detalles.

Opciones de licencias en un entorno de nube

Trabajar en el entorno de nube está fuera de la funcionalidad básica de Kaspersky Security Center, por tanto, requiere una licencia específica.

Hay dos opciones de licencia de Kaspersky Security Center disponibles para trabajar en un entorno de nube:

- AMI pagada (en Amazon Web Services) o SKU facturado en función del uso (en Microsoft Azure).

  Esto otorga una licencia para Kaspersky Security Center, así como licencias para Kaspersky Endpoint Security para Linux y Kaspersky Security for Windows Server. Tiene que pagar de acuerdo con las reglas del entorno de nube que utiliza.

  Este modelo no le permite tener más de 200 dispositivos cliente para un Servidor de administración.

- Una imagen de uso gratuito y lista para usar con una licencia de propietario, según el modelo de su propia licencia (BYOL).

  Para las licencias de Kaspersky Security Center en AWS o Azure, debe tener una licencia para una de las siguientes aplicaciones:
  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

El modelo BYOL le permite tener hasta 100 000 dispositivos cliente para un Servidor de administración. Este modelo también le permite administrar dispositivos fuera del entorno de nube de AWS, o Azure o Google.

Puede elegir el modelo BYOL en cualquiera de los siguientes casos:

- ya posee una licencia válida de Kaspersky Security for Virtualization,
- ya posee una licencia válida para seguridad de Kaspersky Hybrid Cloud Security,
- está dispuesto a comprar una licencia inmediatamente antes del despliegue de Kaspersky Security Center.

En la etapa de la instalación inicial, Kaspersky Security Center le solicitará un código de activación o un archivo clave.

Si elige BYOL, no tendrá que pagar Kaspersky Security Center a través de Azure Marketplace o la plataforma AWS.

En ambos casos, la Administración de vulnerabilidades y parches se activa automáticamente, y la Administración de dispositivos móviles no se puede activar.

Puede encontrar un error al intentar activar la función Soporte del entorno de nube con la licencia de Kaspersky Hybrid Cloud Security.

Al suscribirse a Kaspersky Security Center, obtiene una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o una máquina virtual de Microsoft Azure con el Servidor de administración de Kaspersky Security Center. Los paquetes de instalación para Kaspersky Security for Windows Server y Kaspersky Endpoint Security para Linux están disponibles en el Servidor de administración. Puede instalar estas aplicaciones en dispositivos en el entorno de nube. No tiene que licenciar estas aplicaciones.

Si el Servidor de administración no puede ver un dispositivo administrado durante más de una semana, la aplicación (Kaspersky Security for Windows Server o Kaspersky Endpoint Security para Linux) cambiará al modo de funcionalidad limitada en el dispositivo. Para volver a activar la aplicación, debe hacer que el Servidor de administración vuelva a ver el dispositivo en el que está instalada la aplicación.

Opciones de base de datos para trabajar en un entorno de nube

Debe tener una base de datos para trabajar con Kaspersky Security Center. Al desplegar Kaspersky Security Center en AWS, en Microsoft Azure o en Google Cloud, tiene tres opciones:

- Crear una base de datos local en el mismo dispositivo con el Servidor de administración. Kaspersky Security Center viene con una base de datos SQL Server Express que puede admitir hasta 5000 dispositivos administrados. Elija esta opción si SQL Server Express Edition es suficiente para sus necesidades.
- Crear una base de datos con el Servicio de bases de datos relacionales (RDS) en el entorno de nube de AWS o con el Servicio de base de datos de Azure en el entorno de nube de Microsoft Azure. Elija esta opción si desea un DBMS que no sea SQL Express. Sus datos se transferirán dentro del entorno de nube, donde permanecerán y no tendrá ningún gasto adicional. Si ya trabaja con Kaspersky Security Center en las instalaciones y tiene algunos datos en su base de datos, puede transferir sus datos a la nueva base de datos.

  Para trabajar en Google Cloud Platform, solo puede usar Cloud SQL para MySQL.
- Utilice un servidor de la base de datos existente. Elija esta opción si ya tiene un servidor de la base de datos y desea usarlo para Kaspersky Security Center. Si este servidor está fuera del entorno de nube, sus datos se transferirán a Internet, lo que podría causar gastos adicionales.

El procedimiento de despliegue de Kaspersky Security Center en el entorno de nube tiene un paso especial para crear (elegir) una base de datos.

Trabajo con el entorno de nube de Amazon Web Services

Esta sección le explica cómo prepararse para trabajar con Kaspersky Security Center en los servicios web de Amazon.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Sobre trabajar con el entorno de nube de Amazon Web Services

Puede comprar Kaspersky Security Center en AWS Marketplace en forma de imagen de máquina de Amazon (AMI), que es una imagen lista para usar de una máquina virtual preconfigurada. Puede suscribirse a una AMI pagada o BYOL AMI y, según esa imagen, crear una instancia de Amazon EC2 con el Servidor de administración de Kaspersky Security Center instalado.

Para funcionar con la plataforma AWS y, en particular, comprar aplicaciones en AWS Marketplace y crear instancias, necesitará una cuenta de Amazon Web Services. Puede crear una cuenta gratuita en https://aws.amazon.com/es. También puede usar una cuenta de Amazon existente.

Si se suscribió a una AMI disponible en AWS Marketplace, recibirá una instancia con su Kaspersky Security Center listo para usar. No tiene que instalar la aplicación usted mismo. En este caso, Servidor de administración de Kaspersky Security Center se instala en la instancia sin su participación. Después de la instalación, puede iniciar la Consola de administración y conectar al Servidor de administración para comenzar a trabajar con Kaspersky Security Center.

Para obtener más información sobre una AMI y cómo funciona AWS Marketplace, visite la página de Ayuda de la plataforma AWS. Para obtener más información sobre el funcionamiento con la plataforma de AWS, usando instancias y conceptos relacionados, consulte la documentación de Amazon Web Services.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Creación de funciones de IAM y cuentas de usuario de IAM para instancias de Amazon EC2

Esta sección describe las acciones que se deben realizar para garantizar el funcionamiento correcto del Servidor de administración. Estas acciones incluyen el trabajo con las funciones y las cuentas de usuario de AWS Identity and Access Management (IAM). También se describen las acciones que se deben tomar en los dispositivos cliente para instalar en ellos el Agente de red y luego instalar Kaspersky Security for Windows Server y Kaspersky Endpoint Security para Linux.

Asegurarse de que el Servidor de administración de Kaspersky Security Center tiene los permisos para funcionar con AWS

Las normas para operar en el entorno de nube de Amazon Web Services exigen que se asigne una función de IAM especial a la instancia del Servidor de administración para que funcione con los servicios de AWS. Una función de IAM es una entidad IAM que define el conjunto de permisos para la ejecución de solicitudes a servicios AWS. La función de IAM proporciona los permisos para el sondeo de segmentos de la nube y la instalación de aplicaciones en las instancias.

Después de crear una función de IAM y asignarla al Servidor de administración, podrá desplegar la protección de las instancias usando esta función, sin necesidad de facilitar información adicional a Kaspersky Security Center.

Sin embargo, puede ser aconsejable no crear una función de IAM para el Servidor de administración en los siguientes casos:

- Los dispositivos cuya protección quiere administrar son instancias de EC2 localizadas dentro del entorno de nube de Amazon Web Services, pero el Servidor de administración está fuera del entorno.
- Tiene pensado administrar la protección de las instancias, no solo dentro de su segmento de la nube, sino también dentro de otros segmentos de la nube que se crearon con otra cuenta en AWS. En este caso, necesitará una función de IAM solamente para proteger su segmento de la nube. Para proteger otros segmentos de la nube, no será necesaria una función de IAM.

En estos casos, en lugar de crear una función de IAM, deberá crear una *cuenta de usuario de IAM* que Kaspersky Security Center utilizará para funcionar con los servicios de AWS. Antes de comenzar a trabajar con el Servidor de administración, cree una cuenta de usuario de IAM con una *clave de acceso de AWS IAM* (en lo sucesivo, también denominada *clave de acceso de IAM*).

La creación de una función de IAM o cuenta de usuario de IAM requiere la consola de administración de AWS. Para trabajar con la consola de administración de AWS, necesitará un nombre de usuario y contraseña desde una cuenta en AWS.

Crear una función de IAM para el Servidor de administración

Antes de instalar el Servidor de administración, en la consola de administración de AWS debe crear una función de IAM con los permisos necesarios para la instalación de aplicaciones en las instancias. Para obtener más detalles, consulte las secciones de Ayuda de AWS sobre las funciones de IAM.

Para crear una función de IAM para el Servidor de administración:

1. Abra la consola de administración de AWS e inicie sesión en su cuenta AWS.
2. En la sección **Funciones**, cree una función con los siguientes permisos:
   - **AmazonEC2ReadOnlyAccess**, si planea ejecutar solo el sondeo de segmentos de la nube y no planea instalar aplicaciones en instancias EC2 con API AWS.
   - **AmazonEC2ReadOnlyAccess** y **AmazonSSMFullAccess**, si planea ejecutar el sondeo de segmentos de la nube e instalar aplicaciones en instancias EC2 con API AWS. En este caso, también necesitará asignar una función de IAM con el permiso AmazonEC2RoleforSSM a las instancias EC2 protegidas.

Deberá asignar esta función a la instancia de EC2 que usará como Servidor de administración.

La función recién creada está disponible para todas las aplicaciones del Servidor de administración. Por lo tanto, cualquier aplicación que se ejecute en el Servidor de administración tiene la capacidad de sondear segmentos de la nube o instalar aplicaciones en instancias de EC2 dentro de un segmento de la nube.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Crear una cuenta de usuario de IAM para trabajar con Kaspersky Security Center

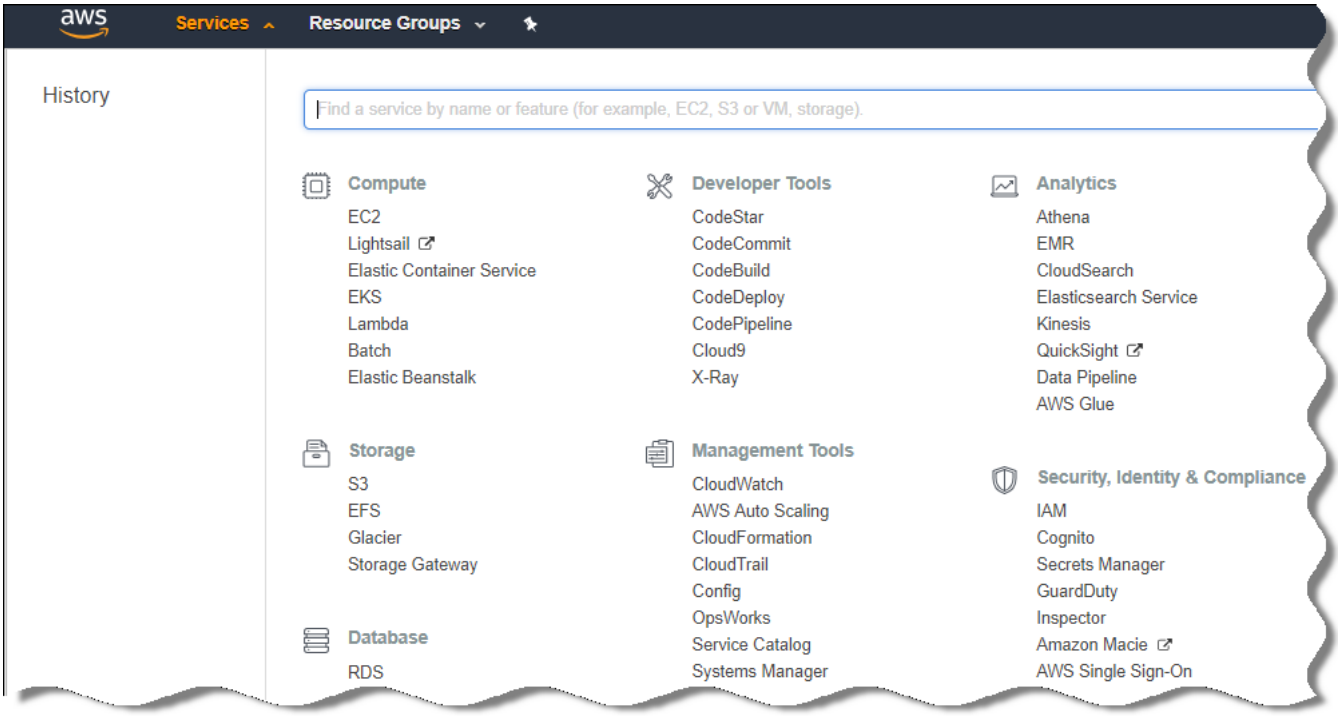
Se necesita una cuenta de usuario de IAM para trabajar con Kaspersky Security Center si al Servidor de administración no se le ha asignado una función de IAM con permisos para efectuar la detección de dispositivos e instalaciones de aplicaciones en las instancias. La misma cuenta, o una cuenta diferente, también se requiere para hacer una copia de seguridad de la tarea de datos del Servidor de administración si usa un bucket S3. Puede crear una cuenta de usuario de IAM con todos los permisos necesarios o puede crear dos cuentas de usuario separadas.

Se crea automáticamente una *clave de acceso de IAM* para el usuario de IAM que deberá proporcionar a Kaspersky Security Center durante la configuración inicial. La clave de acceso de IAM consiste en un Id. de clave de acceso y una clave secreta. Para obtener más información sobre el servicio IAM, consulte las páginas de referencia de AWS:

- http://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/es_es/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Para crear una cuenta de usuario de IAM con los permisos necesarios:

1. Abra la consola de administración de AWS e inicie sesión en su cuenta.
2. En la lista de servicios de AWS, seleccione **IAM** (como se muestra en la siguiente figura).



Lista de servicios en la Consola de administración de AWS

Se abre una ventana que contiene una lista de nombres de usuarios y un menú que le permite trabajar con la herramienta.

3. Navegue por las áreas de la consola que se ocupan de las cuentas de usuario y añada un nuevo nombre o nombres de usuario.

4. Para los usuarios que añada, especifique las siguientes propiedades de AWS:

   - Tipo de acceso: **Programmatic Access**.
   - Límite de permisos no establecido.
   - Permisos:
     - **ReadOnlyAccess**, si planea ejecutar solo el sondeo de segmentos de la nube y no planea instalar aplicaciones en instancias EC2 con API AWS.
     - **ReadOnlyAccess** y **AmazonSSMFullAccess**: si planea ejecutar el sondeo de segmentos de la nube e instalar aplicaciones en instancias EC2 con API AWS. En este caso, también deberá asignar una función de IAM con el permiso AmazonEC2RoleforSSM a las instancias EC2 protegidas.

   Después de añadir los permisos, verlos para la precisión. En caso de una selección errónea, vuelva a la pantalla anterior y vuelva a realizar la selección.

5. Después de crear la cuenta de usuario, aparece una tabla que contiene la clave de acceso de IAM del nuevo usuario de IAM. El id. de la clave de acceso se mostrará en la columna **Access Key ID**. La clave secreta se mostrará como asteriscos en la columna **Secret access key**. Para ver la clave secreta, haga clic en **Show**.

La cuenta recién creada se mostrará en la lista de cuentas de usuarios de IAM que corresponde a su cuenta en AWS.

Al desplegar Kaspersky Security Center en un segmento de la nube, deberá especificar que está utilizando una cuenta de usuario de IAM y proporcionar el id. de la clave de acceso y la clave de acceso secreta a Kaspersky Security Center.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Crear una función de IAM para la instalación de aplicaciones en instancias de Amazon EC2

Antes de que inicie el despliegue de la protección en instancias de Amazon EC2 usando Kaspersky Security Center, en la consola de administración de AWS debe crear una función de IAM con los permisos necesarios para la instalación de aplicaciones en las instancias. Para obtener más detalles, consulte las secciones de Ayuda de AWS sobre las funciones de IAM.

La función de IAM es necesaria para poder asignársela a todas las instancias de Amazon EC2 en las que planee instalar aplicaciones de seguridad usando Kaspersky Security Center. Si no asigna a una instancia la función de IAM con los permisos necesarios, la instalación de aplicaciones en esta instancia mediante las herramientas de API AWS generará un error.

Para trabajar con la consola de administración de AWS, necesitará un nombre de usuario y contraseña desde una cuenta en AWS.

Para crear una función de IAM para la instalación de aplicaciones en instancias:

1. Abra la consola de administración de AWS e inicie sesión en su cuenta AWS.

2. En el menú de la izquierda, seleccione **Roles**.
3. Haga clic en el botón **Create Role**.
4. En la lista de servicios que aparece, seleccione **EC2** y luego, en la lista **Select Your Use Case**, seleccione **EC2** otra vez.
5. Haga clic en el botón **Next: Permissions**.
6. En la lista que se abre, seleccione la casilla de verificación junto a **AmazonEC2RoleforSSM**.
7. Haga clic en el botón **Next: Review**.
8. Introduzca un nombre y una descripción para la función de IAM y haga clic en el botón **Create role**.

   La función que ha creado aparece en la lista de funciones con el nombre y la descripción que ha introducido.

Más adelante, puede usar la función de IAM recién creada para crear nuevas instancias que planee proteger a través de Kaspersky Security Center, así como asociarla con instancias de EC2 existentes.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Trabajar con Amazon RDS

Esta sección describe qué acciones se deben tomar para preparar una base de datos del Servicio de bases de datos relacionales de Amazon (RDS) para Kaspersky Security Center, ubicarla en un grupo de opciones, crear una función de IAM para trabajar con una base de datos de RDS, preparar un bucket S3 para el almacenamiento y migrar una base de datos existente a RDS.

Amazon RDS es un servicio web que ayuda a los usuarios de AWS a configurar, operar y escalar una base de datos relacional en el entorno de nube de AWS. Si lo desea, puede usar una base de datos de RDS de Amazon para trabajar con Kaspersky Security Center.

Puede trabajar con las siguientes bases de datos:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Creación de una instancia de RDS de Amazon

Si desea utilizar Amazon RDS como DBMS, debe crear una instancia de base de datos de Amazon RDS. Esta sección describe cómo seleccionar SQL Express Edition; si desea trabajar con Aurora MySQL o Standard MySQL (versiones 5.7, 8.0), debe seleccionar uno de esos motores.

Para crear una instancia de base de datos de Amazon RDS:

1. Abra la Consola de administración de AWS en https://console.aws.amazon.com e inicie sesión en su cuenta.
2. Utilizando la interfaz de AWS, cree una base de datos con la siguiente configuración:
   - Motor: Microsoft SQL Server, SQL Express Edition
   - Versión del motor de BD: SQL Server 2014 12.00.5546.0v1
   - Clase de instancia de BD: db.t2.medium
   - Tipo de almacenamiento: propósito general
   - Almacenamiento asignado: mínimo 50 GiB
   - Grupo de seguridad: el mismo grupo donde se ubicará la instancia de EC2 con el Servidor de administración de Kaspersky Security Center

   Crea un identificador, un nombre de usuario y una contraseña para su instancia de RDS.

   Puede dejar la configuración predeterminada en todos los demás campos. O cambie la configuración predeterminada si desea personalizar su instancia de Amazon RDS. Para obtener ayuda, consulte las páginas de información de AWS.
3. En el último paso, AWS muestra los resultados del proceso. Si desea ver los detalles de su instancia de Amazon RDS, presione **Ver detalles de la instancia de BD**. Si desea continuar con la siguiente acción, comience a crear un grupo de opciones para su instancia de Amazon RDS.

La creación de una nueva instancia de Amazon RDS puede llevar varios minutos. Después de crear la instancia, puede usarla para trabajar con los datos de Kaspersky Security Center.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

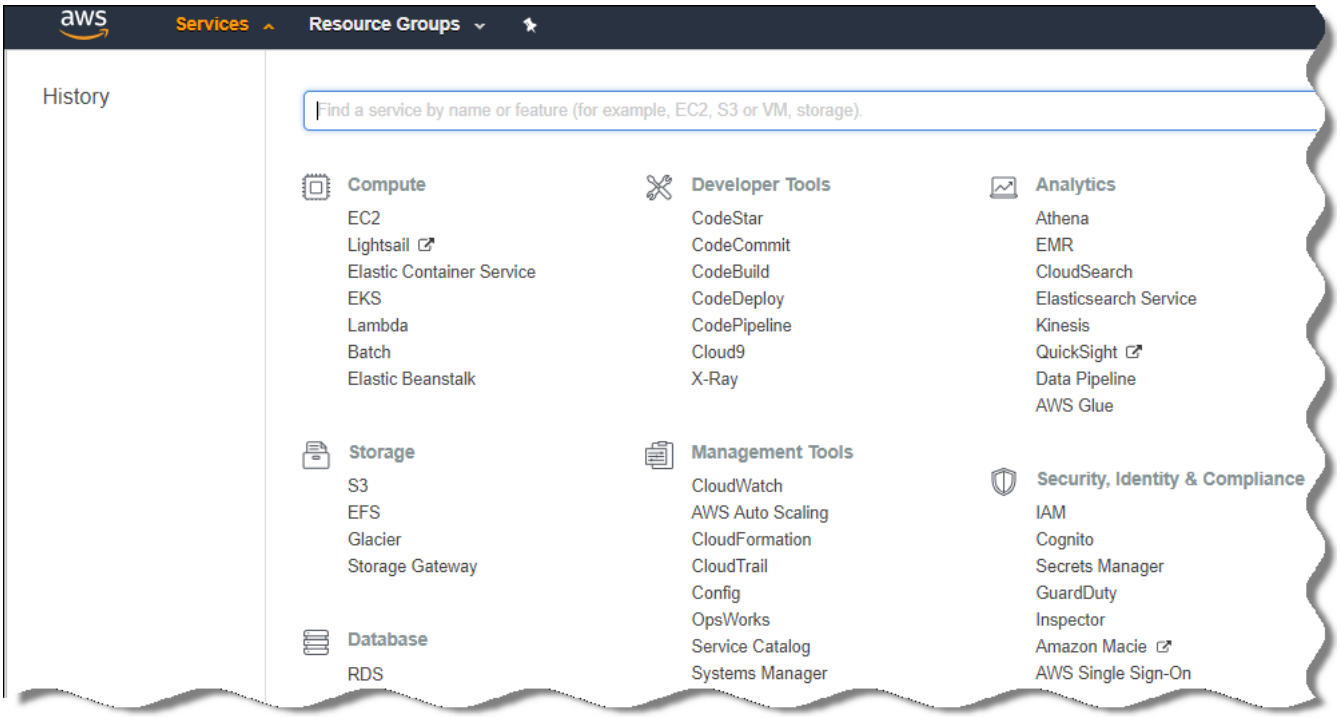
Creación de un grupo de opciones para la instancia de RDS de Amazon

Debe colocar su instancia de Amazon RDS en un grupo de opciones.

Para crear un grupo de opciones para su instancia de Amazon RDS:

1. Asegúrese de estar en la Consola de administración de AWS (https://console.aws.amazon.com) y de haber iniciado sesión en su cuenta.
2. En la línea del menú, haga clic en **Services**.

   Aparece la lista de servicios disponibles (ver figura a continuación).



Lista de servicios en la Consola de administración de AWS

3. En la lista, haga clic en **RDS**.
4. En el panel izquierdo, haga clic en **Option groups**.
5. Haga clic en el botón **Create group**.
6. Cree un grupo de opciones con la siguiente configuración, si eligió SQL Server en la etapa de creación de la instancia de Amazon RDS:

   - Motor: SQLserver-ex
   - Versión de motor principal: 12.00

   Si eligió una base de datos SQL diferente en la etapa de creación de la instancia de Amazon RDS, elija un motor correspondiente.

El grupo se crea y aparece en la lista de sus grupos.

Después de crear el grupo de opciones, coloque su instancia de Amazon RDS en este grupo de opciones.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Modificación del grupo de opciones

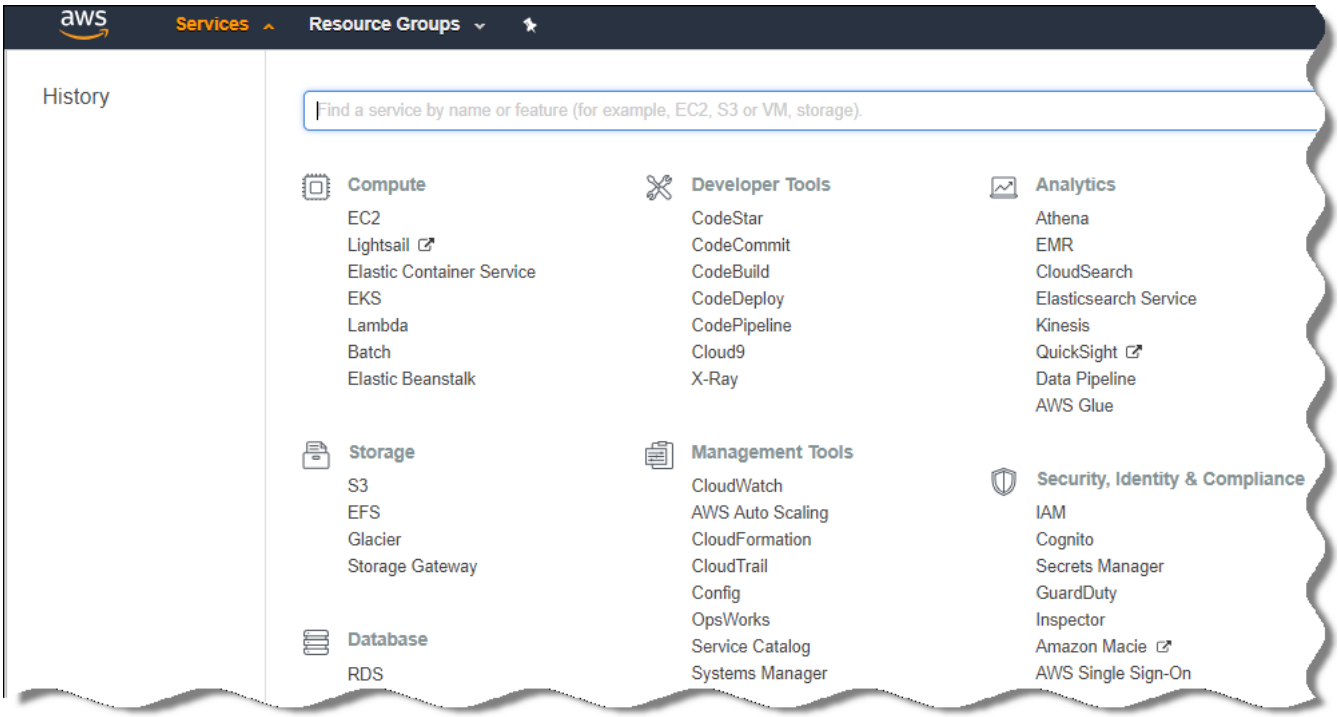
La configuración predeterminada del grupo de opciones en el que colocó la instancia de Amazon RDS no es suficiente para trabajar con la base de datos de Kaspersky Security Center. Debe añadir opciones al grupo de opciones y crear una nueva función de IAM para trabajar con la base de datos.

Para modificar el grupo de opciones y crear una nueva función de IAM:

1. Asegúrese de estar en la Consola de administración de AWS (https://console.aws.amazon.com) y de haber iniciado sesión en su cuenta.

2. En la línea del menú, haga clic en **Services**.

   Aparece la lista de servicios disponibles (ver figura a continuación).



Lista de servicios en la Consola de administración de AWS

3. En la lista, seleccione RDS.

4. En el panel izquierdo, haga clic en **Option groups**.

   Se muestra la lista de grupos de opciones.

5. Seleccione el grupo de opciones en el que colocó su instancia de Amazon RDS y haga clic en el botón **Add option**.

   Se abre la ventana **Add option**.

6. En la sección de la función de IAM, seleccione la opción **Add option**/**Yes** e ingrese un nombre para la nueva función de IAM.

   La función se crea con un conjunto predeterminado de permisos. Más adelante, tendrá que cambiar sus permisos.

7. En la sección del bucket S3, haga uno de los siguientes:

   - Si no ha creado una instancia de bucket de Amazon S3 para la copia de seguridad de datos, seleccione el enlace **Create a new bucket S3** y cree un nuevo bucket S3 utilizando la interfaz de AWS.

   - Si ya ha creado una instancia de bucket de Amazon S3 para la tarea de copia de seguridad de datos del Servidor de administración, seleccione su bucket S3 en el menú desplegable.

8. Termine de añadir opciones haciendo clic en el botón **Add option** en la parte inferior de la página.

Ha modificado el grupo de opciones y ha creado una nueva función de IAM para trabajar con la base de datos de RDS.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Modificación de permisos para la función de IAM para la instancia de base de datos de Amazon RDS

Después de añadir opciones al grupo de opciones, debe asignar los permisos necesarios a la función de IAM que creó para trabajar con la instancia de base de datos de Amazon RDS.

Para asignar los permisos necesarios a la función de IAM que creó para trabajar con la instancia de base de datos de Amazon RDS:

1. Asegúrese de estar en la Consola de administración de AWS (https://console.aws.amazon.com) y de haber iniciado sesión en su cuenta.
2. En la lista de servicios, seleccione **IAM**.

   Se abre una ventana que contiene una lista de nombres de usuarios y un menú que le permite trabajar con la herramienta.
3. En el menú, seleccione **Roles**.
4. En la lista de funciones de IAM que se muestran en el espacio de trabajo, seleccione la función que creó al añadir la opción al grupo de opciones.
5. Al usar la interfaz AWS, elimine la directiva **sqlNativeBackup-<date>**.
6. Al utilizar la interfaz AWS, adjunte la directiva **AmazonS3FullAccess** a la función.

A la función de IAM se le asignan los permisos necesarios para trabajar con Amazon RDS.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Preparación de un bucket de Amazon S3 para la base de datos

Si planea utilizar la base de datos del Sistema de base de datos relacional de Amazon (Amazon RDS), debe crear una instancia de bucket del Servicio de almacenamiento simple de Amazon (Amazon S3) donde se almacenará la Copia de seguridad regular de la base de datos. Para obtener información sobre Amazon S3 y sobre los bucket S3, haga referencia a las páginas de ayuda de Amazonas. Para obtener más información sobre cómo crear una instancia de Amazon S3, consulte la página de ayuda de Amazon S3.

Crear un bucket de Amazon S3:

1. Asegúrese de que Consola de administración de AWS esté abierto y de que haya iniciado sesión en su cuenta.
2. En la lista de servicios AWS, seleccione S3.

3. Navegue por la consola para crear un bucket, siguiendo las instrucciones del Asistente.

4. Seleccione la misma región donde se encuentra (o se ubicará) su Servidor de administración.

5. Cuando finalice el Asistente, asegúrese de que el nuevo grupo aparezca en la lista de grupos.

Se crea un nuevo bucket S3 y aparece en su lista de grupos. Tiene que especificar este bucket al añadir opciones al grupo de opciones. También deberá especificar la dirección de su bucket S3 en Kaspersky Security Center cuando Kaspersky Security Center cree la tarea de datos *Copia de seguridad del Servidor de administración*.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Migrar la base de datos a Amazonas RDS

Puede migrar su base de datos de Kaspersky Security Center desde un dispositivo local a una instancia de Amazon S3 que admita Amazon RDS. Para hacer esto, necesita un bucket S3 para una base de datos de RDS y una cuenta de usuario de IAM con el permiso AmazonS3FullAccess para este bucket S3.

Para realizar la migración de la base de datos:

1. Asegúrese de haber creado una instancia de RDS (consulte las páginas de referencia de Amazon RDS para obtener más información).

2. En su Servidor de administración físico (local), ejecute la utilidad de copia de seguridad de Kaspersky para hacer una copia de seguridad de los datos del Servidor de administración.

   Debe asegurarse de que el archivo se denomine backup.zip.

3. Copie el archivo backup.zip en la instancia de EC2 en la que está instalado el Servidor de administración.

   Asegúrese de tener suficiente espacio en el disco en la instancia de EC2 en la que está instalado el Servidor de administración. En el entorno de AWS, puede añadir espacio en disco a su instancia para adaptarse al proceso de migración de la base de datos.

4. En el Servidor de administración de AWS, vuelva a iniciar la utilidad de copia de seguridad de Kaspersky en modo interactivo.

   Se inicia el Asistente de copias de seguridad y restauración.

5. En el paso **Seleccionar acción**, seleccione **Restaurar datos del Servidor de administración** y haga clic en **Siguiente**.

6. En el paso **Restaurar la configuración** de la restauración, pulse el botón **Examinar** al lado de la **Carpeta para el almacenamiento de copias de seguridad**.

7. En la ventana **Iniciar sesión en el almacenamiento en línea** que se abre, complete los siguientes campos y luego haga clic en **Aceptar**:

   - **Nombre del bucket S3**

El nombre de su bucket S3.

- **Capeta de copia de seguridad**

  Especifique la ubicación de la carpeta de almacenamiento que está destinada a la copia de seguridad.

- **Id. de clave de acceso**

  El Id. de la clave de acceso de AWS IAM que pertenece al usuario de IAM que tiene los permisos para usar el bucket S3 (el permiso AmazonS3FullAccess).

- **Clave secreta**

  La clave secreta de AWS IAM que pertenece al usuario de IAM que tiene los permisos para usar el bucket S3 (el permiso AmazonS3FullAccess).

8. Seleccione la opción **Migrar desde la copia de seguridad local**. El botón **Examinar estará disponible**.
9. Haga clic en el botón **Examinar** para elegir la carpeta en el Servidor de administración de AWS donde copió el archivo backup.zip.
10. Haga clic en **Siguiente** y complete el procedimiento.

    Sus datos se restaurarán en la base de datos de RDS utilizando su bucket S3. Puede usar esta base de datos para seguir trabajando con Kaspersky Security Center en el entorno de AWS.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Trabajo en el entorno de nube de Microsoft Azure

Esta sección proporciona información sobre el despliegue de Kaspersky Security Center y el mantenimiento en un entorno de nube proporcionado por Microsoft Azure, así como detalles del despliegue de la protección en máquinas virtuales en este entorno de nube.

En un Kaspersky Security Center que se ha desplegado desde un SKU facturado basado en el uso, la Administración de vulnerabilidades y parches se activa automáticamente, y la Administración de dispositivos móviles no se puede activar.

Acerca de trabajar en Microsoft Azure

Para trabajar con la plataforma Microsoft Azure y, en particular, para comprar aplicaciones en Azure Marketplace y crear máquinas virtuales, necesitará una suscripción de Azure. Antes de desplegar el Servidor de administración, cree un Id. de la aplicación en Azure con los permisos necesarios para la instalación de aplicaciones en máquinas virtuales.

Si compra una imagen de Kaspersky Security Center en Azure Marketplace, puede desplegar una máquina virtual con su Servidor de administración de Kaspersky Security Center listo para usar. Debe seleccionar la configuración de la máquina virtual pero no tiene que instalar la aplicación usted mismo. Después del despliegue, puede iniciar la Consola de administración y conectar al Servidor de administración para comenzar a trabajar con Kaspersky Security Center.

También puede usar una máquina virtual de Azure con el Servidor de administración de Kaspersky Security Center desplegado para proteger los dispositivos locales (por ejemplo, si un servidor en la nube resulta ser más fácil de inspeccionar y mantener que uno físico). Si este es el caso, trabajará con el Servidor de administración de la misma manera que lo haría si el Servidor de administración se instalara en un dispositivo físico. Si no planea usar las herramientas de la API de Azure, no necesita un Id. de la aplicación en Azure. En este caso, una suscripción de Azure es suficiente.

Creación de una suscripción, Id. de la aplicación y contraseña

Para trabajar con Kaspersky Security Center en el entorno de Microsoft Azure, necesita una suscripción de Azure, el Id. de la aplicación en Azure y la contraseña de la aplicación Azure. Puede utilizar una suscripción existente, si ya tiene una.

Una suscripción de Azure otorga a su propietario acceso al Portal de administración de la plataforma de Microsoft Azure y a los servicios de Microsoft Azure. El propietario puede usar la plataforma Microsoft Azure para administrar servicios como Azure SQL y Azure Storage.

Para crear una suscripción de Microsoft Azure,

Vaya a https://account.windowsazure.com/Subscriptions y siga las instrucciones.

Más información sobre la creación de una suscripción está disponible en el sitio web de Microsoft. Obtendrá una identificación de suscripción, que luego proporcionará a Kaspersky Security Center junto con el Id. de la aplicación y la contraseña.

Para crear y guardar el Id. de la aplicación en Azure y la contraseña:

1. Vaya a https://portal.azure.com y asegúrese de haber iniciado sesión.
2. Siguiendo las instrucciones de la página de referencia, cree su Id. de la aplicación.
3. Ir a la sección **Claves** de la configuración de la aplicación.
4. En la sección **Claves**, complete los campos **Descripción** y **Caducidad** y deje el campo **Valor** en blanco.
5. Hacer clic en **Guardar**.

   Cuando hace clic en **Guardar**, el sistema rellena automáticamente el campo **Valor** con una larga secuencia de caracteres. Esta secuencia es su contraseña de la aplicación Azure (por ejemplo, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). La descripción se muestra a medida que la introduce.
6. Copie la contraseña y guárdela para que luego pueda proporcionar el id. y la contraseña de la aplicación a Kaspersky Security Center.

Podrá copiar la contraseña solo cuando se haya creado. Más adelante, la contraseña ya no se mostrará y no podrá restaurarla.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

La asignación de una función al Id. de la aplicación en Azure

Si solo desea detectar máquinas virtuales mediante la detección de dispositivos, su Id. de la aplicación en Azure debe tener la función de lector. Si no solo desea detectar máquinas virtuales, sino también desplegar la protección en las máquinas virtuales, su id. de la aplicación en Azure debe tener la función de Colaborador de máquina virtual.

Siga las instrucciones en el sitio web de Microsoft para asignar una función a su Id. de la aplicación en Azure.

El despliegue de Servidor de administración en Microsoft Azure y la selección de base de datos

Para desplegar el Servidor de administración en el entorno de Microsoft Azure:

1. Inicie sesión en Microsoft Azure utilizando su cuenta.
2. Vaya al portal de Azure.
3. En el recuadro izquierdo, haga clic en el signo más verde.
4. Escriba "Kaspersky Hybrid Cloud Security" en el campo de búsqueda del menú.

   Kaspersky Hybrid Cloud Security es una combinación de Kaspersky Security Center y dos aplicaciones de seguridad para la protección de instancias: Kaspersky Endpoint Security para Linux y Kaspersky Security for Windows Server.
5. En la lista de resultados, seleccione Kaspersky Hybrid Cloud Security o Kaspersky Hybrid Cloud Security (BYOL).

   En la parte derecha de la pantalla, aparecerá una ventana de información.
6. Lea la información y haga clic en el botón Crear al final de la ventana de información.
7. Rellene todos los campos necesarios. Utilice la información sobre las herramientas para obtener información y asistencia.
8. Al seleccionar el tamaño, seleccione una de las tres opciones destacadas.

   En la mayoría de los casos, 8 gigabytes (GB) de RAM son bastante. Sin embargo, en Azure, puede aumentar el tamaño de RAM y otros recursos de la máquina virtual en cualquier momento.
9. Al seleccionar una base de datos, seleccione una de las siguientes opciones, de acuerdo con su plan:

   - Local: si desea una base de datos en la misma máquina virtual donde se desplegará el Servidor de administración. Kaspersky Security Center viene con una base de datos SQL Server Express. Elija esta opción si SQL Server Express es suficiente para sus necesidades.

- Nuevo: si desea una nueva base de datos de RDS en el entorno de Azure. Elija esta opción si desea un DBMS que no sea SQL Server Express. Sus datos se transferirán al entorno de nube, donde permanecerán y no tendrá ningún gasto adicional.

- Existente: si desea utilizar un servidor de la base de datos existente. En este caso, tendrá que especificar su ubicación. Si este servidor está fuera del entorno de Azure, sus datos se transferirán a Internet, lo que podría causar gastos adicionales.

10. Al introducir el Id. de la suscripción, utilice la suscripción que creó anteriormente.

Después del despliegue, puede conectar al Servidor de administración utilizando RDP. Puede utilizar la Consola de administración para trabajar con el Servidor de administración.

Trabajar con Azure SQL

Esta sección describe qué acciones se deben tomar para preparar una base de datos de Microsoft Azure para Kaspersky Security Center, preparar una cuenta de almacenamiento de Azure y migrar una base de datos existente a Azure SQL.

SQL Database es un servicio administrado de base de datos relacional de propósito general en Microsoft Azure.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Crear una cuenta de almacenamiento de Azure

Debe crear una cuenta de almacenamiento en Microsoft Azure para trabajar con la base de datos de SQL Azul y para los scripts de despliegue.

Para crear una cuenta de almacenamiento:

1. Inicie sesión en el portal de Azure.

2. En el recuadro izquierdo, seleccione **Cuentas de Almacenamiento** para ir a la ventana de **Cuentas de Almacenamiento**.

3. En la ventana **Cuentas de almacenamiento**, haga clic en el botón **Añadir** para ir a la ventana **Crear cuenta de almacenamiento**.

4. Rellene todos los campos necesarios para crear una cuenta de almacenamiento:

   - Ubicación: debe ser la misma que la ubicación que la del Servidor de administración.

   - Otros campos: puede dejar los valores por defecto.

   Utilice la información sobre herramientas para obtener información sobre cada campo.

   Después de crear la cuenta de almacenamiento, se muestra la lista de sus cuentas de almacenamiento.

5. En la lista de sus cuentas de almacenamiento, haga clic en el nombre de la cuenta recién creada para ver información sobre esta cuenta.

6. Asegúrese de conocer el nombre de la cuenta, el grupo de recursos y las claves de acceso para esta cuenta de almacenamiento. Necesitará esta información para trabajar con Kaspersky Security Center.

Puede consultar el sitio web de Azure para obtener ayuda.

Si ya tiene una cuenta de almacenamiento, puede usarla para trabajar con Kaspersky Security Center.

Creación de base de datos de SQL Azure y SQL Server

Necesita una base de datos de SQL y SQL Server en el entorno de Azure.

Para crear una base de datos de SQL Azure y SQL Server:

1. Siga las instrucciones en el sitio web de Azure.

   Puede crear un nuevo servidor cuando Microsoft Azure le pida que lo haga; si ya tiene un servidor SQL de Azure, puede usarlo para Kaspersky Security Center en lugar de crear uno nuevo.

2. Después de crear la base de datos de SQL y SQL Server, asegúrese que conoce el nombre del recurso y grupo del recurso:

   a. Vaya a https://portal.azure.com y asegúrese de haber iniciado sesión.

   b. En el panel izquierdo, **seleccione las bases de datos de SQL**.

   c. Haga clic en el nombre de la base de datos de la lista de sus bases de datos.

      Se abre la ventana de propiedades.

   d. El nombre de la base de datos es el nombre del recurso. El nombre del grupo de recursos se muestra en la sección **Información general** de la ventana Propiedades.

Necesita el nombre del recurso y el grupo del recurso de la base de datos para migrar la base de datos a Azure SQL.

Migrar la base de datos a Azure SQL

Después del despliegue del Servidor de administración en el entorno de Azure, puede migrar su base de datos de Kaspersky Security Center desde un dispositivo local a Azure SQL. Necesita una cuenta de almacenamiento de Azure para una base de datos SQL de Azure. También debe tener el Marco de aplicación de nivel de datos de Microsoft SQL Server (DacFx) y SQLSysCLRTypes en su Servidor de administración.

Para realizar la migración de la base de datos:

1. Asegúrese de haber creado una cuenta de almacenamiento de Azure.

2. Asegúrese de tener SQLSysCLRTypes y DacFx en su Servidor de administración.

   Puede descargar Marco de aplicación de nivel de datos de Microsoft SQL Server (17.0.1 DacFx) y SQLSysCLRTypes (elija la versión correspondiente a la versión de su SQL Server) desde el sitio web oficial de Microsoft.

3. En su Servidor de administración físico (local), ejecute la utilidad Copia de seguridad de Kaspersky para hacer una copia de seguridad de los datos del Servidor de administración con la opción de formato **Migrar al formato de Azure** activada.

4. Copiar la copia de seguridad al Servidor de administración de Azure.

   Asegúrese de tener suficiente espacio en el disco en la máquina virtual de Azure donde está instalado el Servidor de administración. En el entorno de Azure, puede añadir espacio en disco a sus máquinas virtuales para adaptarse al proceso de migración de la base de datos.

5. En el Servidor de administración localizado en el entorno de Microsoft Azure, inicie nuevamente la utilidad de copia de seguridad de Kaspersky en modo interactivo.

   Se inicia el Asistente de copias de seguridad y restauración.

6. En el paso **Seleccionar acción**, seleccione **Restaurar datos del Servidor de administración** y haga clic en **Siguiente**.

7. En el paso **Restaurar la configuración** de la restauración, pulse el botón **Examinar** al lado de la **Carpeta para el almacenamiento de copias de seguridad**.

8. En la ventana **Iniciar sesión en el almacenamiento en línea** que se abre, complete los siguientes campos y luego haga clic en **Aceptar**:

   - **Nombre de la cuenta de almacenamiento de Azure**

     Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

   - **Capeta de copia de seguridad**

     Especifique la ubicación de la carpeta de almacenamiento que está destinada a la copia de seguridad.

   - **Id. de suscripción de Azure**

     Usted creó la suscripción en el portal de Azure.

   - **Contraseña de la aplicación Azure**

     Recibió la contraseña del Id. de la aplicación cuando creó el Id. de la aplicación.

     Los caracteres de la contraseña se muestran como asteriscos. Después de empezar a introducir la contraseña, el botón **Mostrar** estará disponible. Haga clic y mantenga presionado este botón para ver los caracteres que introdujo.

   - **Clave de acceso al almacenamiento de Azure**

     Disponible en las propiedades de su cuenta de almacenamiento, en la sección Claves de acceso. Puede utilizar cualquiera de las claves (clave1 o clave2).

   - **Nombre del servidor SQL de Azure**

     Disponible en las propiedades de su servidor SQL de Azure.

   - **Grupo de recursos del servidor SQL de Azure**

Disponible en las propiedades de su servidor SQL de Azure.

- **Id. de la aplicación en Azure**

  Usted creó este Id. de la aplicación en el portal de Azure.

  Solo puede proporcionar un Id. de la aplicación en Azure para sondeos y otros fines. Si desea sondear otro segmento de Azure, primero debe eliminar la conexión de Azure existente.

9. Seleccione la opción **Migrar desde la copia de seguridad local**.

   El botón **Examinar estará disponible**.

10. Pulse el botón **Examinar** para elegir la carpeta en el Servidor de administración de Azure donde copió la copia de seguridad.

11. Haga clic en **Siguiente** y complete el procedimiento.

Sus datos se restaurarán en la base de datos SQL de Azure usando su almacenamiento de Azure. Puede usar esta base de datos para seguir trabajando con Kaspersky Security Center en el entorno de Azure.

Las direcciones de las páginas web que se mencionan en este documento son correctas a partir de la fecha de lanzamiento de Kaspersky Security Center.

Trabajando en Google Cloud

Esta sección proporciona información sobre el trabajo con Kaspersky Security Center en un entorno de nube proporcionado por Google.

Creación del correo electrónico, ID de proyecto y clave privada del cliente

Puede usar la API de Google para trabajar con Kaspersky Security Center en Google Cloud Platform. Se requiere una cuenta de Google. Consulte la documentación de Google en https://cloud.google.com para obtener más información.

Deberá crear las siguientes credenciales y proporcionárselas a Kaspersky Security Center:

- **Correo electrónico del cliente**

  El correo electrónico del cliente es el correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. del proyecto es el id. que recibió cuando registró su proyecto en Google Cloud.

- Clave privada

  La clave privada es la secuencia de caracteres que recibió como clave privada cuando registró su proyecto en Google Cloud. Es posible que desee copiar y pegar esta secuencia para evitar errores.

Trabajo con la instancia de Google Cloud SQL para MySQL

Puede crear una base de datos en Google Cloud y usarla para Kaspersky Security Center.

Kaspersky Security Center funciona con MySQL 5.7 y 5.6. No se han probado otras versiones de MySQL.

Para crear y configurar una base de datos MySQL:

En su navegador, vaya a https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen y siga las instrucciones proporcionadas.

Al configurar una base de datos MySQL, use los siguientes marcadores:

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

Requisitos previos para dispositivos cliente en un entorno de nube necesarios para trabajar con Kaspersky Security Center

Los dispositivos en los que tenga planeado instalar el Servidor de administración, el Agente de red y las aplicaciones de seguridad de Kaspersky, deben cumplir las siguientes condiciones:

- La configuración de los grupos de seguridad abre los siguientes puertos en el Servidor de administración (conjunto mínimo de puertos necesarios para el despliegue):
  - 8060 HTTP - para transferir paquetes de instalación del Agente de red y paquetes de instalación de aplicaciones de seguridad desde el Servidor de administración a las instancias protegidas

- 8061 HTTPS - para transferir paquetes de instalación del Agente de red y paquetes de instalación de aplicaciones de seguridad desde el Servidor de administración a las instancias protegidas
- 13000 TCP - para transferir datos desde instancias protegidas y Servidores de administración secundarios al Servidor de administración principal mediante SSL
- 13000 UDP - para transferir información sobre el cierre de instancias al Servidor de administración
- 14000 TCP - para transferir datos desde instancias protegidas y Servidores de administración secundarios al Servidor de administración principal sin usar SSL
- 13291 - para conectar la Consola de administración al Servidor de administración
- 40080 - Para el funcionamiento de scripts de despliegue

Puede configurar los grupos de seguridad en la Consola de administración de AWS o en el portal de Azure. Si va a utilizar Kaspersky Security Center en una configuración no predeterminada, consulte la Base de conocimiento. Algunos ejemplos de configuraciones no predeterminadas son no instalar la Consola de administración en el dispositivo del Servidor de administración, sino instalarla en su estación de trabajo, o utilizar un Servidor Proxy KSN.

- El puerto 15000 UDP está abierto en los dispositivos cliente (para recibir solicitudes de comunicación con el Servidor de administración).
- En el entorno de nube AWS:
  - Si planea usar la API de AWS, la función de IAM se establece bajo la cual se instalarán las aplicaciones en las instancias.
  - En cada instancia de Amazon EC2, el Agente de Systems Manager (Agente de SSM) está instalado y en ejecución.
  - El agente de SSM activa Kaspersky Security Center para instalar automáticamente aplicaciones en dispositivos y grupos de dispositivos sin solicitar confirmación por un administrador cada vez.
  - En instancias que están ejecutando un sistema operativo Windows y se instalaron desde las AMI con posterioridad a noviembre de 2016, el agente de SSM está instalado y en funcionamiento. Tendrá que instalar manualmente el agente de SSM en todos los demás dispositivos. Para obtener más información sobre la instalación del agente de SSM en dispositivos con sistemas operativos de Windows y Linux, consulte la página de Ayuda de AWS.
- En el entorno de nube de Microsoft Azure:
  - En cada máquina virtual de Azure, Agente de VM de Azure está instalado y en ejecución.

    De forma predeterminada, se crea una nueva máquina virtual con el Agente de VM de Azure y no tiene que instalarla o habilitarla manualmente. Consulte las páginas de Ayuda de Microsoft para obtener detalles sobre el Agente de VM de Azure en dispositivos Windows y en dispositivos Linux.
  - Su Id. de la aplicación en Azure tiene las siguientes funciones:
    - Lector (para detectar máquinas virtuales mediante el uso de sondeos)
    - Colaborador de máquina virtual (para desplegar la protección en las máquinas virtuales)
    - SQL Server Contributor (para usar una base de datos SQL en el entorno de Microsoft Azure)

    Si desea realizar todas estas operaciones, asigne las tres funciones a su Id. de la aplicación en Azure.

Creación de los paquetes de instalación necesarios para el Asistente de configuración del entorno de nube

El Asistente de configuración del entorno de nube en Kaspersky Security Center está disponible si tiene los paquetes de instalación y los complementos de administración para los siguientes programas:

- Kaspersky Security for Windows Server
- Kaspersky Endpoint Security for Linux

Estos paquetes de instalación son necesarios para instalar Kaspersky Security for Windows Server y Kaspersky Endpoint Security for Linux en las instancias o máquinas virtuales que desea proteger. Si no tiene estos paquetes de instalación, debe crearlos. De lo contrario, el Asistente no puede funcionar.

Para crear paquetes de instalación:

1. Descargue las últimas versiones de las siguientes aplicaciones y complementos en el sitio web de Kaspersky:
   - El instalador y el complemento de administración de Kaspersky Security for Windows Server.
   - El instalador, los archivos para la instalación remota a través de Kaspersky Security Center y el complemento de administración de Kaspersky Endpoint Security for Linux.
2. Guarde todos los archivos en la instancia (o máquina virtual) donde está instalado el Servidor de administración.
3. Extraiga los archivos de todos los paquetes.
4. Inicie Kaspersky Security Center.
5. En el árbol de la consola, vaya a **Avanzado** → **Instalación remota** → **Paquetes de instalación** y haga clic en **Crear paquete de instalación**.
6. Seleccione **Crear el paquete de instalación de Kaspersky**.
7. Especifique el nombre del paquete y la ruta al instalador de la aplicación: <folder>\<file name>.kud, and then click **Siguiente**.
8. Lea el Contrato de licencia de usuario final y seleccione la casilla de verificación para confirmar que acepta sus términos y luego haga clic en **Siguiente**.

El paquete de instalación se cargará en el Servidor de administración y estará disponible en la lista de paquetes de instalación.

El Asistente de configuración del entorno de nube estará disponible tan pronto como cree los paquetes de instalación e instale los complementos de administración para Kaspersky Security for Windows Server y Kaspersky Endpoint Security for Linux en el Servidor de administración.

Asistente de configuración del entorno de nube

Para configurar Kaspersky Security Center usando este Asistente, debe tener lo siguiente:

- Credenciales para el entorno de nube:
  - Una función de IAM a la que se le ha otorgado el derecho de sondear el segmento de la nube o una cuenta de usuario de IAM a la que se le ha otorgado el derecho de sondear el segmento de la nube (para trabajar con Amazon Web Services)
  - Id. de la aplicación en Azure, contraseña y suscripción de Azure (para trabajar con Microsoft Azure)
  - Correo electrónico del cliente de Google, ID del proyecto y clave privada (para trabajar con Google Cloud)

Si no desea usar las capacidades del entorno de nube (si, por ejemplo, desea administrar solo la protección de dispositivos cliente físicos), puede salir del Asistente de configuración del entorno de nube y ejecutar el Asistente de inicio rápido del Servidor de administración manualmente.

El Asistente de configuración del entorno de nube se inicia automáticamente en la primera conexión con el Servidor de administración a través de la Consola de administración si está desplegando Kaspersky Security Center desde una imagen. También puede iniciar el Asistente de configuración del entorno de nube manualmente en cualquier momento.

Para iniciar el Asistente de configuración del entorno de nube manualmente:

1. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.
2. En el menú contextual del nodo, seleccione **Todas las tareas → Asistente de configuración del entorno de nube**.

La sesión de trabajo media con este Asistente es aproximadamente 15 minutos.

Sobre el Asistente de configuración del entorno de nube

Este Asistente le permite configurar Kaspersky Security Center teniendo en cuenta los aspectos específicos del trabajo en un entorno de nube.

El Asistente crea los siguientes objetos:

- Directiva del Agente de red con configuraciones predeterminadas
- Directiva para Kaspersky Endpoint Security para Linux
- Directiva para Kaspersky Security for Windows Server
- Grupo de administración para instancias y una regla para mover automáticamente instancias a este grupo de administración
- Tarea de copia de seguridad de datos del Servidor de administración
- Tareas para instalar la protección en dispositivos con Linux y Windows
- Tareas para cada dispositivo administrado:
  - Análisis antivirus rápido
  - Actualizar descarga

Si ha seleccionado la opción de licencias BYOL, el Asistente también activa Kaspersky Security Center con un archivo clave o código de activación y aplica el archivo clave o código de activación en el almacenamiento de la licencia.

Paso 1. Selección del método de activación de la aplicación

Este paso no se muestra si se registró en una de las AMI listas para usar (en AWS Marketplace) o en un SKU facturado mensual basado en el uso (en Azure Marketplace). En este caso, el Asistente pasa inmediatamente al siguiente paso. Sin embargo, no puede comprar una AMI lista para usar en Google Cloud.

Si seleccionó la opción de licencias BYOL para Kaspersky Security Center, el Asistente le pedirá que seleccione el método de activación de la aplicación.

Activar la aplicación con un código de activación (o archivo clave) para Kaspersky Security for Virtualization o para la Seguridad de la nube del híbrido de Kaspersky.

Puede activar la aplicación de una de las siguientes formas:

- Introduciendo un código de activación.

  Se inicia la activación en línea. Este proceso implica la comprobación del código de activación especificado, además de la emisión y activación de un archivo clave.

- Especificar un archivo clave

  La aplicación comprobará el archivo clave y lo activará si contiene la información correcta, o le pedirá que indique otro archivo clave.

Kaspersky Security Center aplica la clave de licencia en el almacenamiento de la licencia y la marca como distribuida automáticamente en dispositivos administrados.

Si se conecta a una instancia usando la conexión de escritorio remoto estándar en Microsoft Windows o una aplicación similar, en las propiedades de conexión remota tiene que especificar la unidad del dispositivo físico que está utilizando para conectarse. Esto garantiza el acceso desde la instancia a los archivos en su dispositivo físico, y le permite seleccionar y especificar el archivo clave.

Cuando trabaje con Kaspersky Security Center desplegado desde una AMI pagada o para un SKU facturado basado en el uso, no puede añadir archivos clave o códigos de activación al almacenamiento de la licencia.

Paso 2. Selección del entorno de nube

Seleccione el entorno de nube en el que está desplegando Kaspersky Security Center: AWS, Azure o Google Cloud.

Paso 3. Autorización en el entorno de nube

AWS

Si seleccionó AWS, debe especificar que tiene una función de IAM con los derechos requeridos, o proporcionar a Kaspersky Security Center una clave de acceso de AWS IAM. El sondeo de segmentos de la nube no es posible sin una función de IAM o una clave de acceso de AWS IAM.

Especifique los siguientes parámetros para la conexión que se utilizará para seguir sondeando el segmento de la nube:

- **Nombre de conexión**

  Introduzca un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres de Unicode.

  Este nombre también se utilizará como el nombre del grupo de administración para los dispositivos de la nube.

  Si planea trabajar con más de un entorno de nube, es posible que desee incluir el nombre del entorno en el nombre de la conexión, por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google".

- **Usar función AWS IAM**

  Seleccione esta opción si ya ha creado una función de IAM para que el Servidor de administración use los servicios de AWS.

- **Usar la cuenta de usuario AWS IAM**

  Seleccione esta opción si tiene una cuenta de usuario de IAM con los permisos necesarios y puede introducir una ID de clave y una clave secreta.

  - **Id. de clave de acceso**

    El Id. de clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Recibió el ID de clave cuando creó la cuenta de usuario de IAM.

    El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

  - **Clave secreta**

    La clave secreta que recibió con el Id. de clave de acceso cuando creó la cuenta de usuario de IAM.

    Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a introducir la clave secreta, aparecerá el botón **Mostrar**. Haga clic y mantenga pulsado este botón durante la cantidad de tiempo necesaria para ver los caracteres que introdujo.

    El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

Esta conexión se guarda en la configuración de la aplicación. El Asistente de configuración del entorno de nube le permite crear solo una clave de acceso de AWS IAM. Posteriormente, puede especificar más conexiones para administrar otros segmentos de la nube.

Si desea instalar aplicaciones en instancias mediante Kaspersky Security Center, debe asegurarse de que su función de IAM (o el usuario de IAM cuya cuenta esté asociada con la clave que está introduciendo) tenga todos los permisos necesarios.

Azure

Si seleccionó Azure, especifique la siguiente configuración para la conexión que se usará para un sondeo adicional del segmento de la nube:

- **Nombre de conexión**

  Introduzca un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres de Unicode.

  Este nombre también se utilizará como el nombre del grupo de administración para los dispositivos de la nube.

  Si planea trabajar con más de un entorno de nube, es posible que desee incluir el nombre del entorno en el nombre de la conexión, por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google".

- **Id. de la aplicación en Azure**

  Usted creó este Id. de la aplicación en el portal de Azure.

  Solo puede proporcionar un Id. de la aplicación en Azure para sondeos y otros fines. Si desea sondear otro segmento de Azure, primero debe eliminar la conexión de Azure existente.

- **Id. de suscripción de Azure**

  Usted creó la suscripción en el portal de Azure.

- **Contraseña de la aplicación Azure**

  Recibió la contraseña del Id. de la aplicación cuando creó el Id. de la aplicación.

  Los caracteres de la contraseña se muestran como asteriscos. Después de empezar a introducir la contraseña, el botón **Mostrar** estará disponible. Haga clic y mantenga presionado este botón para ver los caracteres que introdujo.

- **Nombre de la cuenta de almacenamiento de Azure**

  Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Clave de acceso al almacenamiento de Azure**

  Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  La clave está disponible en la sección "Descripción general de la cuenta de almacenamiento de Azure", en la subsección "Claves".

Esta conexión se guarda en la configuración de la aplicación.

Google Cloud

Si ha seleccionado Google Cloud, especifique la siguiente configuración para la conexión que se usará para un sondeo adicional del segmento de la nube:

- **Nombre de conexión**

  Introduzca un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres de Unicode.

  Este nombre también se utilizará como el nombre del grupo de administración para los dispositivos de la nube.

  Si planea trabajar con más de un entorno de nube, es posible que desee incluir el nombre del entorno en el nombre de la conexión, por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google".

- **Correo electrónico del cliente**

  El correo electrónico del cliente es el correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. del proyecto es el id. que recibió cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La clave privada es la secuencia de caracteres que recibió como clave privada cuando registró su proyecto en Google Cloud. Es posible que desee copiar y pegar esta secuencia para evitar errores.

Esta conexión se guarda en la configuración de la aplicación.

Paso 4. Configuración de la sincronización con Cloud y elección de otras acciones

En este paso, se inicia al sondeo de segmentos de nube y se crea el grupo de administración especial para instancias. Se aplican las instancias encontradas durante el sondeo. La planificación del sondeo de segmentos de la nube se configura (cada 5 minutos de forma predeterminada).

También se crea la regla de movimiento automática **Sincronizar con Cloud**. Para cada análisis posterior de la red en la nube, los dispositivos virtuales detectados se moverán al subgrupo correspondiente dentro del grupo **Dispositivos administrados\Cloud**.

En la página **Sincronización con el segmento de la nube**, puede definir las siguiente configuración:

- **Sincronizar la estructura del grupo de administración con el segmento de la nube**

Si esta opción está activada, el grupo **Cloud** se crea automáticamente en el grupo **Dispositivos administrados** y se inicia una detección de dispositivos de nube. Las instancias y máquinas virtuales detectadas durante cada análisis de la red de la nube se colocan en el grupo Cloud. La estructura de los subgrupos de administración dentro de este grupo coincide con la estructura de su segmento de la nube (en AWS, las zonas de disponibilidad y los grupos de ubicación no están representados en la estructura; en Azure, las subredes no están representadas en la estructura). Los dispositivos que no se han identificado como instancias en el entorno de nube están en el grupo **Dispositivos no asignados**. Esta estructura de grupo le permite usar tareas de instalación en grupo para instalar aplicaciones antivirus en instancias, así como configurar diferentes directivas para diferentes grupos.

Si esta opción está desactivada, también se crea el grupo de la **nube** y también se inicia la detección de dispositivos de la nube; sin embargo, los subgrupos que coinciden con la estructura del segmento de la nube no se crean dentro del grupo. Todas las instancias detectadas están en el grupo de administración **Cloud**, por lo que se muestran en una lista sola. Si su trabajo con Kaspersky Security Center requiere sincronización, puede modificar las propiedades de la regla **Sincronizar con Cloud** y aplicarla. Aplicar esta regla cambia la estructura de los subgrupos en el grupo Cloud de modo que coincida con la estructura de su segmento de la nube.

Esta opción está desactivada de forma predeterminada.

- **Desplegar protección**

  Si se selecciona esta opción, el Asistente crea una tarea para instalar las aplicaciones de seguridad en instancias. Una vez que finalice el Asistente, el Asistente de despliegue de la protección automáticamente comienza en dispositivos en sus segmentos de la nube, y usted podrá instalar el Agente de red y las aplicaciones de seguridad en esos dispositivos.

  Kaspersky Security Center puede realizar el despliegue con sus herramientas nativas. Si no tiene permisos para instalar las aplicaciones en instancias EC2 o máquinas virtuales Azure, puede configurar la tarea de **Instalación remota** manualmente y especificar una cuenta con los permisos requeridos. En este caso, la tarea de instalación remota no funcionará para los dispositivos detectados utilizando la API de AWS o Azure. Esta tarea solo funciona para los dispositivos descubiertos mediante el sondeo de Active Directory, el sondeo de dominios de Windows o el sondeo de rango de IP.

  Si esta opción no está seleccionada, el Asistente de despliegue de la protección no se inicia y no se crean tareas para instalar aplicaciones de seguridad en las instancias. Puede realizar manualmente ambas acciones más adelante.

Para Google Cloud, solo puede realizar el despliegue con las herramientas nativas de Kaspersky Security Center. Si seleccionó Google Cloud, la opción **Desplegar protección** no está disponible.

Paso 5. Configuración de Kaspersky Security Network en el entorno de nube

Especifique la configuración para transmitir la información sobre las operaciones de Kaspersky Security Center a la base de conocimientos de Kaspersky Security Network. Seleccione una de las siguientes opciones:

- **Acepto usar Kaspersky Security Network**

Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos cliente transferirán automáticamente su información de operación a Kaspersky Security Network. La participación en Kaspersky Security Network garantiza actualizaciones más rápidas de bases de datos que contienen información sobre virus y otras amenazas, y asegura una respuesta más rápida ante amenazas de seguridad emergentes.

- **No acepto usar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se desactivará el uso de Kaspersky Security Network.

Kaspersky recomienda la participación en Kaspersky Security Network.

Paso 6. Configuración de notificaciones por correo electrónico en el entorno de nube

Configure el envío de notificaciones sobre eventos registrados durante el funcionamiento de aplicaciones Kaspersky en los dispositivos cliente virtuales. Estos parámetros servirán de configuración predeterminada de las directivas de la aplicación.

Para configurar la entrega de notificaciones sobre eventos que ocurren en aplicaciones de Kaspersky, use la configuración siguiente:

- **Destinatarios (direcciones de correo electrónico)**

  Las direcciones de correo electrónico de usuarios a quien la aplicación enviará notificaciones. Puede introducir una o más direcciones; si introduce más de una dirección, sepárelas con un punto y coma.

- **Servidores SMTP**

  La dirección o direcciones de los servidores de correo de su organización.

  Si introduce más de una dirección, sepárelas con un punto y coma. Puede usar los siguientes valores:

  - Dirección IPv4 o IPv6
  - Nombre de la red de Windows (nombre NetBIOS) del dispositivo
  - Nombre DNS del servidor SMTP

- **Puerto del servidor SMTP**

  Número del puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

- **Utilizar autenticación ESMTP**

Activa la compatibilidad con autenticación de ESMTP. Cuando la casilla está seleccionada, en los campos **Nombre de usuario** y **Contraseña**, puede especificar la configuración de la autorización de ESMTP. De forma predeterminada, esta casilla está vacía y los parámetros de autenticación ESMTP no están disponibles.

Puede probar la nueva configuración de la notificación por correo electrónico haciendo clic en el botón **Enviar mensaje de prueba**. Si el mensaje de prueba se recibe correctamente en las direcciones especificadas en el campo **Destinatarios (direcciones de correo electrónico)**, la configuración es correcta.

Paso 7. Creación de una configuración inicial de la protección del entorno de nube

En este paso, Kaspersky Security Center automáticamente crea directivas y tareas. La ventana **Configurar la protección inicial** muestra una lista de directivas y tareas creadas por la aplicación.

Si utiliza una base de datos de RDS en el entorno de nube de AWS, debe proporcionar el par de claves de acceso de IAM a Kaspersky Security Center cuando se está creando la tarea de copia de seguridad del Servidor de administración. En este caso, rellene los siguientes campos:

- **Nombre del bucket S3**

  El nombre del bucket S3 que creó para la copia de seguridad.

- **Id. de clave de acceso**

  Recibió el Id. de clave (secuencia de caracteres alfanuméricos) cuando creó la cuenta de usuario de IAM para trabajar con la instancia de almacenamiento de bucket S3.

  El campo está disponible Si ha seleccionado la base de datos de RDS en un bucket S3.

- **Clave secreta**

  La clave secreta que recibió con el Id. de clave de acceso cuando creó la cuenta de usuario de IAM.

  Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a introducir la clave secreta, aparecerá el botón **Mostrar**. Haga clic y mantenga pulsado este botón durante la cantidad de tiempo necesaria para ver los caracteres que introdujo.

  El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

Si utiliza una base de datos SQL de Azure en el entorno de nube de Azure, debe proporcionar información sobre su servidor SQL de Azure a Kaspersky Security Center cuando se cree la tarea de copia de seguridad del Servidor de administración. En este caso, rellene los siguientes campos:

- **Nombre de la cuenta de almacenamiento de Azure**

  Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Id. de suscripción de Azure**

Usted creó la suscripción en el portal de Azure.

- **Contraseña de la aplicación Azure**

  Recibió la contraseña del Id. de la aplicación cuando creó el Id. de la aplicación.

  Los caracteres de la contraseña se muestran como asteriscos. Después de empezar a introducir la contraseña, el botón **Mostrar** estará disponible. Haga clic y mantenga presionado este botón para ver los caracteres que introdujo.

- **Id. de la aplicación en Azure**

  Usted creó este Id. de la aplicación en el portal de Azure.

  Solo puede proporcionar un Id. de la aplicación en Azure para sondeos y otros fines. Si desea sondear otro segmento de Azure, primero debe eliminar la conexión de Azure existente.

- **Nombre del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en sus propiedades de Azure SQL Server.

- **Grupo de recursos del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en sus propiedades de Azure SQL Server.

- **Clave de acceso al almacenamiento de Azure**

  Disponible en las propiedades de su cuenta de almacenamiento, en la sección Claves de acceso. Puede utilizar cualquiera de las claves (clave1 o clave2).

Si está implementando el Servidor de administración en Google Cloud, debe seleccionar una carpeta donde se almacenarán las copias de seguridad. Seleccione una carpeta en su dispositivo local o una carpeta en una instancia de máquina virtual.

El botón **Siguiente** se vuelve disponible después de la creación de todas las directivas y tareas que son necesarias para la configuración mínima de la protección.

Si un servidor en el que se supone que las tareas deben ejecutarse no es visible para el Servidor de administración, las tareas se inician solo cuando el dispositivo se vuelve visible. Si crea una nueva instancia de EC2 o una nueva máquina virtual de Azure, puede tomar algún tiempo antes de que sea visible para el Servidor de administración. Si desea que el Agente de red y las aplicaciones de seguridad se instalen en todos los dispositivos recién creados tan pronto como sea posible, asegúrese de que la opción **Ejecutar tareas pendientes** esté activada para las tareas de **instalación remota de la aplicación**. De lo contrario, una instancia/máquina virtual recién creada no obtendrá el Agente de red y las aplicaciones de seguridad hasta que la tarea comience de acuerdo con su programación.

Paso 8. Seleccionar la acción cuando el sistema operativo debe reiniciarse durante la instalación (para el entorno de nube)

Si seleccionó anteriormente **Desplegar protección**, debe elegir qué hacer cuando se deba reiniciar el sistema operativo de un dispositivo de destino. Si no seleccionó la opción **Desplegar protección**, este paso se omitirá.

Seleccione si reiniciar instancias si el sistema operativo de su dispositivo debe reiniciarse durante la instalación de aplicaciones:

- **No reiniciar el dispositivo**

  Si se selecciona esta opción, el dispositivo no se reiniciará después de la instalación de la aplicación de seguridad.

- **Reiniciar el dispositivo**

  Si se selecciona esta opción, el dispositivo se reiniciará después de la instalación de la aplicación de seguridad.

Si desea forzar el cierre de todas las aplicaciones en sesiones bloqueadas en las instancias antes del reinicio, seleccione la casilla **Forzar el cierre de aplicaciones en sesiones bloqueadas**. Si se desactiva esta casilla, deberá cerrar manualmente todas las aplicaciones que se ejecutan en instancias bloqueadas.

Paso 9. Recepción de actualizaciones por un Servidor de administración

En este paso, puede ver el progreso de la descarga de actualizaciones necesarias para el correcto funcionamiento del Servidor de administración. Puede hacer clic en el botón **Siguiente** sin esperar a que la descarga finalice para ir a la página final del Asistente.

El Asistente finaliza.

Comprobación de la configuración

Para comprobar si Kaspersky Security Center 14 está correctamente configurado para funcionar en el entorno de nube:

1. Inicie Kaspersky Security Center y asegúrese de que puede conectarse al Servidor de administración a través de la Consola de administración.
2. En el árbol de consola, seleccione **Dispositivos administrados\Cloud**.
3. Al ver a cualquier de los subgrupos en el grupo **Dispositivos administrados\Cloud**, asegúrese de que la ficha **Dispositivos** muestre todas los dispositivos de ese subgrupo.

   Si no se muestran los dispositivos, puede sondear manualmente los segmentos de la nube correspondientes para encontrarlos.
4. Asegúrese de que la ficha **Directivas** tenga directivas activas para las siguientes aplicaciones:
   - Agente de red de Kaspersky Security Center
   - Kaspersky Security for Windows Server

- Kaspersky Endpoint Security for Linux

Si no están en la lista, puede crearlos manualmente.

5. Asegúrese que la ficha **Tareas** enumere las tareas siguientes:

   - **Copia de seguridad de los datos del Servidor de administración**
   - **Tarea de actualización para Windows Server**
   - **Mantenimiento de bases de datos**
   - **Descargar actualizaciones en el repositorio del Servidor de administración**
   - **Buscar vulnerabilidades y actualizaciones requeridas**
   - **Instalar protección para Windows**
   - **Instalar protección para Linux**
   - **Tarea de análisis rápido para Windows Server**
   - **Análisis rápido**
   - **Instalar actualizaciones para Linux**

   Si no están en la lista, puede crearlos manualmente.

Kaspersky Security Center 14 está correctamente configurado para funcionar en el entorno de nube.

Grupo de dispositivos de Cloud

Puede administrar dispositivos en la nube combinándolos en grupos. En la etapa de configuración inicial de Kaspersky Security Center, se crea el grupo de administración **Dispositivos administrados\Cloud** de forma predeterminada y los dispositivos en la nube detectados durante el sondeo se colocan en este grupo.

Si seleccionó la opción **Sincronizar la estructura del grupo de administración con el segmento de la nube** cuando configuró la sincronización, la estructura de los subgrupos en este grupo de administración es idéntica a la estructura de sus segmentos de la nube. (sin embargo, en AWS, las zonas de disponibilidad y los grupos de ubicación no están representados en la estructura; en Microsoft Azure, las subredes no están representadas en la estructura). Los subgrupos vacíos del grupo que se detectan durante el sondeo automáticamente se eliminan.

También puede crear manualmente grupos de administración al combinar todos los dispositivos específicos.

De forma predeterminada, el grupo **Dispositivos administrados\Cloud** hereda las directivas y tareas desde el grupo **Dispositivos administrados**. Puede cambiar la configuración si las casillas **Edición permitida** se selecciona en las propiedades de la configuración de las directivas y tareas correspondientes.

Sondeo de segmentos de la red

El Servidor de administración recibe información sobre la estructura de la red y sus dispositivos mediante sondeos regulares de los segmento de la nube utilizando herramientas API de AWS, API de Azure o API de Google. Kaspersky Security Center usa esta información para actualizar los contenido de los **Dispositivos no asignados** y las carpetas **Dispositivos administrados**. Si configuró dispositivos para que se trasladen de forma automática a grupos de administración, los dispositivos detectados se incluirán en los grupos de administración.

Para permitir que un Servidor de administración sondee segmentos de la nube, debe tener los derechos con una función de IAM o una cuenta de usuario de IAM (en AWS) o con un Id. de la aplicación y contraseña (en Azure), o con un correo electrónico de cliente de Google un ID de proyecto de Google y una clave privada.

Puede añadir y eliminar conexiones, así como configurar la planificación del sondeo de cada segmento de la nube.

Añadir conexiones para sondear segmentos de la nube

Para añadir una conexión para el sondeo de segmentos de la nube a la lista de conexiones disponibles:

1. En el árbol de consola, seleccione el nodo **Detección de dispositivos** → **Cloud**.
2. En el espacio de trabajo de la ventana, haga clic en **Configurar sondeo**.

   Una ventana de propiedades se abre con una lista de conexiones disponibles para el sondeo de segmentos de la nube.
3. Haga clic en el botón **Agregar**.

   Se abre la ventana **Conexión**.
4. Especifique el nombre del entorno de nube para la conexión que se utilizará para seguir sondeando el segmento de la nube:

   Entorno de nube

   El entorno en el que se ubican las instancias (o máquinas virtuales) de EC2 puede ser Amazon Web Services (AWS), Microsoft Azure o Google Cloud.

   Si ha seleccionado AWS, especifique la siguiente configuración:

   - **Nombre de conexión**

     Introduzca un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres de Unicode.

     Este nombre también se utilizará como el nombre del grupo de administración para los dispositivos de la nube.

     Si planea trabajar con más de un entorno de nube, es posible que desee incluir el nombre del entorno en el nombre de la conexión, por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google".

   - **Usar función AWS IAM**

     Seleccione esta opción si ya ha creado una función de IAM para que el Servidor de administración use los servicios de AWS.

   - **Usar la cuenta de usuario AWS IAM**

Seleccione esta opción si tiene una cuenta de usuario de IAM con los permisos necesarios y puede introducir una ID de clave y una clave secreta.

- **Id. de clave de acceso**

  El Id. de clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Recibió el ID de clave cuando creó la cuenta de usuario de IAM.

  El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

- **Clave secreta**

  La clave secreta que recibió con el Id. de clave de acceso cuando creó la cuenta de usuario de IAM.

  Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a introducir la clave secreta, aparecerá el botón **Mostrar**. Haga clic y mantenga pulsado este botón durante la cantidad de tiempo necesaria para ver los caracteres que introdujo.

  El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

El Asistente de configuración del entorno de nube le permite especificar solo una clave de acceso de AWS IAM. Posteriormente, puede especificar más conexiones para administrar otros segmentos de la nube.

Si ha seleccionado Azure, especifique la siguiente configuración:

- **Nombre de conexión**

  Introduzca un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres de Unicode.

  Este nombre también se utilizará como el nombre del grupo de administración para los dispositivos de la nube.

  Si planea trabajar con más de un entorno de nube, es posible que desee incluir el nombre del entorno en el nombre de la conexión, por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google".

- **Id. de la aplicación en Azure**

  Usted creó este Id. de la aplicación en el portal de Azure.

  Solo puede proporcionar un Id. de la aplicación en Azure para sondeos y otros fines. Si desea sondear otro segmento de Azure, primero debe eliminar la conexión de Azure existente.

- **Id. de suscripción de Azure**

  Usted creó la suscripción en el portal de Azure.

- **Contraseña de la aplicación Azure**

Recibió la contraseña del Id. de la aplicación cuando creó el Id. de la aplicación.

Los caracteres de la contraseña se muestran como asteriscos. Después de empezar a introducir la contraseña, el botón **Mostrar** estará disponible. Haga clic y mantenga presionado este botón para ver los caracteres que introdujo.

- **Nombre de la cuenta de almacenamiento de Azure**

  Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Clave de acceso al almacenamiento de Azure**

  Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  La clave está disponible en la sección "Descripción general de la cuenta de almacenamiento de Azure", en la subsección "Claves".

Si ha seleccionado Google Cloud, especifique la siguiente configuración:

- **Nombre de conexión**

  Introduzca un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres de Unicode.

  Este nombre también se utilizará como el nombre del grupo de administración para los dispositivos de la nube.

  Si planea trabajar con más de un entorno de nube, es posible que desee incluir el nombre del entorno en el nombre de la conexión, por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google".

- **Correo electrónico del cliente**

  El correo electrónico del cliente es el correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. de proyecto**

  El id. del proyecto es el id. que recibió cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La clave privada es la secuencia de caracteres que recibió como clave privada cuando registró su proyecto en Google Cloud. Es posible que desee copiar y pegar esta secuencia para evitar errores.

5. Si lo desea, seleccione **Establecer programación de sondeo** y cambiar la configuración predeterminada.

La conexión se guarda en la configuración de la aplicación.

Después de sondear por primera vez un nuevo segmento de la nube, aparece un subgrupo correspondiente a ese segmento en el grupo de administración **Dispositivos administrados\Cloud**.

Si especifica credenciales incorrectas, no se encontrarán instancias durante el sondeo del segmento de la nube y no aparecerá un nuevo subgrupo en el grupo de administración **Dispositivos administrados\Cloud**.

Eliminar conexiones para sondear segmentos de la nube

Si ya no tiene que sondear un segmento específico de la nube, puede eliminar la conexión correspondiente a ese segmento en la lista de conexiones disponibles. También puede eliminar una conexión si, por ejemplo, los permisos para sondear un segmento de la nube se han transferido al otro usuario AWS IAM con otra clave.

Para eliminar una conexión:

1. En el árbol de consola, seleccione el nodo **Detección de dispositivos → Cloud**.
2. En el espacio de trabajo de la ventana, seleccione **Configurar sondeo**.

   Una ventana se abre con una lista de conexiones disponibles para el sondeo de segmentos de la nube.
3. Seleccione la conexión que desea eliminar y haga clic en el botón **Eliminar** en la parte derecha de la ventana.
4. En la ventana que se abre, haga clic en el botón **Aceptar** para confirmar su selección.

Si está eliminando conexiones de la lista de conexiones disponibles, los dispositivos que se encuentran en los segmentos correspondientes se eliminan automáticamente de los grupos de administración correspondiente.

Configurar la planificación del sondeo

El sondeo de segmentos de la nube se realiza según programación. Puede configurar la frecuencia del sondeo.

La frecuencia del sondeo está automáticamente configurada en 5 minutos por el Asistente de configuración del entorno de nube Puede cambiar este valor en cualquier momento y configurar otra planificación. Sin embargo, no se recomienda configurar el sondeo para que se ejecute con una frecuencia mayor a cada 5 minutos, porque esto podría dar lugar a errores en el funcionamiento de la API.

Para configurar una planificación de sondeo de segmentos de la nube:

1. En el árbol de consola, seleccione el nodo **Detección de dispositivos → Cloud**.
2. En el espacio de trabajo, haga clic en **Configurar sondeo**.

   Se abre la ventana de propiedades de la nube.
3. En la lista, seleccione la conexión que desea y haga clic en el botón **Propiedades**.

   Se abre la ventana de propiedades de la conexión.
4. En la ventana de propiedades, haga clic en **Establecer programación de sondeo**.

   Se abre la ventana **Programación**.

5. Defina los siguientes parámetros:

- **Inicio programado**

  Opciones de planificación de sondeo:

  - Cada N días

    El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

    De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.

  - Cada N minutos

    El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.

    De forma predeterminada, el sondeo se ejecuta cada cinco minutos, a partir de la hora actual del sistema.

  - Por días de la semana

    El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.

    De forma predeterminada, el sondeo se realiza todos los viernes a las 6:00:00 p.m.

  - Cada mes, en días concretos de las semanas seleccionadas

    El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.

    De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 6:00:00 p.m.

- Ejecutar tareas no realizadas

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de que se encienda o esperar a la próxima vez que se programe el sondeo.

  Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de que se encienda.

  Si esta opción está desactivada, el Servidor de administración espera a la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

6. Haga clic en **Aceptar** para guardar los cambios.

El horario de sondeo está configurado y guardado.

Instalación de aplicaciones en dispositivos en un entorno de nube

Puede instalar las siguientes aplicaciones de Kaspersky en los dispositivos en un entorno de nube: Kaspersky Security for Windows Server (para dispositivos Windows) y Kaspersky Endpoint Security para Linux (para dispositivos Linux).

Los dispositivos cliente en los cuales tiene la intención de instalar la protección deben cumplir con los requisitos para la operación de Kaspersky Security Center en el entorno de nube. Debe tener una licencia válida para instalar aplicaciones en instancias de AWS, en máquinas virtuales de Microsoft Azure o en instancias de máquina virtual de Microsoft Azure.

Kaspersky Security Center 14 admite los siguientes escenarios:

- Un dispositivo cliente se descubre mediante una API; la instalación también se realiza mediante una API. Este escenario se admite para entornos de nube de AWS y Azure.
- Un dispositivo cliente se descubre mediante sondeo de Active Directory, sondeo de dominios de Windows o sondeo de rango de IP; la instalación se realiza a través de Kaspersky Security Center.
- Un dispositivo cliente se descubre mediante una API; la instalación se realiza mediante Kaspersky Security Center. Para Google Cloud, solo se admite este escenario.

No se admiten otras formas de instalación de las aplicaciones.

Para instalar aplicaciones en dispositivos virtuales, use paquetes de instalación.

Para crear una tarea de instalación remota de la aplicación en instancias utilizando la API de AWS o la API de Azure:

1. En el árbol de consola, seleccione la carpeta **Tareas**.
2. Haga clic en el botón **Nueva tarea**.

   Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.
3. En la página **Seleccionar el tipo de tarea**, seleccione **Instalar aplicación en remoto** como tipo de tarea.
4. En la página **Seleccionar dispositivos**, seleccione los dispositivos relevantes del grupo **Dispositivos administrados\Cloud**.
5. Si el Agente de red todavía no se ha instalado en los dispositivos donde pretende instalar la aplicación, en la página **Seleccionar una cuenta para ejecutar la tarea**, seleccione **Se necesita una cuenta (no se utiliza Agente de red)** y haga clic en el botón **Agregar** en la parte derecha de la ventana. En el menú que aparece seleccione uno de lo siguiente:

   - Cuenta en la nube

Seleccione esta opción si desea instalar aplicaciones en instancias en AWS y tiene una clave de acceso de AWS IAM con los permisos necesarios pero no tiene una función de IAM. También seleccione esta opción si desea instalar aplicaciones en dispositivos en el entorno de Azure.

En la ventana que se abre, proporcione a Kaspersky Security Center las credenciales que le otorguen derechos para instalar aplicaciones en los dispositivos pertinentes.

Seleccione el entorno de nube: AWS o Azure.

En el campo **Nombre de la cuenta**, introduzca un nombre para estas credenciales. Este nombre aparecerá en la lista de cuentas para ejecutar la tarea.

Si seleccionó AWS, en los campos **Id. de clave de acceso** y **Clave secreta**, introduzca las credenciales para la cuenta de usuario de IAM que tiene los derechos para instalar aplicaciones en los dispositivos especificados.

Si seleccionó Azure, en los campos **Id. de suscripción de Azure** y **Contraseña de la aplicación Azure** introduzca las credenciales para la cuenta de Azure que tiene los derechos para instalar aplicaciones en los dispositivos especificados.

Si especifica credenciales incorrectas, la tarea de instalación remota terminará con un error en los dispositivos para los que está programada.

- **Cuenta**

  Para instancias que ejecutan Windows, seleccione esta opción en caso de que no tenga la intención de instalar la aplicación utilizando las herramientas de AWS o API de Azure. En este caso, asegúrese de que los dispositivos en su segmento de la nube cumplan con las condiciones necesarias. Kaspersky Security Center instala aplicaciones por sí solo, sin utilizar API de AWS o API de Azure.

  Si especifica datos incorrectos, la tarea de instalación remota terminará con un error en los dispositivos para los que está programada.

- **Función de IAM**

  Seleccione esta opción si desea instalar aplicaciones en las instancias del entorno de AWS y tiene una función de IAM con los derechos necesarios.

  Si selecciona esta opción pero no tiene una función de IAM con los derechos necesarios, la tarea de instalación remota terminará con un error en los dispositivos para los que está programada.

- **Certificado SSH**

  Para instancias que ejecutan Linux, seleccione esta opción en caso de que no tenga la intención de instalar la aplicación utilizando las herramientas de AWS o API de Azure. En este caso, asegúrese de que los dispositivos en su segmento de la nube cumplan con las condiciones necesarias. Kaspersky Security Center instala aplicaciones por sí solo, sin utilizar API de AWS o API de Azure.

Puede proporcionar varias credenciales haciendo clic en el botón **Agregar** para cada una nueva. Si diferentes segmentos de la nube requieren diferentes credenciales, proporcione las credenciales de todos los segmentos.

Después de finalizar el Asistente, la tarea para la instalación remota de la aplicación aparece en la lista de tareas en el espacio de trabajo de la carpeta **Tareas**.

En Microsoft Azure, la instalación remota de aplicaciones de seguridad en una máquina virtual puede tener como resultado la eliminación de la extensión de script personalizada instalada en la máquina virtual.

Visualización de las propiedades de dispositivos de la nube

Para ver las propiedades de un dispositivo de la nube, siga estos pasos:

1. En el árbol de consola, en el nodo **Detección de dispositivos** → **Cloud**, seleccione el subnodo que se corresponda con el grupo donde se encuentra la instancia relevante.

   Si no conoce el grupo donde se encuentra el dispositivo virtual relevante, use la función de búsqueda:

   a. Haga clic derecho en el nombre del nodo **Dispositivos administrados** → **Nube** y luego seleccione **Buscar** en el menú contextual.

   b. En la ventana que se abre, realice una búsqueda.

      Si un dispositivo cumple los criterios que usted establece, se mostrarán su nombre y detalles en la parte inferior de la ventana.

2. Haga clic con el botón derecho en el nombre del nodo relevante. En el menú contextual, seleccione **Propiedades**.

   En la ventana que se abre, se muestran las propiedades del objeto.

   La **sección Información del sistema** → **Información general del sistema** contiene las propiedades que son específicas para dispositivos en un entorno de nube:

   - **Dispositivo descubierto mediante API** (**AWS**, **Azure** o **Google Cloud**; si el dispositivo no se puede detectar mediante herramientas API, se muestra el valor **No**).
   - **Región de la nube**.
   - **Cloud VPC** (solo para dispositivos de AWS y Google Cloud).
   - **Zona de disponibilidad en la nube** (solo para dispositivos de AWS y Google Cloud).
   - **Subred de nube**.
   - **Grupo de ubicación en la nube** (esta unidad solo se muestra si la instancia pertenece a un grupo de ubicación; de lo contrario, no se muestra).

Puede hacer clic en el botón **Exportar a archivo** si desea exportar esta información a un archivo CSV o TXT.

Sincronización con la nube

Durante el funcionamiento del Asistente de configuración del entorno de nube, Sincronizar con Cloud se crea automáticamente. Esta regla le permite mover automáticamente las instancias detectadas en cada sondeo, desde el grupo **Dispositivos no asignados** al grupo **Dispositivos administrados\Cloud** para poner estas instancias a disposición para la administración centralizada. De forma predeterminada, la regla está activa tras crearse. Puede desactivar, modificar o aplicar la regla en cualquier momento.

Para modificar las propiedades de la regla Sincronizar con Cloud y / o aplicar la regla:

1. En el árbol de consola, haga clic con el botón derecho en el nombre del nodo de **Detección de dispositivos**.

2. En el menú contextual, seleccione **Propiedades**.

3. En la ventana de propiedades que se abre, en el panel **Secciones**, seleccione **Mover dispositivos**.

4. En la lista de reglas de movimiento de dispositivos en el espacio de trabajo, seleccione **Sincronizar con la nube** y haga clic en el botón **Propiedades** en la parte inferior de la ventana.

   Se abre la ventana de propiedades de la regla.

5. Si es necesario, especifique la siguiente configuración en el grupo de configuración de **segmentos de la nube**:

   - **El dispositivo está en un segmento de la nube**

     La regla solo se aplica a los dispositivos que se encuentran en el segmento de la nube seleccionado. De lo contrario, la regla se aplica a todos los dispositivos que han sido detectados.

     Esta opción está seleccionada de forma predeterminada.

     - **Incluir objetos secundarios**

       La regla se aplica a todos los dispositivos en el segmento seleccionado y a todas las subsecciones de la nube anidadas. De lo contrario, la regla solo se aplicará a los dispositivos que estén en el segmento raíz.

       Esta opción está seleccionada de forma predeterminada.

     - **Mover dispositivos desde objetos anidados a subgrupos correspondientes**

       Si esta opción está activada, los dispositivos se mueven automáticamente a los subgrupos que corresponden a su estructura.

       Si esta opción está desactivada, los dispositivos de los objetos anidados se mueven automáticamente a la raíz del subgrupo de la nube sin ninguna otra ramificación.

       Esta opción está activada de forma predeterminada.

       - **Crear subgrupos correspondientes a contenedores de dispositivos recién detectados**

         Si esta opción está activada, cuando la estructura del grupo **Dispositivos administrados\Cloud** no tiene subgrupos que coincidan con la sección que contiene el dispositivo, Kaspersky Security Center crea tales subgrupos. Por ejemplo, si se descubre una nueva subred durante la detección de dispositivos, se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Grupo nube**.

         Si esta opción está desactivada, Kaspersky Security Center no crea ningún subgrupo nuevo. Por ejemplo, si se descubre una nueva subred durante el sondeo de la red, no se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**, y los dispositivos que se encuentran en esa subred se moverán al grupo **Dispositivos administrados\Cloud**.

         Esta opción está activada de forma predeterminada.

       - **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube**

Si esta opción está activada, la aplicación elimina del grupo de la nube todos los subgrupos que no coinciden con ningún objeto de nube existente.

Si esta opción está desactivada, se conservan los subgrupos que no coinciden con ninguno de los objetos de nube existentes.

Esta opción está activada de forma predeterminada.

Si ha activado la opción **Sincronizar con la nube** al ejecutar el Asistente de configuración del entorno de nube, se crea la regla Sincronizar con la nube con las casillas **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente** y **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube** marcadas.

Si no activó la opción **Sincronizar con la nube**, la regla Sincronizar con la nube se crea con estas opciones desactivadas (eliminadas). Si su trabajo con Kaspersky Security Center requiere que la estructura de los subgrupos en el subgrupo **Dispositivos administrados\Cloud** coincida con la estructura de segmentos de la nube, active las opciones **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente** y **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube** en las propiedades de la regla y, a continuación, aplique la regla.

6. En la lista desplegable **Dispositivo descubierto mediante la API**, seleccione uno de los siguientes valores:

   - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de AWS.
   - **Azure**. El dispositivo se descubre mediante la Azure API, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
   - **Google Cloud.** El dispositivo se descubre mediante la API de Google, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de Google.
   - **No**. El dispositivo no se puede detectar con AWS, Azure o Google API, es decir, o bien está fuera del entorno de nube, o está en el entorno de nube pero no se puede detectar mediante API por algún motivo.
   - Ningún valor. Este criterio no se puede aplicar.

7. Si es necesario, configure otras propiedades de reglas en otras secciones.

8. Si es necesario, aplique la regla haciendo clic en el botón **Forzar** en la parte inferior de la ventana.

   Se inicia el Asistente de ejecución de reglas. Siga las instrucciones del Asistente. Cuando finalice el Asistente, la regla se ejecutará y la estructura de subgrupos en el subgrupo **Dispositivos administrados\nube** coincidirá con la estructura de sus segmentos de la nube.

9. Haga clic en el botón **Aceptar**.

Las propiedades están configuradas y guardadas.

Para desactivar la regla Sincronizar con la nube, realice lo siguiente:

1. En el árbol de consola, haga clic con el botón derecho en el nombre del nodo de **Detección de dispositivos**.
2. En el menú contextual, seleccione **Propiedades**.
3. En la ventana de propiedades que se abre, en el panel **Secciones**, seleccione **Mover dispositivos**.

4. En la lista de reglas de movimiento de dispositivos en el espacio de trabajo, desactive (elimine) la opción **Sincronizar con la nube** y haga clic en **Aceptar**.

La regla está desactivada y ya no se aplicará.

Uso de scripts de despliegue para desplegar programas de seguridad

Cuando Kaspersky Security Center se despliega en un entorno de nube, puede usar scripts de despliegue para automatizar el despliegue de las aplicaciones de seguridad. Los scripts de despliegue para Amazon Web Services, Microsoft Azure y Google Cloud están disponibles como archivos ZIP en la página de Soporte de Kaspersky.

Puede desplegar las últimas versiones de Kaspersky Endpoint Security for Linux y Kaspersky Security for Windows Server mediante el uso de scripts de despliegue solo si ya ha creado paquetes de instalación y complementos de administración para estos programas. Para desplegar las últimas versiones de las aplicaciones de seguridad mediante el uso de scripts de despliegue, realice lo siguiente en el Servidor de administración en el entorno de nube:

1. Ejecute el Asistente de configuración del entorno de nube.

2. Siga las instrucciones proporcionadas en https://support.kaspersky.com/14713.

Despliegue de Kaspersky Security Center en Yandex.Cloud

Puede implementar Kaspersky Security Center en Yandex.Cloud. Solo está disponible el modo de pago por uso; no se admiten bases de datos de nube.

En Yandex.Cloud están disponibles los siguientes métodos de implementación para las aplicaciones de seguridad:

- Por funciones propias de Kaspersky Security Center, es decir, a través de la tarea de *Instalación remota* (el despliegue de los programas de seguridad solo es posible si el Servidor de administración y las máquinas virtuales que se pretende proteger están en el mismo segmento de red)

- A través de scripts de despliegue

Para la implementación de Kaspersky Security Center en Yandex.Cloud, debe tener una cuenta de servicio en Yandex.Cloud. Debe otorgar a esta cuenta el permiso marketplace.meteringAgent y asociarla con la máquina virtual (consulte https://cloud.yandex.com/en para obtener más detalles).

Apéndices

Esta sección proporciona información de referencia y datos adicionales para usar Kaspersky Security Center.

Funciones avanzadas

Esta sección describe un rango de opciones adicionales de Kaspersky Security Center diseñadas para ampliar la funcionalidad de la administración centralizada de aplicaciones en dispositivos.

Funcionamiento automático de Kaspersky Security Center. Utilidad klakaut

Puede automatizar la operación de Kaspersky Security Center usando la utilidad klakaut. La utilidad klakaut y su sistema de ayuda se encuentran en la carpeta de instalación de Kaspersky Security Center.

Herramientas personalizadas

Kaspersky Security Center permite crear una lista de *herramientas personalizadas* (en adelante *herramientas*), es decir, aplicaciones activadas para un dispositivo cliente desde la Consola de administración, mediante el grupo **Herramientas personalizadas** del menú contextual. Cada herramienta de la lista se asociará con un comando de menú independiente que la Consola de administración utiliza para iniciar la aplicación correspondiente a esa herramienta.

Las aplicaciones se inician en la estación de trabajo del administrador. La aplicación puede aceptar los atributos de un dispositivo cliente remoto como argumentos de la línea de comandos (nombre NetBIOS, nombre DNS, dirección IP). La conexión con el dispositivo remoto puede establecerse mediante la conexión de túnel.

De forma predeterminada, la lista de herramientas personalizadas contiene los siguientes programas de servicio para cada dispositivo cliente:

- **Diagnósticos remotos** es una utilidad para realizar diagnósticos remotos de Kaspersky Security Center.
- **Escritorio remoto** es un componente estándar de Microsoft Windows denominado Conexión a Escritorio remoto.
- **Administración de equipos** es un componente estándar de Microsoft Windows.

Para agregar o quitar herramientas personalizadas, o editar sus parámetros,

En el menú contextual del dispositivo cliente, seleccione **Herramientas personalizadas → Configurar herramientas personalizadas**.

Se abre la ventana **Herramientas personalizadas**. En esta ventana, puede añadir o quitar herramientas personalizadas y editar los parámetros mediante los botones **Agregar**, **Modificar** y **Quitar** ( ).

Modo de clonación de disco del Agente de red

Clonar el disco duro de un dispositivo de referencia es un método popular para instalar software en dispositivos nuevos. Si el Agente de red se está ejecutando en modo estándar en el disco duro del dispositivo de referencia, surge el siguiente problema:

Una vez que la imagen del disco de referencia con el Agente de red se despliega en los dispositivos nuevos, aparecen bajo un solo icono en la Consola de administración. Este problema se produce porque la clonación hace que los nuevos dispositivos conserven datos internos idénticos, lo cual permite al Servidor de administración asociar un dispositivo con un icono en la Consola de administración.

El *modo de clonación de disco del Agente de red* especial permite evitar dichos problemas de visualización incorrecta de los nuevos dispositivos en la Consola de administración después de la clonación. Use este modo cuando despliegue software (con el Agente de red) en nuevos dispositivos mediante clonación del disco.

En el modo de clonación de disco, el Agente de red sigue ejecutándose, pero no se conecta al Servidor de administración. Al salir del modo de clonación, el Agente de red elimina los datos internos, que hacen que el Servidor de administración asocie varios dispositivos con un único icono en la Consola de administración. Después de completar la clonación de la imagen del dispositivo de referencia, los nuevos dispositivos se mostrarán correctamente en la Consola de administración (con iconos individuales).

Caso de uso del modo de clonación de disco del Agente de red

1. El administrador instala el Agente de red en un dispositivo de referencia.
2. El administrador comprueba la conexión entre el Agente de red y el Servidor de administración con la utilidad klnagchk.
3. El administrador activa el modo de clonación de disco del Agente de red.
4. El administrador instala software y parches en el dispositivo, y lo reinicia las veces que sea necesario.
5. El administrador clona el disco duro del dispositivo de referencia en cualquier cantidad de dispositivos.
6. Cada copia clonada debe reunir estas condiciones:
   a. El nombre del dispositivo debe cambiarse.
   b. Se debe reiniciar el dispositivo.
   c. El modo de clonación de disco se debe desactivar.

Activación y desactivación del modo de clonación con la utilidad klmover

Para activar o desactivar el modo de clonación de disco del Agente de red:

1. Ejecute la utilidad klmover en el dispositivo donde esté instalado el Agente de red que necesite clonar.
   La utilidad klmover se encuentra en la carpeta de instalación del Agente de red.
2. Para activar el modo de clonación de disco, escriba el comando siguiente en la solicitud de comando de Windows: `klmover -cloningmode 1`.
   El Agente de red cambia al modo de clonación de disco.
3. Para solicitar el estado actual del modo de clonación de disco, escriba el comando siguiente en la solicitud de comando: `klmover -cloningmode`.
   La ventana de la utilidad muestra si se ha activado o desactivado el modo de clonación de disco.
4. Para desactivar el modo de clonación de disco, introduzca el siguiente comando en la línea de comando de utilidad: `klmover -cloningmode 0`.

Preparación de un dispositivo de referencia con el Agente de red instalado para crear una imagen del sistema operativo

Es posible que desee crear una imagen del sistema operativo de un dispositivo de referencia con el Agente de red instalado y luego implementar la imagen en los dispositivos en red. En este caso, crea una imagen del sistema operativo de un dispositivo de referencia en el que el Agente de red aún no se ha iniciado. Si inicia el Agente de red en un dispositivo de referencia antes de crear una imagen del sistema operativo, la identificación del Servidor de administración de los dispositivos implementados desde una imagen del sistema operativo del dispositivo de referencia será problemática.

Para preparar el dispositivo de referencia para crear una imagen del sistema operativo:

1. Asegúrese de que el sistema operativo Windows esté instalado en el dispositivo de referencia e instale el otro software que necesita en ese dispositivo.

2. En el dispositivo de referencia, en la configuración de Conexiones de red de Windows, desconecte el dispositivo de referencia de la red donde está instalado Kaspersky Security Center.

3. En el dispositivo de referencia, inicie la instalación local del Agente de red utilizando el archivo setup.exe.

   Se inicia el Asistente de instalación del Agente de red de Kaspersky Security Center. Siga las instrucciones del Asistente.

4. En la página **Servidor de administración** del Asistente, especifique la dirección IP del Servidor de administración.

   Si no conoce la dirección exacta del Servidor de administración, introduzca localhost. Puede cambiar la dirección IP más tarde utilizando la utilidad klmover con la clave `-address`.

5. En la página **Inicio de la aplicación** del Asistente, desactive la opción **Iniciar aplicación durante la instalación**.

6. Cuando finalice la instalación del Agente de red, no reinicie el dispositivo antes de crear una imagen del sistema operativo.

   Si reinicia el dispositivo, deberá repetir todo el proceso de preparación de un dispositivo de referencia para crear una imagen del sistema operativo.

7. En el dispositivo de referencia, en la línea de comando, inicie la utilidad sysprep y ejecute el siguiente comando: `sysprep.exe /generalize /oobe /shutdown`.

El dispositivo de referencia está listo para crear una imagen del sistema operativo.

Configuración de la recepción de mensajes desde Monitor de integridad de archivos

Las aplicaciones administradas, como Kaspersky Security for Windows Server o Kaspersky Security for Virtualization Light Agente, envían mensajes desde Monitor de integridad de archivos a Kaspersky Security Center. Kaspersky Security Center también le permite supervisar cualquier cambio en los componentes importantes de los sistemas (por ejemplo, servidores web y cajeros automáticos) y responder lo antes posible de amenazas a la integridad de tales sistemas. Para este fin, puede recibir mensajes del componente Monitor de integridad de archivos. El componente Monitor de integridad de archivos no solo le permite supervisar el sistema de archivos de un dispositivo, sino también los subárboles de registro, el estado del firewall y el estado del hardware conectado.

Debe configurar Kaspersky Security Center para recibir mensajes del componente Monitor de integridad de archivos sin usar Kaspersky Security for Windows Server o Kaspersky Security for Virtualization Light Agent.

Para configurar la recepción de mensajes desde Monitor de integridad de archivos:

1. Abra el registro del sistema del dispositivo en el que está instalado el Servidor de administración (por ejemplo, de forma local con el comando regedit en el menú **Iniciar** → **Ejecutar**).

2. Vaya al siguiente subárbol:

   - Para un sistema de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

   - Para un sistema de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

3. Creación de claves:

   - Cree la clave KLSRV_EVP_FIM_PERIOD_SEC para especificar el período de tiempo para contar el número de eventos procesados. Especifique los siguientes parámetros:

     a. Especifique KLSRV_EVP_FIM_PERIOD_SEC como nombre de la clave.

     b. Especifique DWORD como tipo de clave.

     c. Especifique un intervalo de valores para el intervalo de tiempo desde 43.200 hasta 172.800 segundos. De forma predeterminada, el intervalo de tiempo es 86.400 segundos.

   - Cree la clave KLSRV_EVP_FIM_LIMIT para limitar el número de eventos recibidos para el intervalo de tiempo especificado. Especifique los siguientes parámetros:

     a. Especifique KLSRV_EVP_FIM_LIMIT como nombre de la clave.

     b. Especifique DWORD como tipo de clave.

     c. Especifique un intervalo de valores para eventos recibidos desde 2000 hasta 50 000. El número predeterminado de eventos es de 20 000.

   - Cree la clave KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC para contar eventos con exactitud hasta un intervalo de tiempo específico. Especifique los siguientes parámetros:

     a. Especifique KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC como nombre de la clave.

     b. Especifique DWORD como tipo de clave.

     c. Especifique un intervalo de valores desde 120 hasta 600 segundos. De forma predeterminada, el intervalo de tiempo es 300 segundos.

   - Cree la clave KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC de modo que, después de la cantidad de tiempo especificada, la aplicación puede comprobar si el número de eventos procesados en el intervalo de tiempo está resultando ser menos que el límite especificado. Esta comprobación se realiza después de alcanzar el límite de eventos recibidos. Si esta condición se cumple, la aplicación vuelve a guardar eventos en la base de datos. Especifique los siguientes parámetros:

     a. Especifique KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC como tipo de clave.

     b. Especifique DWORD como tipo de clave.

     c. Especifique un intervalo de valores desde 600 hasta 3.600 segundos. De forma predeterminada, el intervalo de tiempo es 1.800 segundos.

Si las claves no se crean, los valores predeterminados se utilizan.

4. Reinicie el servicio del Servidor de administración.

Se configurarán los límites de la recepción de eventos desde el componente Monitor de integridad de archivos. Puede ver los resultados del componente Monitor de integridad de archivos en los informes denominados **Las 10 reglas del Monitor de integridad de archivos/Control de integridad del sistema que se activaron en los dispositivos la mayoría de las veces** y **Los 10 principales dispositivos en los que las reglas de Monitor de integridad de archivos/Control de integridad del sistema se activan con mayor frecuencia**.

Mantenimiento del Servidor de administración

El mantenimiento del Servidor de administración le permite reducir el volumen de la base de datos y mejorar el rendimiento y la fiabilidad del funcionamiento de la aplicación. Le recomendamos realizar un mantenimiento del Servidor de administración por lo menos una vez a la semana.

El mantenimiento del Servidor de administración se lleva a cabo a través de la tarea especializada. La aplicación realiza las acciones siguientes durante el mantenimiento del Servidor de administración:

- Comprueba la base de datos en busca de errores.
- Reorganiza los índices de la base de datos.
- Actualiza las estadísticas de la base de datos.
- Reduce la base de datos (si es necesario).

La tarea *Mantenimiento del Servidor de administración* no admite MariaDB. Si se utiliza este DBMS en su red, los administradores deberán mantener MariaDB por su cuenta.

Para crear la tarea Mantenimiento del Servidor de administración:

1. En el árbol de consola, seleccione el nodo del Servidor de administración para el que desea crear la tarea de *Mantenimiento del Servidor de administración*.
2. Seleccione la carpeta **Tareas**.
3. Haga clic en el botón **Nueva tarea** en el espacio de trabajo de la carpeta **Tareas**.

   Se inicia el Asistente para añadir tareas.
4. En la ventana **Seleccionar el tipo de tarea** del Asistente, seleccione **Mantenimiento del Servidor de administración** como tipo de tarea y haga clic en **Siguiente**.
5. Si necesita reducir la base de datos del Servidor de administración durante el mantenimiento, vaya a la ventana **Configuración** del Asistente y seleccione la casilla de verificación **Reducir base de datos**.
6. Siga el resto de instrucciones del Asistente.

La tarea recién creada se muestra en la lista de tareas en el espacio de trabajo de la carpeta **Tareas**. Solo se puede ejecutar una tarea de *Mantenimiento del Servidor de administración* por Servidor de administración. Si ya se ha creado una tarea de *Mantenimiento del Servidor de administración* para un Servidor de administración, no se puede crear otra tarea de *Mantenimiento del Servidor de administración* de este tipo.

Ventana Método de notificación del usuario

En la ventana **Método de notificación del usuario**, puede configurar la notificación que recibe el usuario sobre la instalación del certificado en el dispositivo móvil:

- **Mostrar enlace en el Asistente**. Si selecciona esta opción, se mostrará un enlace al paquete de instalación en el paso final del Asistente de conexión de nuevo dispositivo.
- **Enviar enlace al usuario**. Si selecciona esta opción, puede especificar la configuración para notificarle al usuario la conexión de un dispositivo.

En el grupo de configuración **Por correo electrónico**, puede configurar notificaciones de usuario sobre la instalación de un nuevo certificado en su dispositivo móvil mediante mensajes de correo electrónico. Este método de notificación solo está disponible si el servidor SMTP está activado.

En el grupo de configuración **Por SMS**, puede configurar notificaciones de usuario sobre la instalación de un certificado en su dispositivo móvil mediante SMS. Este método de notificación solo está disponible si la opción Notificación por SMS está activada.

Haga clic en el enlace **Editar mensaje** en los grupos de configuración **Por correo electrónico** y **Por SMS** para ver y editar el mensaje de notificación, si es necesario.

Sección General

En esta sección, puede ajustar la configuración general del perfil para dispositivos móviles de Exchange ActiveSync:

- **Nombre**

  Nombre del perfil.

- **Permitir dispositivos no aprovisionables**

  Si esta opción está activada, a los dispositivos que no pueden acceder a toda la configuración de la directiva de Exchange ActiveSync se les permite conectarse al servidor de dispositivos móviles. Mediante el uso de la conexión, puede administrar dispositivos móviles de Exchange ActiveSync. Por ejemplo, puede establecer contraseñas, configurar el envío de correos electrónicos o ver información sobre los dispositivos, como la Id. del dispositivo o el estado de la directiva.

  Si esta opción está desactivada, no puede conectarse al servidor de dispositivos móviles y administrar dispositivos móviles de Exchange ActiveSync.

  Esta opción está activada de forma predeterminada. Puede desactivar esta opción si no va a administrar dispositivos móviles de Exchange ActiveSync y recibir información sobre ellos.

- **Frecuencia de actualización (horas)**

Si esta opción está activada, la aplicación restaura la información acerca de la directiva de Exchange ActiveSync con la frecuencia especificada en el campo de entrada.

Si la opción está desactivada, la información sobre la política de Exchange ActiveSync no se actualiza.

De forma predeterminada, esta opción está activada y el intervalo de actualización es de una hora.

Ventana Selección de dispositivos

Elija una selección de la lista **Selección de dispositivos**. La lista contiene las selecciones predeterminadas y las selecciones creadas por el usuario.

Puede ver los detalles de los selecciones de dispositivos en el espacio de trabajo de la sección **Selecciones de dispositivos**.

Definir el nombre de la ventana del nuevo objeto

En la ventana, especifique el nombre del objeto recién creado. El nombre no puede contener más de 100 caracteres de largo y no puede incluir ningún carácter especial (como "*<>-_?:\"|).

Sección Categorías de aplicaciones

En esta sección, puede configurar la distribución de información sobre las categorías de aplicaciones en dispositivos cliente.

Transmisión de datos completos (para Agentes de red Service Pack 2 y anterior)

Si esta opción está seleccionada, todos los datos de una categoría de aplicaciones se transmiten a los dispositivos cliente, después de que esa categoría cambie. Esta opción de la transmisión de información se utiliza con el Agente de red Service Pack 2 y versiones anteriores.

Transmisión de datos modificados solamente (para Agentes de red Service Pack 2 y posterior)

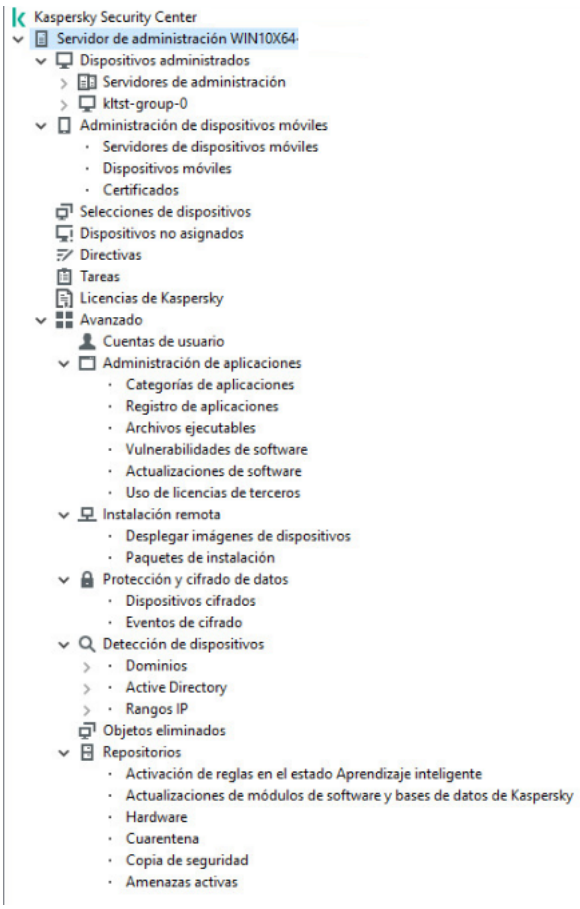
Si esta opción está seleccionada, cuando una categoría de aplicación cambia, solo los datos que se han modificado se transmitirán a los dispositivos cliente, en vez de todos los datos de esa categoría. Esta opción de transmisión de información se utiliza con el Agente de red Service Pack 2 y versiones posteriores.

Funciones de uso de la interfaz de administración

Esta sección describe las acciones que puede llevar a cabo en la ventana principal de Kaspersky Security Center.

Árbol de consola

El árbol de consola (consulte la figura siguiente) está diseñado para mostrar la jerarquía de los Servidores de administración existentes en la red corporativa, la estructura de sus grupos de administración y otros objetos de la aplicación, tales como las carpetas **Repositorios** o **Administración de aplicaciones**. El espacio de nombres de Kaspersky Security Center puede contener varios nodos, incluidos los nombres de los servidores correspondientes a los Servidores de administración incluidos en la jerarquía.



Árbol de consola

Nodo del Servidor de administración

El nodo **Servidor de administración: <Nombre del dispositivo>** es un contenedor que refleja la organización estructural del Servidor de administración seleccionado.

El espacio de trabajo del nodo **Servidor de administración** contiene información resumida sobre el estado actual de la aplicación y de los dispositivos administrados por el Servidor de administración. La información del espacio de trabajo se distribuye en diferentes fichas:

- **Supervisión**. Muestra información sobre el funcionamiento de la aplicación y el estado actual de los dispositivos cliente en tiempo real. Los mensajes importantes para el administrador (por ejemplo, mensajes sobre vulnerabilidades, errores o virus detectados) se resaltan en un determinado color. Puede utilizar enlaces en la ficha **Supervisión** para efectuar las tareas estándar del administrador (por ejemplo, instalar y configurar la aplicación de seguridad en dispositivos cliente) y para acceder a otras carpetas del árbol de consola.

- **Estadísticas**. Contiene un conjunto de gráficos agrupados por temas (estado de la protección, estadísticas antivirus, actualizaciones, etc.). Dichos gráficos visualizan información actual sobre el funcionamiento de la aplicación y el estado de los dispositivos cliente.

- **Informes**. Contiene plantillas para informes generados por la aplicación. En esta ficha, puede crear informes mediante plantillas predefinidas y crear plantillas de informe personalizadas.

- Ventana **Eventos**. Contiene registros de eventos que se han registrado durante el funcionamiento de la aplicación. Estos registros se distribuyen entre temas para facilitar la lectura y el filtrado. En esta ficha, puede ver selecciones de eventos que se han generado automáticamente, así como crear selecciones personalizadas.

Carpetas del nodo Servidor de administración

El nodo **Servidor de administración: <Nombre del dispositivo>** incluye las carpetas siguientes:

- **Dispositivos administrados**. La carpeta está diseñada para almacenar y mostrar la configuración y modificación de la estructura de los grupos de administración, directivas de grupo y tareas de grupo.
- **Administración de dispositivos móviles**. La finalidad de esta carpeta es la administración de dispositivos móviles. La carpeta **Administración de dispositivos móviles** contiene las siguientes subcarpetas:
  - **Servidores de dispositivos móviles**. Su finalidad es gestionar servidores de MDM para iOS y servidores de dispositivos móviles de Microsoft Exchange.
  - **Dispositivos móviles**. Destinada a administrar dispositivos móviles, KES, Exchange ActiveSync y MDM de iOS.
  - **Certificados**. Su finalidad es la administración de certificados de dispositivos móviles.
- **Selecciones de dispositivos**. Esta carpeta está destinada a la selección rápida de dispositivos que cumplan determinados criterios (selección de dispositivos) de entre todos los Dispositivos administrados. Por ejemplo, puede hacer selecciones rápidas de dispositivos que no tengan instalada ninguna aplicación de seguridad y acceder a ellos (verlos en una lista). Puede realizar acciones específicas con estos dispositivos seleccionados, por ejemplo asignarles determinadas tareas. Puede utilizar selecciones predefinidas o crear selecciones personalizadas.
- **Dispositivos no asignados**. Esta carpeta contiene una lista de los dispositivos que no se han incluido en ningún grupo de administración. Puede efectuar determinadas acciones en dispositivos no asignados, por ejemplo moverlos a grupos de administración o instalar aplicaciones en ellos.
- **Directivas**. La finalidad de esta carpeta es la visualización y creación de directivas.
- **Tareas**. La finalidad de esta carpeta es la visualización y creación de tareas.
- **Licencias de Kaspersky**. Contiene una lista de las claves de licencia disponibles para aplicaciones de Kaspersky. En el espacio de trabajo de esta carpeta, puede añadir claves de licencia nuevas al repositorio de clave de licencia, desplegar claves de licencia en dispositivos administrados y ver informes sobre el uso de las claves de licencia.
- **Avanzado**. Esta carpeta contiene una serie de subcarpetas que corresponden a diferentes grupos de funciones de la aplicación.

Carpeta Avanzado. Traslado de carpetas al árbol de consola

La carpeta **Avanzado** contiene las subcarpetas siguientes:

- **Cuentas de usuario**. Contiene una lista de cuentas de usuario de red.
- **Administración de aplicaciones**. Su finalidad es administrar las aplicaciones instaladas en los dispositivos que son parte de la red. La carpeta **Administración de aplicaciones** contiene las siguientes subcarpetas:
  - **Categorías de aplicaciones**. Su finalidad es gestionar categorías de aplicaciones personalizadas.

- **Registro de aplicaciones**. Contiene una lista de las aplicaciones presentes en los dispositivos que tienen instalado el Agente de red.
- **Archivos ejecutables**. Contiene la lista de los archivos ejecutables almacenados en los dispositivos cliente que tienen instalado el Agente de red.
- **Vulnerabilidades de software**. Contiene una lista de las vulnerabilidades presentes en las aplicaciones de los dispositivos que tienen instalado el Agente de red.
- **Actualizaciones de software**. Contiene una lista de actualizaciones de aplicaciones recibidas por el Servidor de administración que se puede distribuir en los dispositivos.
- **Uso de licencias de terceros**. Contiene una lista de grupos de aplicaciones con licencia. Puede utilizar grupos de aplicaciones con licencia para supervisar el uso de licencias para software de terceros (aplicaciones que no son de Kaspersky) y posibles incumplimientos en las restricciones de las licencias.

- **Instalación remota**. La carpeta sirve para administrar la instalación remota de sistemas operativos y aplicaciones. La carpeta **Instalación remota** contiene las siguientes subcarpetas:
  - **Desplegar imágenes de dispositivos**. Sirve para desplegar imágenes de sistemas operativos en los dispositivos.
  - **Paquetes de instalación**. Contiene una lista de los paquetes de instalación que se pueden usar para la instalación remota de aplicaciones en dispositivos cliente.
- **Protección y cifrado de datos**. Esta carpeta sirve para administrar el proceso de cifrado de datos en unidades de disco duro y unidades extraíbles.
- **Sondeo de la red**. Esta carpeta muestra la red en que está instalado el Servidor de administración. El Servidor de administración recibe información sobre la estructura de la red y sus dispositivos mediante sondeos regulares de la red Windows, las subredes IP y Active Directory® en la red corporativa. Los resultados del sondeo se muestran en las áreas de trabajo de las carpetas correspondientes: **Dominios**, **Rangos IP** y **Active Directory**.
- **Repositorios**. Esta carpeta está diseñada para realizar operaciones con los objetos utilizados para controlar el estado de los dispositivos y llevar a cabo su mantenimiento. La carpeta **Repositorios** contiene los siguientes subcarpetas:
  - **Detección adaptable de anomalías**. Contiene una lista de detecciones realizada mediante las reglas de Kaspersky Endpoint Security que funcionan en el modo Aprendizaje inteligente en los dispositivo cliente.
  - **Actualizaciones y parches del software de** Kaspersky. Contiene una lista de actualizaciones recibidas por el Servidor de administración que puede ser distribuida en los dispositivos.
  - **Hardware**. Incluye una lista de hardware conectado a la red de la organización.
  - **Cuarentena**. Contiene una lista de objetos que el software antivirus ha puesto en Cuarentena.
  - **Copia de seguridad**. Contiene una lista de copias de seguridad de los archivos que se han eliminado o modificado durante el proceso de desinfección de dispositivos.
  - **Archivos no procesados**. Contiene una lista de archivos asignados para que las aplicaciones antivirus los analicen posteriormente.

Puede cambiar el conjunto de subcarpetas que se incluyen en la carpeta **Avanzado**. Las subcarpetas que se utilizan con frecuencia se pueden subir un nivel con respecto a la carpeta **Avanzado**. Las subcarpetas que se usan muy pocas veces se pueden transferir a la carpeta **Avanzado**.

*Para quitar una subcarpeta de la carpeta **Avanzado**:*

1. En el árbol de consola, seleccione la subcarpeta que desea quitar de la carpeta **Avanzado**.
2. En el menú contextual de la subcarpeta, seleccione **Ver** → **Quitar de carpeta Avanzado**.

También es posible quitar una subcarpeta de la carpeta **Avanzado** en el espacio de trabajo de la carpeta **Avanzado** haciendo clic en el enlace **Quitar de carpeta Avanzado** en la sección con el nombre de dicha subcarpeta.

*Para mover una subcarpeta a la carpeta **Avanzado**:*

1. En el árbol de consola, seleccione la subcarpeta que desea mover a la carpeta **Avanzado**.
2. En el menú contextual de la subcarpeta, seleccione **Ver** → **Mover a carpeta Avanzado**.

Cómo actualizar datos en el espacio de trabajo

En Kaspersky Security Center, los datos del espacio de trabajo (por ejemplo, estados del dispositivo, estadísticas e informes) nunca se actualizan automáticamente.

Para actualizar datos en el espacio de trabajo:

- Pulse la tecla **F5**.
- en el menú contextual del objeto del árbol de consola, seleccione **Actualizar**.
- Haga clic en el botón del espacio de trabajo.

Cómo navegar en el árbol de consola

Para navegar por el árbol de consola, puede utilizar los siguientes botones de la barra de herramientas:

- – Un paso hacia atrás.
- – Un paso hacia adelante.
- – Un nivel hacia arriba.

También puede utilizar una cadena de navegación ubicada en la esquina superior derecha del espacio de trabajo. La cadena de navegación contiene la ruta completa a la carpeta del árbol de la consola en la que se encuentra actualmente. Todos los elementos de la cadena, excepto el último, son enlaces a los objetos en el árbol de consola.

Cómo abrir la ventana de propiedades del objeto en el espacio de trabajo

Puede cambiar las propiedades de la mayoría de los objetos de la Consola de administración en la ventana de propiedades del objeto.

Para abrir la ventana de propiedades de un objeto ubicado en el espacio de trabajo:

- Desde el menú contextual del objeto, seleccione **Propiedades**.
- Seleccione un objeto y pulse **ALT**+**INTRO**.

Cómo seleccionar un grupo de objetos en el espacio de trabajo

Puede seleccionar un grupo de objetos en el espacio de trabajo. Puede seleccionar un grupo de objetos, por ejemplo, para crear un conjunto de dispositivos para los cuales puede crear tareas más adelante.

Para seleccionar un intervalo de objetos:

1. Seleccione el primer objeto del intervalo y pulse **Mayús**.
2. Mantenga pulsada la tecla **Mayús** y seleccione el último objeto del intervalo.

Se seleccionará el intervalo.

Para agrupar objetos separados:

1. Seleccione el primer objeto del grupo y pulse **Ctrl**.
2. Mantenga pulsada la tecla **Ctrl** y seleccione otros objetos que desee incluir en el grupo.

Los objetos se agruparán.

Cómo cambiar el conjunto de columnas en el espacio de trabajo

La Consola de administración le permite cambiar un conjunto de columnas visualizadas en el espacio de trabajo.

Para cambiar un conjunto de columnas visualizadas en el espacio de trabajo:

1. En el árbol de consola, haga clic en el objeto para el que desea cambiar el conjunto de columnas.
2. En el espacio de trabajo de la carpeta, abra la ventana destinada a la configuración del conjunto de columnas haciendo clic en el vínculo **Agregar/Quitar columnas**.
3. En la ventana **Agregar/Quitar columnas**, especifique el conjunto de columnas que mostrarse.

Información de referencia

Las tablas de esta sección proporcionan información resumida sobre el menú contextual de los objetos de la Consola de administración, así como de los estados de los objetos del árbol de consola y del espacio de trabajo.

Comandos de menú contextual

Esta sección enumera los objetos de la Consola de administración y los elementos correspondientes del menú contextual (consulte la tabla siguiente).

Elementos del menú contextual de los objetos de la Consola de administración

Objeto	Elemento del menú	Función del elemento del menú
Elementos generales del menú contextual	**Buscar**	Abre la ventana de búsqueda de dispositivos.
	Actualizar	Actualizar la visualización del objeto seleccionado.
	Exportar lista	Exporta la lista actual a un archivo.
	Propiedades	Abre la ventana de propiedades del objeto seleccionado.
	Ver → Agregar/Quitar columnas	Añade o elimina columnas en la tabla de objetos del espacio de trabajo.
	Ver → Iconos grandes	Muestra los objetos en el espacio de trabajo como iconos grandes.
	Ver → Iconos pequeños	Muestra los objetos en el espacio de trabajo como iconos pequeños.
	Ver → Lista	Muestra los objetos en el espacio de trabajo como una lista.
	Ver → Tabla	Muestra los objetos en el espacio de trabajo como una tabla.
	Ver → Configurar	Configura la visualización de elementos de la Consola de administración.
Kaspersky Security Center	**Nuevo → Servidor de administración**	Agrega un Servidor de administración al árbol de consola.
<Nombre del Servidor de administración>	**Conectar al Servidor de administración**	Se conecta al Servidor de administración.
	Desconectar del Servidor de administración	Desconectar del Servidor de administración.
Dispositivos administrados	**Instalar aplicación**	Iniciar Asistente de instalación remota de aplicaciones.
	Ver → Configuración de la interfaz	Configura la visualización de elementos de la interfaz.
	Quitar	Elimina el Servidor de administración del árbol de consola.
	Instalar aplicación	Inicia el Asistente de instalación remota para el grupo de administración.
	Restablecer Contador de virus	Reinicia los contadores de virus en los dispositivos incluidos en el grupo de administración.
	Ver informe de	Crea un informe de amenazas y actividad de

	amenazas	virus en dispositivos incluidos en el grupo de administración.
	Nuevo → Grupo	Crear grupo de administración.
	Todas las tareas → Nueva estructura de grupo	Crea una estructura de grupos de administración basada en la estructura de dominios o Active Directory.
	Todas las tareas → Mostrar mensaje	Inicia el Asistente de nuevo mensaje para usuarios, diseñado para usuarios de dispositivos incluidos en el grupo de administración.
Dispositivos administrados → Servidores de administración	**Nuevo → Servidor de administración secundario**	Inicia el Asistente para agregar un Servidor de administración secundario.
	Nuevo → Servidor de administración virtual	Inicia el Asistente para crear nuevo Servidor de administración virtual.
Administración de dispositivos móviles → Dispositivos móviles	**Nuevo → Dispositivo móvil**	Conectar un nuevo dispositivo móvil del usuario.
Administración de dispositivos móviles → Certificados	**Nuevo → Certificado**	Creando certificado.
	Creado → Dispositivo móvil	Conectar un nuevo dispositivo móvil del usuario.
Selecciones de dispositivos	**Nuevo → Nueva selección**	Crear selección de dispositivos.
	Todas las tareas → Importar	Importar selección desde archivo.
Licencias de Kaspersky	**Agregar código de activación o archivo clave**	Agrega una clave de licencia al repositorio del Servidor de administración.
	Activar aplicación	Inicia el Asistente para crear tareas de activación de aplicaciones.
	Informe de uso de claves de licencia	Crea y muestra un informe sobre las claves de licencia de dispositivos cliente.
Administración de aplicaciones → Categorías de aplicaciones	**Nuevo → Categoría**	Crea una categoría de aplicaciones.
Administración de aplicaciones → Registro de aplicaciones	**Filtro**	Configura un filtro para la lista de aplicaciones.
	Aplicaciones supervisadas	Configura la publicación de eventos relacionados con la instalación de aplicaciones.
	Quitar las aplicaciones que no están instaladas	Borra la lista de todos los detalles de las aplicaciones que ya no estén instaladas en los dispositivos conectados a la red.
Administración de aplicaciones → Actualizaciones de software	**Aceptar Contratos de licencia para obtener actualizaciones**	Aceptar los Contratos de licencia de las actualizaciones de software.
Administración de	**Nuevo → Grupo de**	Crear Grupo de aplicaciones con licencia.

aplicaciones → Uso de licencias de terceros	**aplicaciones con licencia**	
Instalación remota → Paquetes de instalación	**Mostrar las versiones actuales de la aplicación**	Muestra la lista de versiones actualizadas de aplicaciones Kaspersky disponibles en servidores web.
	Nuevo → Paquete de Instalación	Crear paquete de instalación.
	Todas las tareas → Actualizar bases de datos	Actualiza las bases de datos de la aplicación en los paquetes de instalación.
	Todas las tareas → Mostrar lista general de paquetes independientes	Muestra la lista de paquetes independientes creados para los paquetes de instalación.
Detección de dispositivos → Dominios	**Todas las tareas → Actividad de los dispositivos**	Configura la respuesta del Servidor de administración a la inactividad de dispositivos conectados a la red.
Detección de dispositivos → Rangos IP	**Nuevo → Rango IP**	Creación de un rango IP.
Repositorios → Actualizaciones de módulos de software y bases de datos de Kaspersky	**Descargar actualizaciones**	Abre la ventana de propiedades de la tarea Descargar actualizaciones en el repositorio del Servidor de administración.
	Parámetros de descarga de actualizaciones	Configura la tarea Descargar actualizaciones en el repositorio del Servidor de administración.
	Informe de uso de las bases& de datos antivirus	Crea y muestra un informe sobre las versiones de bases de datos.
	Todas las tareas → Limpiar repositorio de actualizaciones	Borra el repositorio de actualizaciones del Servidor de administración.
Repositorios → Hardware	**Nuevo → Dispositivo**	Crea un dispositivo nuevo.

Lista de dispositivos administrados. Descripción de columnas

La tabla siguiente muestra los nombres y las respectivas descripciones de las columnas de la lista de dispositivos administrados.

Descripciones de las columnas de la lista de dispositivos administrados

Nombre de columna	Valor
Nombre	Nombre NetBIOS del dispositivo cliente. Las descripciones de los iconos de nombres de dispositivo se proporcionan en el apéndice.
Tipo de sistema operativo	Tipo de sistema operativo instalado en el dispositivo cliente.
Dominio de	Nombre del dominio de Windows en el que se encuentra el dispositivo cliente.

Windows	
Agente de red instalado	Resultado de la instalación de Agente de red en el dispositivo cliente (*Sí*, *No*, *Desconocido*).
El Agente de red está en ejecución	Resultado del funcionamiento del Agente de red (*Sí*, *No*, *Desconocido*).
Protección en tiempo real	La aplicación de seguridad está instalada (*Sí*, *No*, *Desconocido*).
Última conexión al Servidor de administración	Período de tiempo transcurrido desde que el dispositivo cliente se conectó al Servidor de administración.
Protección actualizada por última vez	El período de tiempo transcurrido desde la última actualización de los dispositivos administrados.
Estado	Estado actual del dispositivo cliente (*Correcto, Crítico, Advertencia*).
Descripción del estado	Motivos del cambio del estado del dispositivo cliente a *Crítico* o a *Advertencia*. El estado del dispositivo cambia a *Advertencia* o a *Crítico* por los motivos siguientes: • La aplicación de seguridad no está instalada. • Demasiados virus detectados. • El nivel de protección en tiempo real es distinto del establecido por el administrador. • No se ha realizado ningún análisis antivirus desde hace mucho tiempo. • Las bases de datos están desactualizadas. • No conectado durante mucho tiempo. • Se han detectado amenazas activas. • Se requiere reiniciar. • Hay aplicaciones incompatibles instaladas. • Se han detectado vulnerabilidades de software. • Hace mucho tiempo que no se comprueba si hay actualizaciones de Windows Update. • Estado de cifrado no válido. • La configuración del dispositivo móvil no cumple la directiva. • Incidentes sin procesar detectados. • Estado del dispositivo definido por la aplicación. • El dispositivo no tiene espacio disponible en el disco. • La licencia caduca pronto. El estado del dispositivo solamente cambia a *Crítico* por los motivos siguientes:

	• La licencia ha caducado. • Se ha perdido la conexión con el dispositivo. • La protección está desactivada. • La aplicación de seguridad no se está ejecutando. Las aplicaciones de Kaspersky administradas en los dispositivos cliente pueden añadir descripciones de estado de la lista. Kaspersky Security Center puede recibir la descripción del estado de un dispositivo cliente desde las aplicaciones de Kaspersky administradas instaladas en ese dispositivo. Si el estado que la aplicación administrada ha asignado al dispositivo se diferencia del asignado por Kaspersky Security Center, la Consola de administración muestra el estado más crítico para la seguridad del dispositivo. Por ejemplo, si una aplicación administrada ha asignado el estado *Crítico* al dispositivo, mientras Kaspersky Security Center le ha asignado el estado *Advertencia*, la Consola de administración mostrará el estado *Crítico* para ese dispositivo y la descripción correspondiente proporcionada por la aplicación administrada.
Última actualización de información	Período de tiempo transcurrido desde la última sincronización correcta del dispositivo cliente con el Servidor de administración (es decir, desde que se realizó el último análisis de la red).
Nombre DNS	Nombre de dominio DNS del dispositivo cliente.
Dominio DNS	Sufijo DNS principal.
Dirección IP	Dirección IP del dispositivo cliente. Se recomienda utilizar la dirección IPv4.
Visible por última vez	Período de tiempo durante el cual el dispositivo cliente ha permanecido visible en la red.
Último análisis completo	Fecha y hora del último análisis del dispositivo cliente que haya realizado la aplicación de seguridad a petición del usuario.
Número total de amenazas detectadas	Número de amenazas encontrados.
Estado de protección en tiempo real	Estado de protección en tiempo real (*Iniciando, En ejecución, En ejecución (protección máxima), En ejecución (velocidad máxima), En ejecución (configuración recomendada), En ejecución (configuración personalizada), Detenido, En pausa, Fallo*).
Dirección IP de conexión	Dirección IP usada para conectarse al Servidor de administración de Kaspersky Security Center.
Versión del Agente de red	Versión del Agente de red.
Versión de la aplicación	Versión de la aplicación de seguridad instalada en el dispositivo cliente.
Última actualización de las bases de datos antivirus	Versión de la bases de datos antivirus.
Sistema iniciado por última vez	Fecha y hora en que el dispositivo cliente se encendió por última vez.
Se requiere	Se requiere reiniciar el dispositivo cliente.

reiniciar	
Punto de distribución	Nombre del dispositivo que ejerce como punto de distribución para este dispositivo cliente.
Descripción	Descripción del dispositivo cliente recibido después de un análisis de la red.
Estado de cifrado	Estado del cifrado de datos del dispositivo cliente.
Estado del WUA	Estado del Agente de Windows Update en el dispositivo cliente. El valor *Sí* corresponde a los dispositivos cliente que reciben las actualizaciones mediante Windows Update del Servidor de administración. El valor *No* corresponde a los dispositivos cliente que reciben las actualizaciones mediante Windows Update de otros orígenes.
Tamaño de bits del sistema operativo	Tamaño de bits del sistema operativo instalado en el dispositivo cliente.
Estado de la protección antispam	Estado del componente de protección contra correo no deseado (*En ejecución, Iniciando, Detenido, En pausa, Fallo, No hay datos del dispositivo)*
Estado de la prevención contra fugas de datos	Estado del componente de prevención de fuga de datos (*En ejecución, Iniciando, Detenido, En pausa, Fallo, No hay datos del dispositivo)*
Estado de la protección de los servidores de colaboración	Estado del componente de filtrado de contenido (*En ejecución, Iniciando, Detenido, En pausa, Fallo, No hay datos del dispositivo)*
Estado de la protección antivirus de servidores de correo	Estado del componente de protección antivirus del servidor de correo (*En ejecución, Iniciando, Detenido, En pausa, Fallo, No hay datos del dispositivo)*
Estado de Sensor de Endpoint	Estado del componente del sensor de Endpoint (*En ejecución, Iniciando, Detenido, En pausa, Fallo, No hay datos del dispositivo)*
Creado	Hora en que se creó el icono <Nombre del dispositivo>. Este atributo se utiliza para comparar varios eventos entre sí.
Nombre del Servidor de administración virtual o secundario	Nombre del Servidor de administración virtual o secundario. Esta columna solo está disponible en las listas que contienen dispositivos de diferentes Servidores de administración.
Grupo primario	Nombre del grupo de administración donde se encuentra el icono <Nombre del dispositivo>. Esta columna solo está disponible en las listas que contienen dispositivos de diferentes Servidores de administración.

Administrado por otro Servidor de administración	El parámetro puede tomar uno de estos valores: • Verdadero, si durante la instalación remota de aplicaciones de seguridad en el dispositivo, resulta que el dispositivo es administrado por un Servidor de administración diferente. • Falso, en caso contrario.
Compilación del sistema operativo	El número de compilación del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un número de compilación igual, anterior o posterior. También puede configurar la búsqueda de todos los números de compilación, excepto el especificado.
ID de versión del sistema operativo	El identificador de la versión (Id.) del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un Id. de versión igual, anterior o posterior. También puede configurar la búsqueda de todos los números de Id. de versión, excepto el especificado.

Estados de dispositivos, tareas y directivas

La tabla siguiente contiene una lista de iconos que se muestran en el árbol de consola y el espacio de trabajo de la Consola de administración junto a los nombres de los dispositivos, tareas y directivas. Estos iconos definen los estados de los objetos.

Estados de dispositivos, tareas y directivas

Icono	Estado
	Dispositivo con un sistema operativo para estaciones de trabajo detectado en el sistema, pero que todavía no está incluido en ninguno de los grupos de administración.
	Dispositivo con un sistema operativo para estaciones de trabajo incluido en un grupo de administración, con el estado *Aceptar*.
	Dispositivo con un sistema operativo para estaciones de trabajo incluido en un grupo de administración, con el estado *Advertencia*.
	Dispositivo con un sistema operativo para estaciones de trabajo incluido en un grupo de administración, con el estado *Crítico*.
	Dispositivo con un sistema operativo for Workstations incluido en un grupo de administración, que ha perdido conexión con el Servidor de administración.
	Dispositivo con un sistema operativo para servidores detectado en el sistema, pero que todavía no está incluido en ninguno de los grupos de administración.
	Dispositivo con un sistema operativo para servidores incluido en un grupo de administración, con el estado *Aceptar*.
	Dispositivo con un sistema operativo para servidores incluido en un grupo de administración, con el estado *Advertencia*.
	Dispositivo con un sistema operativo para servidores incluido en un grupo de administración, con el estado *Crítico*.
	Dispositivo con un sistema operativo para servidores incluido en un grupo de administración, que ha perdido conexión con el Servidor de administración.

	Dispositivo móvil detectado en el sistema y no incluido en ninguno de los grupos de administración.
	Dispositivo móvil incluido en un grupo de administración, con el estado *Aceptar*.
	Dispositivo móvil incluido en un grupo de administración, con el estado *Advertencia*.
	Dispositivo móvil incluido en un grupo de administración, con el estado *Crítico*.
	Dispositivo móvil incluido en un grupo de administración y que ha perdido su conexión con el Servidor de administración.
	Dispositivo con protección de UEFI detectado en la red pero no incluido en ningún grupo de administración. El dispositivo con protección de UEFI está en la red.
	Dispositivo con protección de UEFI detectado en la red pero no incluido en ningún grupo de administración. El dispositivo con protección de UEFI no está en la red.
	Dispositivo con protección de UEFI incluido en un grupo de administración, con el estado *Aceptar*. El dispositivo con protección de UEFI está en la red.
	Dispositivo con protección de UEFI incluido en un grupo de administración, con el estado *Aceptar*. El dispositivo con protección de UEFI no está en la red.
	Dispositivo con protección de UEFI incluido en un grupo de administración, con el estado *Advertencia*. El dispositivo con protección de UEFI está en la red.
	Dispositivo con protección de UEFI incluido en un grupo de administración, con el estado *Advertencia*. El dispositivo con protección de UEFI no está en la red.
	Dispositivo con protección de UEFI incluido en un grupo de administración, con el estado *Crítico*. El dispositivo con protección de UEFI está en la red.
	Dispositivo con protección de UEFI incluido en un grupo de administración, con el estado *Crítico*. El dispositivo con protección de UEFI no está en la red.
	Directiva activa.
	Directiva inactiva.
	Directiva activa heredada de un grupo creado en el Servidor de administración principal.
	Directiva activa heredada de un grupo de nivel superior.
	Tarea (tarea de grupo, tarea del Servidor de administración o tarea para dispositivos específicos) con el estado *Programado* o *Se completó correctamente*.
	Tarea (tarea de grupo, tarea del Servidor de administración o tarea para dispositivos específicos) con el estado *En ejecución*.
	Tarea (tarea de grupo, tarea del Servidor de administración o tarea para dispositivos específicos) con el estado *Fallo*.
	Tarea heredada de un grupo creado en el Servidor de administración principal.
	Tarea heredada de un grupo de nivel superior.

Iconos de estado de archivos en la Consola de administración

Para facilitar la administración de archivos en la Consola de administración de Kaspersky Security Center, los iconos se muestran al lado de los nombres de archivos (consulte la siguiente tabla). Los iconos indican los estados que las aplicaciones de Kaspersky administradas asignan a los archivos en los dispositivos cliente. Los iconos se muestran en los espacios de trabajo de **Cuarentena**, **Copia de seguridad** y **Amenazas activas**.

Los estados se asignan a objetos por Kaspersky Endpoint Security instalado en el dispositivo cliente en el cual el objeto se encuentra.

Correspondencia entre los iconos y estados de archivos

Icono	Estado
	Archivo con el estado *Infectado*.
	Archivo con el estado *Advertencia* o *Probablemente infectado*.
	Archivo con el estado *Agregado por el usuario*.
	Archivo con el estado *Falso positivo*.
	Archivo con el estado *Desinfectado*.
	Archivo con el estado *Eliminado*.
	Archivo en la carpeta **Cuarentena** con el estado *No infectado, Protegido con contraseña* o *Se debe enviar a Kaspersky*. Si no hay descripción de estado al lado de un icono, esto significa que la aplicación de Kaspersky administrada en el dispositivo cliente ha informado de un estado desconocido a Kaspersky Security Center.
	Archivo en la carpeta **Copia de seguridad** con el estado *No infectado, Protegido con contraseña* o *Se debe enviar a Kaspersky*. Si no hay descripción de estado al lado de un icono, esto significa que la aplicación de Kaspersky administrada en el dispositivo cliente ha informado de un estado desconocido a Kaspersky Security Center.
	Archivo en la carpeta **Amenazas activas** con el estado *No infectado, Protegido con contraseña* o *Se debe enviar a Kaspersky*. Si no hay descripción de estado al lado de un icono, esto significa que la aplicación de Kaspersky administrada en el dispositivo cliente ha informado de un estado desconocido a Kaspersky Security Center.

Búsqueda y exportación de datos

Esta sección contiene información sobre métodos de búsqueda de datos y sobre la exportación de datos.

Buscar dispositivos

Kaspersky Security Center permite encontrar dispositivos según los criterios especificados. Los resultados de la búsqueda pueden guardarse en un archivo de texto.

La función de búsqueda permite encontrar los siguientes dispositivos:

- Dispositivos cliente en grupos de administración de un Servidor de administración y sus Servidores secundarios.
- Dispositivos no asignados administrados por un Servidor de administración y sus Servidores secundarios.

Para encontrar dispositivos cliente de un grupo de administración:

1. En el árbol de consola, seleccione una carpeta del grupo de administración.
2. Seleccione **Buscar** en el menú contextual de la carpeta del grupo de administración.

3. En las fichas de la ventana **Buscar**, especifique los criterios para la búsqueda de dispositivos cliente y haga clic en el botón **Buscar ahora**.

   Los dispositivos que cumplan los criterios de búsqueda especificados aparecerán en una tabla en la parte inferior de la ventana **Buscar**.

Para encontrar dispositivos no asignados:

1. En el árbol de consola, seleccione la carpeta **Dispositivos no asignados**.
2. Seleccione **Buscar** en el menú contextual de la carpeta **Dispositivos no asignados**.
3. En las fichas de la ventana **Buscar**, especifique los criterios para la búsqueda de dispositivos cliente y haga clic en el botón **Buscar ahora**.

   Los dispositivos que cumplan los criterios de búsqueda especificados aparecerán en una tabla en la parte inferior de la ventana **Buscar**.

Siga estos pasos para buscar dispositivos sin tener en cuenta si están incluidos o no en un grupo de administración:

1. En el árbol de consola, seleccione el nodo **Servidor de administración**.
2. En el menú contextual del nodo, seleccione **Buscar**.
3. En las fichas de la ventana **Buscar**, especifique los criterios para la búsqueda de dispositivos cliente y haga clic en el botón **Buscar ahora**.

   Los dispositivos que cumplan los criterios de búsqueda especificados aparecerán en una tabla en la parte inferior de la ventana **Buscar**.

En la ventana **Buscar**, también puede buscar los grupos de administración y los Servidores de administración secundarios que usan una lista desplegable en la esquina superior derecha de la ventana. La función de búsqueda de grupos de administración y Servidores de administración secundarios no está disponible si ha abierto la ventana **Buscar** en la carpeta **Dispositivos no asignados**.

Para encontrar dispositivos, puede utilizar las siguientes expresiones regulares en los campos de entrada de la ventana **Buscar**.

La búsqueda de texto completo en la ventana **Buscar** está disponible:

- En la ficha **Red**, en el campo **Descripción**
- En la ficha **Hardware**, en los campos **Dispositivo**, **Proveedor** y **Descripción**

Configuración de búsqueda del dispositivo

A continuación, se muestran descripciones de la configuración usada para buscar dispositivos administrados. Los resultados de búsqueda se muestran en la parte inferior de la ventana.

Red

En la ficha **Red** puede especificar el criterio de búsqueda de dispositivos según los datos de la red:

- **Nombre o dirección IP del dispositivo**

  Nombre del dispositivo en la red Windows (nombre de NetBIOS).

- **Dominio de Windows**

  Muestra todos los dispositivos incluidos en el dominio de Windows especificado.

- **Grupo de administración**

  Muestra los dispositivos incluidos en el grupo de administración especificado.

- **Descripción**

Texto de la ventana de propiedades del dispositivo: en el campo **Descripción** de la sección **General**.

Para describir texto en el campo **Descripción**, se pueden utilizar los siguientes caracteres:

- Dentro de una palabra:
  - *****. Sustituye cualquier cadena con cualquier número de caracteres.

    Ejemplo:

    Para describir las palabras como **Servidor** o **Servidores** puedes escribir **Servidor***.
  - **?.** Sustituye cualquier carácter individual.

    Ejemplo:

    Para describir palabras como **Window** o **Windows**, puedes escribir **Windo?**.

    El asterisco (*****) o signo de interrogación (**?**) no se puede utilizar como el primer carácter de la pregunta.
- Para encontrar varias palabras:
  - Espacio. Muestra todos los dispositivos cuyas descripciones contienen alguna de las palabras de la lista.

    Ejemplo:

    Para buscar una frase que incluya las palabras **secundario** o **virtual**, en la consulta puede incluir la línea **secundario virtual**.
  - **+**. Cuando se introduce el signo más delante de una palabra, todos los resultados de la búsqueda incluirán esa palabra.

    Ejemplo:

    Para encontrar una frase que contenga tanto **secundario** como **virtual**, introduzca la consulta **+secundario+virtual**.
  - **-**. Cuando se introduce el signo menos delante de una palabra, ningún resultado de la búsqueda incluirá esa palabra.

    Ejemplo:

    Para encontrar una frase que tenga la palabra **secundario**, pero no la palabra **virtual**, introduzca la consulta **+secundario-virtual**.
  - **"<algún texto>"**. El texto escrito entre comillas debe formar parte del texto.

    Ejemplo:

    Para encontrar una frase que contenga la combinación de palabras **Servidor secundario**, introduzca **"Servidor secundario"** en la consulta.

- Rango IP

  Si esta opción está activada, se pueden introducir las direcciones IP inicial y final del rango IP en el que se incluirán los dispositivos pertinentes.

  Esta opción está desactivada de forma predeterminada.

- Administrado por otro Servidor de administración

  Seleccione uno de los siguientes valores:

  - **Sí**. Solo se considerarán los dispositivos cliente administrados por otros Servidores de administración.
  - **No**. Solo se considerarán los dispositivos cliente administrados por el mismo Servidor de administración.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

Etiquetas

En la ficha **Etiquetas**, puede configurar una búsqueda del dispositivo según palabras clave (etiquetas) que se añadieron anteriormente a las descripciones de los dispositivos administrados:

- Aplicar si coincide al menos una etiqueta especificada

  Si esta opción está activada, los resultados de las búsquedas mostrarán dispositivos cuyas descripciones contengan al menos una de las etiquetas seleccionadas.

  Si esta opción está desactivada, los resultados de la búsqueda solo mostrarán dispositivos con descripciones que contengan todas las etiquetas seleccionadas.

  Esta opción está desactivada de forma predeterminada.

- La etiqueta debe incluirse

  Si se selecciona esta opción, los resultados de búsqueda mostrarán los dispositivos cuyas descripciones contienen la etiqueta seleccionada. Para buscar dispositivos, puede usar el asterisco, que significa cualquier cadena con cualquier número de caracteres.

  Esta opción está seleccionada de forma predeterminada.

- La etiqueta debe excluirse

  Si esta opción se selecciona, los resultados de búsqueda mostrarán los dispositivos cuyas descripciones no contienen la etiqueta seleccionada. Para buscar dispositivos, puede usar el asterisco, que significa cualquier cadena con cualquier número de caracteres.

Active Directory

En la pestaña **Active Directory**, puede especificar que los dispositivos deben buscarse en la unidad organizativa (OU) o el grupo de Active Directory. También puede incluir dispositivos de todas las OU secundarias de la OU de Active Directory especificada en la selección. Para seleccionar dispositivos, defina la siguiente configuración:

- **El dispositivo está en una unidad organizativa de Active Directory**
- **Incluir unidades organizativas secundarias**
- **Este dispositivo pertenece al grupo de Active Directory**

Actividad de red

En la ficha **Actividad de red** se puede especificar el criterio de búsqueda de dispositivos según su actividad en la red:

- Este dispositivo es un punto de distribución

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La selección incluirá dispositivos que funcionan como puntos de distribución.
  - **No**. Los dispositivos que funcionan como puntos de distribución no se incluirán en la selección.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- No desconectar del Servidor de administración

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Activado**. La selección incluirá dispositivos en los que la casilla de verificación **No desconectar del Servidor de administración** está seleccionada.
  - **Desactivado**. La selección incluirá dispositivos en los que la casilla de verificación **No desconectar del Servidor de administración** no está seleccionada.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Perfil de conexión cambiado

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La selección incluirá dispositivos que se conectaron al Servidor de administración después del cambio del perfil de conexión.
  - **No**. La selección no incluirá dispositivos que se conectaron al Servidor de administración después del cambio del perfil de conexión.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Última conexión al Servidor de administración

  Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos en función de la hora de la última conexión al Servidor de administración.

  Si se activa esta casilla de verificación, en el campo de entrada se puede especificar el intervalo de tiempo (fecha y hora) durante el que se produjo la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá los dispositivos que se encuentren dentro del intervalo especificado.

  No se aplica el criterio si esta casilla está vacía.

  De forma predeterminada, esta casilla está en blanco.

- El sondeo de la red ha detectado dispositivos nuevos

  Busca los nuevos dispositivos que se han detectado mediante el sondeo de la red hace pocos días.

  Si esta opción está activada, la selección incluirá solamente los nuevos dispositivos que se hayan detectado mediante la detección de dispositivos durante el número de días especificados en el campo **Periodo de detección (días)**.

  Si esta opción está desactivada, la selección incluye todos los dispositivos que han sido detectados por detección de dispositivos.

  Esta opción está desactivada de forma predeterminada.

- El dispositivo es visible

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La aplicación incluye en la selección los dispositivos actualmente visibles en la red.
  - **No**. La aplicación incluye en la selección los dispositivos actualmente invisibles en la red.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

Aplicación

En la ficha **Aplicación** puede especificar el criterio de búsqueda de dispositivos según la aplicación administrada seleccionada:

- Nombre de la aplicación

  En la lista desplegable, puede establecer un criterio para incluir los dispositivos en una selección al realizar búsquedas por el nombre de una aplicación Kaspersky.

  La lista proporciona únicamente los nombres de las aplicaciones con los complementos de administración instalados en la estación de trabajo del administrador.

  No se aplica el criterio si no se selecciona ninguna aplicación.

- Versión de la aplicación

  En el campo de entrada, puede establecer un criterio para incluir los dispositivos en una selección al realizar búsquedas por el número de versión de una aplicación Kaspersky.

  No se aplica el criterio si no indica el número de la versión.

- Nombre de la actualización crítica

  En el campo de entrada, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas por el nombre de una aplicación o el número de paquete de una actualización.

  No se aplica el criterio si deja el campo en blanco.

- Última actualización de los módulos

Puede utilizar esta opción como criterio para realizar búsquedas de dispositivos según la hora de la última actualización de los módulos de las aplicaciones instaladas en esos dispositivos.

Si se selecciona esta casilla, en los campos de entrada podrá especificar el intervalo de tiempo (fecha y hora) en el que se realizó la última actualización de los módulos de las aplicaciones instaladas en esos dispositivos.

No se aplica el criterio si esta casilla está vacía.

De forma predeterminada, esta casilla está en blanco.

- **El dispositivo se administra a través de Kaspersky Security Center 14**

  En la lista desplegable, puede incluir en la selección los dispositivos administrados mediante Kaspersky Security Center:

  - **Sí**. En la selección los dispositivos administrados mediante Kaspersky Security Center.
  - **No**. La aplicación incluye en la selección dispositivos que no estén administrados por Kaspersky Security Center.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- **Aplicación de seguridad instalada**

  En la lista desplegable, puede incluir en la selección todos los dispositivos con la aplicación de seguridad instalada:

  - **Sí**. La aplicación incluye en la selección todos los dispositivos con la aplicación de seguridad instalada.
  - **No**. La aplicación incluye en la selección todos los dispositivos que no tienen aplicación de seguridad instalada.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

Sistema operativo

En la ficha **Sistema operativo**, puede establecer los siguientes criterios para buscar dispositivos en función del tipo de sistema operativo (SO):

- **Versión del sistema operativo**

  Si se selecciona esta casilla de verificación, puede seleccionar un sistema operativo de la lista. Los dispositivos que tienen el sistema operativo especificado instalado se incluyen en los resultados de la búsqueda.

- **Tamaño de bits del sistema operativo**

  En la lista desplegable, puede seleccionar la arquitectura de su sistema operativo, que determinará cómo aplicar la regla de migración a su dispositivo (**Desconocido**, **x86**, **AMD64**, or **IA64**). De forma predeterminada, ninguna opción está seleccionada en la lista de modo que no se define la arquitectura del sistema operativo.

- Versión del Service Pack del sistema operativo

  En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y.*), que determinará cómo aplicar la regla de migración a su dispositivo. De forma predeterminada, no se especifica ningún valor de la versión.

- Compilación del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de Windows.

  El número de compilación del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un número de compilación igual, anterior o posterior. También puede configurar la búsqueda de todos los números de compilación, excepto el especificado.

- ID de versión del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de Windows.

  El identificador de la versión (Id.) del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un Id. de versión igual, anterior o posterior. También puede configurar la búsqueda de todos los números de Id. de versión, excepto el especificado.

Estado del dispositivo

En la ficha **Estado del dispositivo**, puede especificar criterios para buscar dispositivos según el estado del dispositivo desde la aplicación administrada:

- Estado del dispositivo

  Lista desplegable en la que se puede seleccionar uno de los estados del dispositivo: *Aceptar*, *Crítico* o *Advertencia*.

- Estado de protección en tiempo real

  Lista desplegable en la que se puede seleccionar el estado de protección en tiempo real. Se incluyen en la selección los dispositivos que tengan el estado de protección en tiempo real especificado.

- Descripción del estado del dispositivo

  En este campo se pueden seleccionar las casillas de verificación que se muestran junto a las condiciones que, si se cumplen, asignarán uno de los siguientes estados al dispositivo: *Aceptar, Crítico* o *Advertencia*.

- Estado del dispositivo definido por la aplicación

Lista desplegable en la que se puede seleccionar el estado de protección en tiempo real. Se incluyen en la selección los dispositivos que tengan el estado de protección en tiempo real especificado.

Componentes de protección

En la ficha **Componentes de protección** puede configurar los criterios de búsqueda de dispositivos cliente por el estado de protección.

- Fecha de publicación de las bases de datos

  Si esta opción está seleccionada, se puede hacer una búsqueda de dispositivos cliente por la fecha de lanzamiento de la base de datos antivirus. En los campos de entrada se puede establecer el intervalo de tiempo con el que se realizará la búsqueda.

  Esta opción está desactivada de forma predeterminada.

- Último análisis

  Si esta casilla está activada, se puede hacer una búsqueda de dispositivos cliente por la fecha de último análisis antivirus. En los campos de entrada puede especificar el período de tiempo en el cual se realizó el último análisis antivirus.

  Esta opción está desactivada de forma predeterminada.

- Número total de amenazas detectadas

  Si esta opción está activada, puede buscar dispositivos cliente por número de virus detectados. En los campos de entrada se pueden establecer los valores máximo y mínimo del número de virus encontrados.

  Esta opción está desactivada de forma predeterminada.

Registro de aplicaciones

En la ficha **Registro de aplicaciones** se puede configurar la búsqueda de dispositivos según las aplicaciones que tengan instaladas:

- Nombre de la aplicación

  Lista desplegable en la que se puede seleccionar la aplicación. En la selección se incluirán los dispositivos que tengan instalada la aplicación especificada.

- Versión de la aplicación

  Campo de entrada en el que se puede especificar la versión de la aplicación seleccionada.

- Proveedor

  Lista desplegable en la que se puede seleccionar el fabricante de una aplicación instalada en el dispositivo.

- Estado de la aplicación

  Una lista desplegable en la que se puede seleccionar el estado de una aplicación (*Instalada*, *No instalada*). Los dispositivos en los cuales la aplicación especificada está instalada o no instalada, según el estado seleccionado, se incluirán en la selección.

- Buscar por la actualización

  Si esta opción está activada, la búsqueda se realizará utilizando los detalles de las actualizaciones para las aplicaciones instaladas en los dispositivos relevantes. Después de seleccionar la casilla de verificación, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambian a **Nombre de actualización**, **Versión de actualización** y **Estado** respectivamente.

  Esta opción está desactivada de forma predeterminada.

- Nombre de la aplicación de seguridad incompatible

  Lista desplegable en la que se puede seleccionar aplicaciones de seguridad de terceros. Durante la búsqueda, se incluirán en la selección los dispositivos que tengan instalada la aplicación especificada.

- Etiqueta de la aplicación

  En la lista desplegable se puede seleccionar la etiqueta de la aplicación. Todos los dispositivos que han instalado aplicaciones con la etiqueta seleccionada en la descripción se incluyen en la selección de dispositivos.

Jerarquía de Servidores de administración

En la ficha **Jerarquía de Servidores de administración**, marque la casilla **Incluir datos de Servidores de administración secundarios (hasta el nivel)** si desea que se incluya la información almacenada en los Servidores de administración secundarios en la búsqueda de dispositivos; y, en el campo de entrada, puede especificar el nivel de anidamiento del Servidor de administración secundario cuya información se incluye al buscar dispositivos. De forma predeterminada, esta casilla está en blanco.

Máquinas virtuales

En la ficha **Máquinas virtuales** puede configurar la búsqueda de dispositivos según sean dispositivos virtuales o parte de la infraestructura de escritorio virtual (VDI):

- Es una máquina virtual

  En la lista desplegable se pueden seleccionar las siguientes opciones:

  - **No es importante**.
    - **No**. Buscar dispositivos que no son máquinas virtuales.
    - **Sí**. Buscar dispositivos que son máquinas virtuales.

- Tipo de máquina virtual

En la lista desplegable se puede seleccionar el fabricante de la máquina virtual.

Esta lista desplegable está disponible si el valor **Sí** o **No es importante** se selecciona en la lista desplegable **Es una máquina virtual**.

- **Parte de la infraestructura de escritorio virtual**

  En la lista desplegable se pueden seleccionar las siguientes opciones:

  - **No es importante**.
    - **No**. Buscar dispositivos que no formen parte de la Infraestructura de escritorio virtual.
    - **Sí**. Buscar dispositivos que formen parte de una Infraestructura de escritorio virtual (VDI) de Microsoft.

Hardware

En la ficha **Hardware** puede configurar la búsqueda de dispositivos cliente por su tipo de hardware:

- **Dispositivo**

  En la lista desplegable, puede seleccionar el tipo de unidad. Todos los dispositivos con esta unidad se incluyen en los resultados de la búsqueda.

  El campo admite búsqueda de texto completo.

- **Proveedor**

  En la lista desplegable se puede seleccionar el nombre del fabricante de la unidad. Todos los dispositivos con esta unidad se incluyen en los resultados de la búsqueda.

  El campo admite búsqueda de texto completo.

- **Descripción**

  Descripción del dispositivo o unidad de hardware. Los dispositivos con la descripción especificada en este campo se incluirán en la selección.

  La descripción de un dispositivo en cualquier formato se puede introducir en la ventana de propiedades de ese dispositivo. El campo admite búsqueda de texto completo.

- **Número de inventario**

  El equipo con el número de inventario especificado en este campo se incluirá en la selección.

- **Frecuencia de la CPU (MHz)**

  Intervalo de frecuencia de una CPU. Los dispositivos con las CPU que coincidan con el intervalo de frecuencia especificado en estos campos (valores máximo y mínimo incluidos) se incluirán en la selección.

- Núcleos de CPU virtual

  Intervalo del número de núcleos virtuales en una CPU. Los dispositivos con las CPU que coincidan con el intervalo especificado en estos campos (valores máximo y mínimo incluidos) se incluirán en la selección.

- Volumen del disco duro, en GB

  Intervalo de los valores para el tamaño del disco duro en el dispositivo. Los dispositivos con los discos duros que coincidan con el intervalo especificado en estos campos de entrada (valores máximo y mínimo incluidos) se incluirán en la selección.

- Tamaño de RAM, en MB

  Intervalo de los valores para el tamaño de la RAM de un dispositivo. Los dispositivos con las RAM que coincidan con el intervalo especificado en estos campos de entrada (valores máximo y mínimo incluidos) se incluirán en la selección.

Vulnerabilidades y actualizaciones

En la pestaña **Vulnerabilidades y actualizaciones**, puede configurar el criterio para buscar dispositivos según su fuente de Windows Update:

- El WUA se ha cambiado al Servidor de administración

  Puede seleccionar una de las opciones de búsqueda de la lista desplegable:
  - **Sí**. Si se selecciona esta opción, en los resultados de la búsqueda se incluirán los dispositivos que reciben actualizaciones del Servidor de administración a través de Windows Update.
  - **No**. Si se selecciona esta opción, en los resultados se incluirán los dispositivos que reciben actualizaciones de otras fuentes a través de Windows Update.

Usuarios

En la ficha **Usuarios**, puede configurar los criterios para buscar dispositivos según las cuentas de usuarios que han iniciado sesión en el sistema operativo.

- Último usuario que inició sesión en el sistema

  Si esta opción está activada, haga clic en el botón **Examinar** para especificar una cuenta de usuario. Los resultados de la búsqueda incluyen los dispositivos en los que un usuario específico ha iniciado sesión por última vez.

- Usuario que inició sesión en el sistema al menos una vez

  Si esta opción está activada, haga clic en el botón **Examinar** para especificar una cuenta de usuario. Los resultados de la búsqueda incluyen los dispositivos en los que el usuario especificado inició sesión en el sistema al menos una vez.

Problemas relacionados con el estado de las aplicaciones administradas

En la ficha **Problemas relacionados con el estado de las aplicaciones administradas**, puede configurar la búsqueda de dispositivos de acuerdo con las descripciones de sus estados proporcionados por la aplicación administrada:

- **Descripción del estado del dispositivo**

  En este campo puede seleccionar las casillas para las descripciones de estados desde la aplicación administrada; al recibir estos estados, los dispositivos se incluirán en la selección. Cuando selecciona un estado listado para varias aplicaciones, tiene la opción de seleccionar este estado en todas las listas automáticamente.

Estados de los componentes en aplicaciones administradas

En la ficha **Estados de los componentes en aplicaciones administradas**, puede configurar los criterios para buscar dispositivos según los estados de los componentes en aplicaciones administradas:

- **Estado de la prevención contra fugas de datos**

  Buscar dispositivos por el estado de Prevención de fuga de datos (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- **Estado de la protección de los servidores de colaboración**

  Buscar dispositivos por el estado de la protección de colaboración del servidor (*No hay datos del dispositivo*, *Detenido*, *Iniciando, En pausa*, *En ejecución*, *Fallo*).

- **Estado de la protección antivirus de servidores de correo**

  Buscar dispositivos por el estado de protección del servidor de correo (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- **Estado de sensor de Endpoint**

  Buscar dispositivos por el estado del componente del sensor de Endpoint (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

Cifrado

- **Cifrado**

  Algoritmo de cifrado de bloques simétricos Advanced Encryption Standard (AES). En la lista desplegable, puede seleccionar el tamaño de la clave de cifrado (de 56 bits, de 128 bits, de 192 bits o de 256 bits).

  Valores disponibles: *AES56*, *AES128*, *AES192* y *AES256*.

Segmentos de la nube

En la ficha **Segmentos de la nube**, puede configurar una búsqueda según si un dispositivo pertenece a segmentos de la nube específicos:

- **El dispositivo está en un segmento de la nube**

  Si esta opción está activada, puede hacer clic en el **Examinar** para especificar qué segmento buscar.

  Si la opción **Incluir objetos secundarios** también está activada, la búsqueda se ejecuta en todos los objetos secundarios del segmento especificado.

  Los resultados de la búsqueda solo incluyen dispositivos desde el segmento seleccionado.

- **Dispositivo descubierto mediante la API**

  En la lista desplegable, puede seleccionar si un dispositivo es detectado por herramientas API.

  - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de AWS.
  - **Azure**. El dispositivo se descubre mediante la Azure API, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
  - **Google Cloud.** El dispositivo se descubre mediante la API de Google, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de Google.
  - **No**. El dispositivo no se puede detectar con AWS, Azure o Google API, es decir, o bien está fuera del entorno de nube, o está en el entorno de nube pero no se puede detectar mediante API por algún motivo.
  - Ningún valor. Este criterio no se puede aplicar.

Componentes de la aplicación

Esta sección contiene la lista de componentes de aquellas aplicaciones que tienen complementos de administración correspondientes instalados en la Consola de administración.

En la sección **Componentes de la aplicación**, puede especificar los criterios para incluir dispositivos en una selección de acuerdo con los estados y números de versión de los componentes que se refieren a la aplicación que seleccione:

- **Estado**

Buscar dispositivos de acuerdo con el estado del componente enviado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *No se reciben datos del dispositivo*, *Detenido*, *Iniciado*, *Pausado*, *En ejecución*, *Mal funcionamiento* o *No instalado*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo se incluye en la selección de dispositivos.

Estados enviados por solicitudes:

- *Iniciando:* El componente está actualmente en el proceso de iniciación.
- *En ejecución:* El componente se activa y funciona correctamente.
- *En pausa:* El componente se suspende, por ejemplo, después de que el usuario ha hecho una pausa la protección en la aplicación administrada.
- *Mal funcionamiento:* Un error ha ocurrido durante la operación del componente.
- *Detenido:* El componente está desactivado y no funciona en este momento.
- *No instalado:* El usuario no seleccionó el componente para la instalación al configurar la instalación personalizada de la aplicación.

A diferencia de otros estados, las aplicaciones *no envían datos del estado del dispositivo*. Esta opción muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Por ejemplo, esto puede suceder cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

- **Versión**

  Buscar dispositivos de acuerdo con el número de versión del componente que seleccione en la lista. Puede escribir un número de versión, por ejemplo `3.4.1.0`, y luego especificar si el componente seleccionado debe tener una versión igual, anterior o posterior. También puede configurar la búsqueda de todas las versiones excepto la especificada.

Uso de máscaras en variables de cadena

Está permitido el uso de máscaras para variables de cadena. Al crear máscaras, puede utilizar las siguientes expresiones regulares:

- Carácter comodín (*): Cualquier cadena de 0 o más caracteres.
- Signo de interrogación (?): Cualquier carácter individual.
- [<range>]: cualquier carácter individual de un rango o conjunto específico.

  Por ejemplo: [0–9]: cualquier dígito. [abcdef]: cualquiera de los caracteres a, b, c, d, e, o f.

Uso de expresiones regulares en el campo de búsqueda

Puede utilizar las siguientes expresiones regulares en el campo de búsqueda para buscar palabras y caracteres específicos:

- *. Sustituye cualquier secuencia de caracteres. Para buscar las palabras "Servidor", "Servidores" o "sala de Servidores", introduzca la expresión `Servidor*` en el campo de búsqueda.
- ?. Sustituye cualquier carácter individual. Para buscar las palabras "Casa" o "Cosa", introduzca la expresión `C?sa` en el campo de búsqueda.

  El texto del campo de búsqueda no puede comenzar con el signo de interrogación (?).

- [<rango>]. Substituya cualquier carácter único de una gama o un conjunto especificado. Para buscar cualquier número, introduzca la expresión `[0-9]` en el campo de búsqueda. Para buscar uno de los caracteres—a, b, c, d, e o f—introduzca la expresión `[abcdef]` en el campo de búsqueda.

Utilice las siguientes expresiones regulares en los campos de búsqueda para realizar una búsqueda de texto completo:

- Espacio. El resultado son todos los dispositivos cuyas descripciones contengan alguna de las palabras enumeradas. Por ejemplo, para buscar una frase que contenga las palabras "Secundario" o "Virtual" (o ambas), introduzca la expresión `Secundario Virtual` en el campo de búsqueda.
- Signo más (+), AND o &&. Cuando se introduce el signo más delante de una palabra, todos los resultados de la búsqueda incluirán esa palabra. Por ejemplo, para buscar una frase que contenga tanto la palabra "secundario" como la palabra "virtual", puede introducir cualquiera de las expresiones siguientes en el campo de búsqueda: `+Secundario+Virtual`, `Secundario Y Virtual`, `Secundario && Virtual`.
- OR o ||. Cuando se coloca entre dos palabras, indica que se debe buscar una de las dos palabras. Para buscar una frase que contenga bien la palabra "secundario" o bien "virtual", introduzca una de estas expresiones en el campo de búsqueda: `secundario O virtual`, `secundario || virtual`.
- Signo menos (-). Cuando se introduce el signo menos delante de una palabra, ningún resultado de la búsqueda incluirá esa palabra. Para buscar una frase que contenga la palabra "secundario" y que no contenga "virtual", debe introducir la expresión `+secundario-virtual` en el campo de búsqueda.
- `"<algún texto>"`. El texto escrito entre comillas debe formar parte del texto. Para buscar una frase que contenga una combinación de palabras como servidor secundario, debe introducir la expresión `"Servidor secundario"` en el campo de búsqueda.

Las búsquedas de texto completo están disponibles en los siguientes bloques de filtrado:

- En el bloque de filtrado de listas de eventos, junto a las columnas **Evento** y **Descripción**.
- En el bloque de filtrado de cuentas de usuario, junto a la columna **Nombre**.
- En el bloque de filtrado de registro de aplicaciones, junto a la columna **Nombre**, si la casilla **Mostrar en la lista** tiene **no agrupado** seleccionado como criterio de filtrado.

Exportación de listas de cuadros de diálogo

En los cuadros de diálogo de la aplicación, puede exportar las listas de objetos en los archivos de texto.

La exportación de una lista de objetos es posible para las secciones del cuadro de diálogo que contiene el botón **Exportar a archivo**.

Configuración de tareas

Esta sección enumera todas las configuraciones de tareas en Kaspersky Security Center.

Configuración general de la tareas

Configuraciones especificadas durante la creación de tareas

Puede especificar los siguientes ajustes al crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- Configuración de reinicio del sistema operativo:
  - **No reiniciar el dispositivo**

    Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

  - **Reiniciar el dispositivo**

    Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

  - **Solicitar al usuario una acción**

    En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

    Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

Si esta opción está desactivada, la solicitud se muestra solo una vez.

- **Reiniciar después de (min)**

  Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

- Configuración de programación de la tarea:

  - **Inicio programado**

    Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

    - **Cada N horas**

      La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

      De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

    - **Cada N días**

      La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

      De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

    - **Cada N semanas**

La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

  La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

  Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- Cuando se descargan nuevas actualizaciones en el repositorio

  La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar este programa para la tarea de encontrar vulnerabilidades y actualizaciones necesarias.

- Al detectar un foco de virus

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- Al completar otra tarea

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- Usar un retraso aleatorio automático para el inicio de las tareas

Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Dispositivos a los que se asignará la tarea:

  - Seleccionar dispositivos de red detectados por el Servidor de administración

    La tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración así como dispositivos no asignados.

    Por ejemplo, es posible que desee usar esta opción en una tarea de instalación del Agente de red en dispositivos no asignados.

  - Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista

    Puede especificar nombres NetBIOS, nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.

    Es posible que desee utilizar esta opción para ejecutar una tarea para una subred específica. Por ejemplo, es posible que desee instalar una aplicación determinada en dispositivos de contadores o analizar dispositivos en una subred que probablemente esté infectada.

  - Asignar tarea a una selección de dispositivos

    La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

    Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

  - Asignar tarea a un grupo de administración

La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para dispositivos incluidos en un grupo de administración específico.

- Configuraciones de la cuenta:
  - **Cuenta preconfigurada**

    La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

    Esta opción está seleccionada de forma predeterminada.

  - **Especificar cuenta**

    Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

  - **Cuenta**

    Cuenta bajo la que se ejecuta la tarea.

  - **Contraseña**

    La contraseña de la cuenta bajo la cual la tarea se ejecutará.

Configuraciones especificadas después de la creación de tareas

Puede especificar la siguiente configuración solo después de crear una tarea.

- Ajustes de la tarea de grupo:
  - **Distribuir a subgrupos**

    Esta opción solo está disponible en la configuración de las tareas de grupo.

    Cuando esta opción está activada, la cobertura de la tarea incluye:

    - El grupo de administración que seleccionó al crear la tarea.
    - Los grupos de administración subordinados al grupo de administración seleccionado en cualquier nivel inferior al de la jerarquía del grupo.

    Cuando esta opción está desactivada, el alcance de la tarea incluye solo el grupo de administración que seleccionó al crear la tarea.

    Esta opción está activada de forma predeterminada.

  - **Distribuir a Servidores de administración secundarios y virtuales**

Cuando esta opción está activada, la tarea que es efectiva en el Servidor de administración principal también se aplica en los Servidores de administración secundarios (incluidos los virtuales). Si ya existe una tarea del mismo tipo en el Servidor de administración secundario, ambas tareas se aplican en el Servidor de administración secundario: el existente y el heredado del Servidor de administración principal.

Esta opción solo está disponible cuando está activada la opción **Distribuir a subgrupos**.

Esta opción está desactivada de forma predeterminada.

- Configuración de programación avanzada:
  - Encender dispositivos mediante la función Wake-on-LAN antes de iniciar la tarea (min)

    El sistema operativo en el dispositivo se inicia a la hora especificada antes de que se inicie la tarea. El intervalo de tiempo predeterminado es de cinco minutos.

    Active esta opción si desea que la tarea se ejecute en todos los dispositivos cliente desde el ámbito de la tarea, incluidos aquellos dispositivos que están apagados cuando la tarea está a punto de comenzar.

    Si desea que el dispositivo se apague automáticamente una vez completada la tarea, habilite la opción **Apagar los dispositivos después de completar la tarea**. Esta opción se puede encontrar en la misma ventana.

    Esta opción está desactivada de forma predeterminada.

  - Apagar los dispositivos después de completar la tarea

    Por ejemplo, es posible que desee activar esta opción para una tarea de actualización de instalación que instale actualizaciones en los dispositivos cliente todos los viernes después del horario comercial y después apagar estos dispositivos para el fin de semana.

    Esta opción está desactivada de forma predeterminada.

  - Detener la tarea si tarda más de (min)

    Una vez que el periodo de tiempo especificado expira, la tarea se detiene automáticamente, ya esté completa o no.

    Active esta opción si desea interrumpir (o detener) las tareas que tardan mucho en ejecutarse.

    Esta opción está desactivada de forma predeterminada. El tiempo de ejecución de la tarea predeterminado es de 120 minutos.

- Configuración de la notificación:
  - Bloque **Almacenar el historial de tareas**
    - En el Servidor de administración durante (días)

Los eventos de la aplicación relacionados con la ejecución de la tarea en todos los dispositivos cliente del ámbito de la tarea se almacenan en el Servidor de administración durante el número de días especificado. Cuando transcurre este periodo, la información se elimina del Servidor de administración.

Esta opción está activada de forma predeterminada.

- Almacenar en el registro de eventos del SO del dispositivo

  Los eventos de la aplicación relacionados con la ejecución de la tarea se almacenan localmente en el Registro de eventos de Windows de cada dispositivo cliente.

  Esta opción está desactivada de forma predeterminada.

- Almacenar en el registro de eventos del SO de Servidor de administración

  Los eventos de la aplicación relacionados con la ejecución de la tarea en todos los dispositivos cliente del ámbito de la tarea se almacenan de forma centralizada en el Registro de eventos de Windows del sistema operativo (SO) del Servidor de administración.

  Esta opción está desactivada de forma predeterminada.

- Guardar todos los eventos

  Si se selecciona esta opción, todos los eventos relacionados con la tarea se guardan en los registros del evento.

- Guardar eventos sobre el progreso de la tarea

  Si se selecciona esta opción, solo los eventos relacionados con la ejecución de la tarea se guardan en los registros del evento.

- Guardar solo los resultados de ejecución de la tarea

  Si se selecciona esta opción, solo los eventos relacionados con los resultados de la tarea se guardan en los registros del evento.

- Notificar al administrador los resultados de la ejecución de tareas

  Puede seleccionar los métodos por los cuales los administradores reciben notificaciones sobre los resultados de la ejecución de la tarea: por correo electrónico, por SMS y ejecutando un archivo ejecutable. Para configurar la notificación, haga clic en el enlace **Configuración**.

  De forma predeterminada, todos los métodos de notificación están deshabilitados.

- Notificar solo de errores

Si esta opción está habilitada, solo se notifica a los administradores cuando una ejecución de tarea se completa con un error.

Si esta opción está desactivada, se notifica a los administradores después de cada finalización de la ejecución de la tarea.

Esta opción está activada de forma predeterminada.

- Configuración de seguridad
- Configuración de la cobertura de la tarea

  Dependiendo de cómo se determine la cobertura de la tarea, están presentes las siguientes configuraciones:

  - Dispositivos

    Si la cobertura de una tarea está determinada por un grupo de administración, puede ver este grupo. No hay cambios disponibles aquí. Sin embargo, puede configurar **Exclusiones de la cobertura de la tarea**.

    Si la cobertura de una tarea está determinado por una lista de dispositivos, puede modificar esta lista añadiendo y eliminando dispositivos.

  - Selección de dispositivos

    Puede cambiar la selección de dispositivos a la que se aplicará la tarea.

  - Exclusiones de la cobertura de la tarea

    Puede especificar grupos de dispositivos a los que no se aplica la tarea. Los grupos que se excluyen solo pueden ser subgrupos del grupo de administración al que se aplica la tarea.

- **Historial de revisiones**

Descargar las actualizaciones de la configuración de tareas del repositorio del Servidor de administración

Configuraciones especificadas durante la creación de tareas

Puede especificar los siguientes ajustes al crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- Orígenes de actualizaciones

Los siguientes recursos pueden utilizarse como un origen de actualizaciones para el Servidor de administración:

- Servidores de actualización de Kaspersky

  Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación. De forma predeterminada, el Servidor de administración se comunica con los servidores de actualización de Kaspersky y descarga las actualizaciones utilizando el protocolo HTTPS. Puede configurar Servidor de administración para que utilice el protocolo HTTP en lugar del HTTPS.

  Seleccionado de forma predeterminada.

- Servidor de administración principal

  Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

- Carpeta local o de red

  Una carpeta local o de red que contiene las últimas actualizaciones. Una carpeta de red puede ser un servidor FTP o HTTP o un recurso compartido SMB. Si una carpeta de red requiere autenticación, solo se admite el protocolo SMB. Cuando se selecciona una carpeta local, debe especificar una carpeta en un dispositivo que tenga el Servidor de administración instalado.

  Un servidor FTP o HTTP o una carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura creada al usar los servidores de actualización de Kaspersky.

Si activa la opción **No usar servidor proxy** para los orígenes de actualizaciones Servidores de actualización de Kaspersky o Carpeta local o de red, el Servidor de administración no utilizará un servidor proxy para descargar actualizaciones.

- **Otros parámetros**

  - Forzar actualización en los Servidores de administración secundarios

    Si esta opción está activada, el Servidor de administración inicia las tareas de actualización en los Servidores de administración secundarios tan pronto como se descargan nuevas actualizaciones. De lo contrario, las tareas de actualización en los Servidores de administración secundarios comienzan de acuerdo con sus programaciones.

    Esta opción está desactivada de forma predeterminada.

  - Copiar las actualizaciones descargadas en carpetas adicionales

Una vez que el Servidor de administración recibe actualizaciones, las copia en las carpetas especificadas. Utilice esta opción si desea administrar de manera manual la distribución de actualizaciones en su red.

Por ejemplo, puede querer usar esta opción en la siguiente situación: la red de su organización consta de varias subredes independientes y los dispositivos de cada una de las subredes no tienen acceso a otras subredes. Sin embargo, los dispositivos en todas las subredes tienen acceso a un recurso compartido de red común. En este caso, configura el Servidor de administración en una de las subredes para descargar actualizaciones de los servidores de actualización de Kaspersky, active esta opción y luego especifique este recurso compartido de red. En las actualizaciones descargadas de las tareas del repositorio para otros Servidores de administración, especifique el mismo recurso compartido de red que el origen de actualización.

Esta opción está desactivada de forma predeterminada.

- **No forzar la actualización de dispositivos y Servidores de administración secundarios a menos que se complete la copia**

  Las tareas de descarga de actualizaciones a dispositivos cliente y Servidores de administración secundarios comienzan solo después de que esas actualizaciones se copien de la carpeta de actualización principal a carpetas de actualización adicionales.

  Esta opción debe estar activada si los dispositivos cliente y los Servidores de administración secundarios descargan actualizaciones de carpetas de red adicionales.

  Esta opción está desactivada de forma predeterminada.

- **Actualizar módulos del Agente de red (para versiones del Agente de red anteriores a la 10, Service Pack 2)**

  Si esta opción está habilitada, las actualizaciones para los módulos de software del Agente de red se instalan automáticamente después de que el Servidor de administración complete la tarea Descargar actualizaciones en el repositorio. De lo contrario, las actualizaciones recibidas para los módulos del Agente de red se pueden instalar de manera manual.

  Esta opción solo se aplica a las versiones del Agente de red anteriores a la 10 Service Pack 2. A partir de la versión 10 Service Pack 2, los Agentes de red se actualizan automáticamente.

  Esta opción está activada de forma predeterminada.

Configuraciones especificadas después de la creación de tareas

Puede especificar la siguiente configuración solo después de crear una tarea.

- Sección **Configuración**, bloque **Contenido de las actualizaciones**
  - **Descargar archivos diff**

    Esta opción habilita la función de descarga de archivos diff.

    Esta opción está desactivada de forma predeterminada.

- Sección **Verificación de actualizaciones**
  - **Verificar actualizaciones antes de distribuir**

El Servidor de administración descarga las actualizaciones desde el origen, las guarda en un repositorio temporal y ejecuta la tarea definida en el campo **Tarea de verificación de actualizaciones**. Si la tarea se completa con éxito, las actualizaciones se copian desde el repositorio temporal a una carpeta compartida en el Servidor de administración y luego se distribuyen a todos los dispositivos para los cuales el Servidor de administración actúa como fuente de actualizaciones (tareas con el tipo de programación **Cuando se descargan nuevas actualizaciones en el repositorio** empezada). La tarea de descargar actualizaciones al repositorio se termina solo después de completar la tarea *Verificación de actualizaciones*.

Esta opción está desactivada de forma predeterminada.

- **Tarea de verificación de actualizaciones**

  Esta tarea verifica las actualizaciones descargadas antes de que se distribuyan a todos los dispositivos para los cuales el Servidor de administración actúa como fuente de actualizaciones.

  En este campo, puede especificar la tarea *Actualizar verificación* creada anteriormente. O bien, puede crear una nueva tarea *Actualizar verificación*.

Descargar actualizaciones en los repositorios de la configuración de tareas de los puntos de distribución

Configuraciones especificadas durante la creación de tareas

Puede especificar los siguientes ajustes al crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- **Orígenes de actualizaciones**

Los recursos siguientes pueden utilizarse como origen de actualizaciones para el punto de distribución:

- Servidores de actualización de Kaspersky

  Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación.

  Esta opción está seleccionada de forma predeterminada.

- Servidor de administración principal

  Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

- Carpeta local o de red

  Una carpeta local o de red que contiene las últimas actualizaciones. Una carpeta de red puede ser un servidor FTP o HTTP o un recurso compartido SMB. Si una carpeta de red requiere autenticación, solo se admite el protocolo SMB. Cuando se selecciona una carpeta local, debe especificar una carpeta en un dispositivo que tenga el Servidor de administración instalado.

  Un servidor FTP o HTTP o una carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura creada al usar los servidores de actualización de Kaspersky.

Si activa la opción **No usar servidor proxy** para los orígenes de actualización Servidores de actualización de Kaspersky o Carpeta local o de red, un punto de distribución no usa un servidor proxy para descargar actualizaciones, incluso si ha activado la opción **Usar servidor proxy** la configuración de la directiva del Agente de red para el punto de distribución.

- **Otros parámetros**

  - **Carpeta para almacenar actualizaciones**

    La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

Configuraciones especificadas después de la creación de tareas

Puede especificar la siguiente configuración solo después de crear una tarea.

- Sección **Configuración**, bloque **Contenido de las actualizaciones**.

  - **Descargar archivos diff**

    Esta opción habilita la función de descarga de archivos diff.

    Esta opción está desactivada de forma predeterminada.

Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

Configuraciones especificadas durante la creación de tareas

Puede especificar los siguientes ajustes al crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- **Buscar vulnerabilidades y actualizaciones en la lista de Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

  Por ejemplo, es posible que desee desactivar esta opción si tiene diferentes tareas con diferentes configuraciones para las actualizaciones de Microsoft y las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

  - **Conectar al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update en un dispositivo administrado se conecta al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como origen de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center (consulte la configuración de la directiva del Agente de red)
- Windows Server con Servicio de Windows Server Update (WSUS) de Microsoft desplegado en la red de su organización
- Servidores de actualización de Microsoft

Si se activa esta opción, el Agente de Windows Update en un dispositivo administrado se conecta al origen de actualizaciones de Microsoft para actualizar la información sobre las actualizaciones aplicables de Microsoft Windows.

Si se desactiva esta opción, el Agente de Windows Update en un dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que se recibió desde el origen de actualizaciones de Microsoft anteriormente y que se almacena en el caché del dispositivo.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Es posible que quiera desactivar esta opción si establece una conexión periódica a este origen de actualizaciones en otra tarea o en las propiedades de la directiva del Agente de red, en la sección **Vulnerabilidades y actualizaciones de software**. Si no desea desactivar esta opción, para reducir la sobrecarga del servidor, puede configurar la programación de tareas para aleatorizar el retraso del inicio de la tarea en 360 minutos.

Esta opción está activada de forma predeterminada.

La combinación de las siguientes opciones de la configuración de la directiva del Agente de red define el modo de obtener actualizaciones:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada y se selecciona la opción **Activo** en el grupo de configuración **Modo de búsqueda de Windows Update**.
- El Agente de Windows Update en un dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que se recibió del origen de actualizaciones de Microsoft anteriormente y que se almacena en el caché del dispositivo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada y se selecciona la opción **Pasivo** en el grupo de configuración **Modo de búsqueda de Windows Update** o si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está desactivada y se selecciona la opción **Activo** en el grupo de configuración **Modo de búsqueda de Windows Update**.
- Independientemente del estado de la opción **Conectar al servidor de actualizaciones para actualizar los datos** (activado o desactivado), si la opción **Desactivado**, se selecciona en el grupo de configuración **Modo de búsqueda de Windows Update**, Kaspersky Security Center no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones de terceros en la lista de Kaspersky

Si esta opción está activada, Kaspersky Security Center busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especificar rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky gestiona la lista completa de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Por ejemplo, es posible que desee desactivar esta opción si tiene diferentes tareas con diferentes configuraciones para las actualizaciones de Microsoft Windows y las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- **Especificar rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Las carpetas en las que Kaspersky Security Center busca aplicaciones de terceros que requieren reparación de la vulnerabilidad e instalaciones de actualizaciones. Puede usar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- **Activar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe los seguimientos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los seguimientos se escriben en dos archivos a su vez; el tamaño total de ambos archivos se determina por el valor **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando ambos archivos están llenos, el Agente de red comienza a escribirles de nuevo. Los archivos con seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se escriben rastros adicionales.

  Al crear una tarea, no tiene que habilitar los diagnósticos avanzados. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está desactivada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky le pidan que cambie el valor predeterminado cuando la información de los archivos de diagnóstico avanzado que les envía no es suficiente para solucionar el problema.

Instale las actualizaciones necesarias y corrija las configuraciones de tareas de vulnerabilidades

Configuraciones especificadas durante la creación de tareas

Puede especificar los siguientes ajustes al crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- **Especificar reglas para instalar actualizaciones**

  Estas reglas se aplican a la instalación de actualizaciones en dispositivos cliente. Si no se especifican las reglas, la tarea no tiene nada que realizar. Para obtener información sobre las operaciones con reglas, consulte Reglas para la instalación de actualizaciones.

- **Iniciar la instalación al reiniciar o apagar el dispositivo**

  Si esta opción está activada, las actualizaciones se instalan cuando el dispositivo se reinicia o se apaga. De lo contrario, las actualizaciones se instalan de acuerdo con una programación.

  Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento del dispositivo.

  Esta opción está desactivada de forma predeterminada.

- **Instalar componentes generales del sistema requeridos**

  Si esta opción está activada, antes de instalar una actualización, la aplicación instala automáticamente todos los componentes generales del sistema (requisitos previos) que se requieren para instalar la actualización. Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo

  Si esta opción está desactivada, es posible que tenga que instalar los requisitos previos de manera manual.

  Esta opción está desactivada de forma predeterminada.

- **Autorizar la instalación de las nuevas versiones de la aplicación durante las actualizaciones**

  Si esta opción está activada, las actualizaciones se permiten cuando dan lugar a la instalación de una nueva versión de una aplicación de software.

  Si esta opción se desactiva, el software no se actualiza. A continuación, puede instalar nuevas versiones del software de manera manual o mediante otra tarea. Por ejemplo, puede usar esta opción si la infraestructura de su empresa no es compatible con una nueva versión del software o si desea verificar una actualización en una infraestructura de prueba.

  Esta opción está activada de forma predeterminada.

  La actualización de una aplicación puede causar un mal funcionamiento de las aplicaciones dependientes instaladas en los dispositivos cliente.

- **Descargar actualizaciones en el dispositivo sin instalarlas**

  Si esta opción está activada, la aplicación descarga actualizaciones en el dispositivo pero no las instala automáticamente. A continuación, puede instalar las actualizaciones descargadas de manera manual.

  Las actualizaciones de Microsoft se descargan al sistema de almacenamiento de Windows. Las actualizaciones de aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) se descargan en la carpeta especificada en el campo de **Carpeta para la descarga de actualizaciones**.

  Si esta opción está desactivada, las actualizaciones se instalan en el dispositivo automáticamente.

  Esta opción está desactivada de forma predeterminada.

- Carpeta para la descarga de actualizaciones

  Esta carpeta se utiliza para descargar actualizaciones de aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft).

- Activar diagnóstico avanzado

  Si esta función está habilitada, el Agente de red escribe los seguimientos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los seguimientos se escriben en dos archivos a su vez; el tamaño total de ambos archivos se determina por el valor **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando ambos archivos están llenos, el Agente de red comienza a escribirles de nuevo. Los archivos con seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se escriben rastros adicionales.

  Al crear una tarea, no tiene que habilitar los diagnósticos avanzados. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está desactivada de forma predeterminada.

- Tamaño máximo, en MB, de los archivos de diagnóstico avanzado

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky le pidan que cambie el valor predeterminado cuando la información de los archivos de diagnóstico avanzado que les envía no es suficiente para solucionar el problema.

Configuraciones especificadas después de la creación de tareas

Puede especificar la siguiente configuración solo después de crear una tarea.

- Actualizaciones para instalar

  En la sección **Actualizaciones para instalar**, puede ver la lista de actualizaciones que instala la tarea. Solo se muestran las actualizaciones que coinciden con la configuración de tareas aplicada.

- Prueba de instalación de actualizaciones:

  - **No analizar**. Seleccione esta opción si no desea realizar una instalación de prueba de las actualizaciones.
  - **Ejecute el análisis en dispositivos seleccionados**. Seleccione esta opción si desea probar la instalación de actualizaciones en determinados dispositivos. Haga clic en el botón **Agregar** y seleccione los dispositivos en los que desea realizar una instalación de prueba de las actualizaciones.
  - **Ejecutar el análisis en dispositivos del grupo especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en un grupo de dispositivos. En el campo **Especificar un grupo de prueba**, especifique un grupo de dispositivos en los que desee realizar una instalación de prueba.
  - **Ejecutar el análisis en el porcentaje de dispositivos especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en parte de los dispositivos. En el campo **Porcentaje de dispositivos de prueba del total de dispositivos de destino**, especifique el porcentaje de equipos en el que desea realizar una instalación de prueba de las actualizaciones.

Lista global de subredes

Esta sección proporciona información sobre la lista global de subredes que puede usar en las reglas.

Para almacenar la información sobre las subredes de su red, puede configurar una lista global de subredes para cada Servidor de administración que utilice. Esta lista le ayuda a hacer coincidir los pares {dirección IP, máscara} y unidades físicas y sucursales. Puede usar subredes de esta lista en las reglas y configuraciones de red.

Añadir subredes a la lista global de subredes

Puede agregar subredes con sus descripciones a la lista global de subredes.

Para añadir subredes a la lista global de subredes:

1. En el árbol de la consola, seleccione el nodo del Servidor de administración que necesite.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana **Propiedades** que se abre, en el panel **Secciones**, seleccione **Lista de subredes globales**.
4. Haga clic en el botón **Agregar**.
   Se abre la ventana **Nueva subred**.
5. Rellene los siguientes campos:
   - **Configuración general**

     La dirección de subred para la subred que está añadiendo.
   - **Máscara de subred**

     La máscara de subred para la subred que está añadiendo.
   - **Nombre**

     Nombre de la subred. Debe ser único dentro de la lista global de subredes. Si introduce el nombre que ya existe en la lista, se añadirá un índice, por ejemplo: ~~ 1, ~~ 2.
   - **Descripción**

     La descripción puede contener información adicional sobre la sucursal que tiene esta subred. Este texto aparecerá en todas las listas donde esté presente esta subred, por ejemplo, en la lista de reglas de limitación de tráfico.

     Este campo no es obligatorio y puede dejarse vacío.
6. Haga clic en **Aceptar**.

La subred aparece en la lista de subredes.

Ver y modificar las propiedades de subred en la lista global de subredes

Puede ver y modificar las propiedades de las subredes en la lista global de subredes.

Ver o modificar propiedades de una subred en la lista global de subredes:

1. En el árbol de la consola, seleccione el nodo del Servidor de administración que necesite.
2. Seleccione **Propiedades** en el menú contextual del Servidor de administración.
3. En la ventana **Propiedades** que se abre, en el panel de la izquierda **Secciones**, seleccione **Lista de subredes globales**.
4. En la lista, seleccione la subred que desee.
5. Haga clic en el botón **Propiedades**.
   Se abre la ventana **Nueva subred**.
6. Si es necesario, cambie la configuración de la subred.
7. Haga clic en **Aceptar**.

Si ha realizado cambios, serán almacenados.

Usar el Agente de red para Windows, macOS y Linux: comparación

El uso del Agente de red varía según el sistema operativo del dispositivo. La directiva del Agente de red y la configuración del paquete de instalación también difieren según el sistema operativo. La siguiente tabla compara las características del Agente de red y los escenarios de uso disponibles para los sistemas operativos Windows, macOS y Linux.

Función del Agente de red: comparación

Función del Agente de red	Windows	macOS	Linux
Instalación			
Generación automática del paquete de instalación del Agente de red después de la instalación de Kaspersky Security Center	✓	–	–
Instalación en modo forzado, usando opciones especiales en la tarea de instalación remota de Kaspersky Security Center	✓	✓	✓
Instalación al enviar a	✓	✓	✓

usuarios del dispositivo enlaces con paquetes independientes generados por Kaspersky Security Center.			
Instalación mediante la clonación de una imagen del disco duro del administrador con el sistema operativo y el Agente de red usando instrumentos proporcionados por Kaspersky Security Center.	✓	–	–
Instalación mediante la clonación de una imagen del disco duro del administrador con el sistema operativo y el Agente de red mediante instrumentos de terceros	✓	✓	✓
Instalación con herramientas de terceros para la instalación remota de aplicaciones	✓	✓	✓
Instalación manual, al ejecutar instaladores de la aplicación en dispositivos	✓	✓	✓
Instalación del Agente de red en modo silencioso	✓	✓	✓
Instalación del Agente de red en modo no interactivo	✓	✓	✓
Conexión manual del dispositivo cliente al Servidor de administración. Utilidad klmover	✓	✓	✓
Instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center	✓	–	–
Distribución automática de una clave	✓	✓	✓
Forzar sincronización	✓	✓	✓
Punto de distribución			
La utilización como punto de distribución	✓	✓	✓

Asignación automática de puntos de distribución	✓	✓ Sin utilizar la autenticación de nivel de red (NLA).	✓ Sin utilizar la autenticación de nivel de red (NLA).
Modelo de descarga de actualizaciones sin conexión	✓	✓	✓
Todos los tipos de encuestas de red	✓	–	–
Ejecución del servicio de proxy de KSN en un punto de distribución	✓	–	–
Descarga de actualizaciones en los repositorios de puntos de distribución directamente desde los servidores de actualización de Kaspersky	✓	– (si uno o más dispositivos incluidos en la cobertura de la tarea Descargar actualizaciones en los repositorios de puntos de distribución ejecutan Linux o macOS, la tarea se completa con el estado Fallo, incluso si se completa correctamente en todos los dispositivos de Windows)	✓
Instalación de inserción de aplicaciones en dispositivos con Windows	✓	Después de definir el tipo de sistema operativo en los dispositivos en red a través de un sondeo, el Servidor de administración no intentará realizar la instalación push en dispositivos Windows mediante puntos de distribución que no sean de Windows	Después de definir el tipo de sistema operativo en los dispositivos en red a través de un sondeo, el Servidor de administración no intentará realizar la instalación push en dispositivos Windows mediante puntos de distribución que no sean de Windows
Cómo usar un servidor push	✓	–	✓
Manipulación de otras aplicaciones			
Instalación remota de aplicaciones en dispositivos	✓	–	–
Actualizaciones de software	✓	–	–
Configuración de actualizaciones del sistema operativo en una directiva de Agente de red	✓	–	–
Consultar información sobre vulnerabilidades de software	✓	–	–
Análisis de aplicaciones para buscar vulnerabilidades	✓	–	–
Inventario del software	✓	–	–

instalado en dispositivos			
Visualización del registro de aplicaciones	✓	–	–
Máquinas virtuales			
Instalación del Agente de red en una máquina virtual	✓	✓	✓
Optimización de la configuración para Infraestructura de Escritorio Virtual (VDI)	✓	✓	✓
Compatibilidad para máquinas virtuales dinámicas	✓	✓	✓
Otro			
Acciones de auditoría en un dispositivo cliente remoto mediante el uso compartido del escritorio de Windows	✓	–	–
Supervisión del estado de protección antivirus.	✓	✓	✓
Administración de reinicios de dispositivos	✓	–	–
Soporte de restauración del sistema de archivos	✓	✓	✓
Uso de un Agente de red como puerta de enlace de conexión	✓	✓	✓
Administrador de conexiones	✓	✓	✓
Cambio de un Servidor de administración a otro en Agente de red (automáticamente según la ubicación de red)	✓	✓	–
Comprobación de la conexión entre un dispositivo cliente y el Servidor de administración. Utilidad klnagchk	✓	✓	✓
Conexión remota con el escritorio de un dispositivo cliente	✓	✓ Mediante el uso del sistema de computación virtual en red (VNC).	–
Descarga de un paquete de instalación independiente a través del Asistente de migración	✓	✓	✓

Sondeo de Zeroconf	–	–	✓

Kaspersky Security Center 14 Web Console

Esta sección describe las operaciones que puede realizar utilizando Kaspersky Security Center 14 Web Console.

Acerca de Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console es una aplicación web diseñada para administrar el estado del sistema de seguridad de una red protegida por aplicaciones de Kaspersky.

Al usar la aplicación, puede realizar lo siguiente:

- Administrar el estado del sistema de seguridad de la organización.
- Instalar aplicaciones de Kaspersky en dispositivos de su red y administrar aplicaciones instaladas.
- Administrar directivas creadas para dispositivos de su red.
- Administrar cuentas de usuario.
- Administrar tareas de aplicaciones instaladas en sus dispositivos de red.
- Ver informes del estado de seguridad del sistema.
- Administrar el envío de informes a administradores de sistemas y a otros especialistas de TI.

Kaspersky Security Center 14 Web Console proporciona una interfaz web que garantiza la comunicación entre su dispositivo y el Servidor de administración a través de un navegador. El Servidor de administración es una aplicación diseñada para administrar las aplicaciones Kaspersky instaladas en los dispositivos de red. El Servidor de administración se conecta con los dispositivos de su red a través de canales protegidos con Secure Socket Layer (SSL). Cuando se conecta a Kaspersky Security Center 14 Web Console con su navegador, el navegador establece una conexión con Servidor de Kaspersky Security Center 14 Web Console.

Esto es lo que debe hacer para usar Kaspersky Security Center 14 Web Console:

1. Use un navegador para conectarse a Kaspersky Security Center 14 Web Console, donde se muestra la interfaz del portal web.
2. Utilice los controles del portal de Internet para elegir un comando que desea ejecutar. Kaspersky Security Center 14 Web Console realiza las siguientes operaciones:
    - Si selecciona un comando usado para recibir información (por ejemplo, para ver una lista de dispositivos), Kaspersky Security Center 14 Web Console genera una solicitud de información al Servidor de administración, recibe los datos necesarios y los envía al navegador en un formato de fácil visualización.
    - Si ha elegido un comando de administración (por ejemplo, la instalación remota de una aplicación), Kaspersky Security Center 14 Web Console recibe el comando del navegador y lo envía al Servidor de administración. Posteriormente, la aplicación recibe el resultado del Servidor de administración y lo envía al navegador en un formato fácil de visualizar.

Kaspersky Security Center 14 Web Console es una aplicación multilingüe. Puede cambiar el idioma de la interfaz en cualquier momento, sin volver a abrir la aplicación. Cuando instala Kaspersky Security Center 14 Web Console junto con Kaspersky Security Center, Kaspersky Security Center 14 Web Console tiene el mismo idioma de la interfaz que el archivo de instalación. Cuando solo instala Kaspersky Security Center 14 Web Console, la aplicación tiene el mismo idioma de la interfaz que su sistema operativo. Si Kaspersky Security Center 14 Web Console no es compatible con el idioma del archivo de instalación o del sistema operativo, se establece el idioma inglés de forma predeterminada.

La Administración de dispositivos móviles no es compatible con Kaspersky Security Center 14 Web Console. Sin embargo, si agregó dispositivos móviles a un grupo de administración utilizando Microsoft Management Console, estos dispositivos también se muestran en Kaspersky Security Center 14 Web Console.

Requisitos de hardware y software para Kaspersky Security Center 14 Web Console

Servidor de Kaspersky Security Center 14 Web Console

Requisitos mínimos de hardware:

- CPU: 4 núcleos, frecuencia de operación de 2,5 GHz.
- Memoria RAM: 8 GB
- Espacio disponible en disco: 40 GB.

Se admiten los siguientes sistemas operativos:

- Sistema operativo (versiones de solo 64 bits):
  - Microsoft Windows 10 Enterprise 2015 LTSB.
  - Microsoft Windows 10 Enterprise 2016 LTSB.
  - Microsoft Windows 10 Enterprise 2019 LTSC.
  - Microsoft Windows 10 Pro RS5 (Actualización de octubre de 2018, 1809).
  - Microsoft Windows 10 Pro for Workstations RS5 (Actualización de octubre de 2018, 1809).
  - Microsoft Windows 10 Enterprise RS5 (Actualización de octubre de 2018, 1809).
  - Microsoft Windows 10 Education RS5 (Actualización de octubre de 2018, 1809).
  - Microsoft Windows 10 Pro 19H1.
  - Microsoft Windows 10 Pro for Workstations 19H1.
  - Microsoft Windows 10 Enterprise 19H1.
  - Microsoft Windows 10 Education 19H1.
  - Microsoft Windows 10 Pro 19H2.

- Microsoft Windows 10 Pro for Workstations 19H2.
- Microsoft Windows 10 Enterprise 19H2.
- Microsoft Windows 10 Education 19H2.
- Microsoft Windows 10 Home 20H1 (actualización de mayo de 2020).
- Microsoft Windows 10 Pro 20H1 (actualización de mayo de 2020).
- Microsoft Windows 10 Enterprise 20H1 (actualización de mayo de 2020).
- Microsoft Windows 10 Education 20H1 (actualización de mayo de 2020).
- Microsoft Windows 10 Home 20H2 (actualización de octubre de 2020).
- Microsoft Windows 10 Pro 20H2 (actualización de octubre de 2020).
- Microsoft Windows 10 Enterprise 20H2 (actualización de octubre de 2020).
- Microsoft Windows 10 Education 20H2 (actualización de octubre de 2020).
- Microsoft Windows 10 Home 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Education 21H1 (actualización de mayo de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Home 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Pro 21H2 (actualización de octubre de 2021) 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 21H2 (actualización de octubre de 2021) 32 bits/64 bits.
- Microsoft Windows 10 Education 21H2 (actualización de octubre de 2021) 32 bits/64 bits.
- Microsoft Windows 11 Home.
- Microsoft Windows 11 Pro.
- Microsoft Windows 11 Enterprise.
- Microsoft Windows 11 Education.
- Windows Server 2012 Server Core.
- Windows Server 2012 Datacenter.
- Windows Server 2012 Essentials.
- Windows Server 2012 Foundation.
- Windows Server 2012 Standard.

- Windows Server 2012 R2 Server Core.
- Windows Server 2012 R2 Datacenter.
- Windows Server 2012 R2 Essentials.
- Windows Server 2012 R2 Foundation.
- Windows Server 2012 R2 Standard.
- Windows Server 2016 Datacenter (LTSB).
- Windows Server 2016 Standard (LTSB).
- Windows Server 2016 Server Core (Opción de instalación) (LTSB).
- Windows Server 2019 Standard 64 bits.
- Windows Server 2019 Datacenter 64 bits.
- Windows Server 2019 Core 64 bits.
- Windows Server 2022 Standard 64 bits.
- Windows Server 2022 Datacenter 64 bits.
- Windows Server 2022 Core 64 bits.
- Windows Storage Server 2012 64 bits.
- Windows Storage Server 2012 R2 64 bits.
- Windows Storage Server 2016 64 bits.
- Windows Storage Server 2019 64 bits.

- Linux (solo versiones de 64 bits):
  - 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 (todos los Service Packs).

- SUSE Linux Enterprise Server 15 (todos los Service Packs).
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM.
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio).
- Astra Linux Special Edition 1.6 (incluido el modo de entorno de software cerrado y el modo obligatorio).
- Astra Linux Common Edition 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 Certified Edition.

Entre las plataformas de virtualización, la máquina virtual basada en kernel es compatible con los siguientes sistemas operativos:

- Alt 8 SP Server (LKNV.11100-01) 64 bits.
- Alt Server 10 64 bits.
- Astra Linux Special Edition 1.7 (incluido el modo de entorno de software cerrado y el modo obligatorio) 64 bits.
- Debian GNU/Linux 11.x (Bullseye) 32-bit / 64-bit.
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 bits.
- RED OS 7.3 Server 64 bits.
- RED OS 7.3 Certified Edition 64 bits.

Kaspersky Security Center 14 Web Console Server no es compatible con los siguientes sistemas operativos:

- Microsoft Windows Essential Business Server 2008 Standard/Premium.
- Microsoft Windows Small Business Server 2003 Standard/Premium con SP1.
- Microsoft Windows Small Business Server 2003 R2 Standard/Premium.
- Microsoft Windows Small Business Server 2008 Standard/Premium.
- Microsoft Windows Small Business Server 2011 Essentials.

- Microsoft Windows Small Business Server 2011 Premium Add-on.
- Microsoft Windows Small Business Server 2011 Standard.
- Microsoft Windows Home Server 2011.
- Microsoft Windows MultiPoint Server 2010 Standard/Premium.
- Microsoft Windows MultiPoint Server 2011 Standard/Premium.
- Microsoft Windows MultiPoint Server 2012 Standard/Premium.
- Microsoft Windows Server 2000.
- Microsoft Windows Server 2003 Enterprise con SP2.
- Microsoft Windows Server 2003 Standard con SP2.
- Microsoft Windows Server 2003 R2 Enterprise con SP2.
- Microsoft Windows Server 2003 R2 Standard con SP2.

Dispositivos cliente

Para un dispositivo cliente, el uso de Kaspersky Security Center 14 Web Console solo requiere un navegador.

Los requisitos de hardware y software del dispositivo son idénticos a los del navegador utilizado para Kaspersky Security Center 14 Web Console.

Navegadores:

- Mozilla Firefox Extended Support Release 91.8.0 o superior (la versión 91.8.0 se lanzó el 5 de abril de 2022)
- Mozilla Firefox Release 99.0 o superior (la versión 99.0 se lanzó el 5 de abril de 2022)
- Google Chrome 100.0.4896.88 o superior (compilación oficial)
- Microsoft Edge 100 o superior

Diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console

La siguiente figura muestra el diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console.

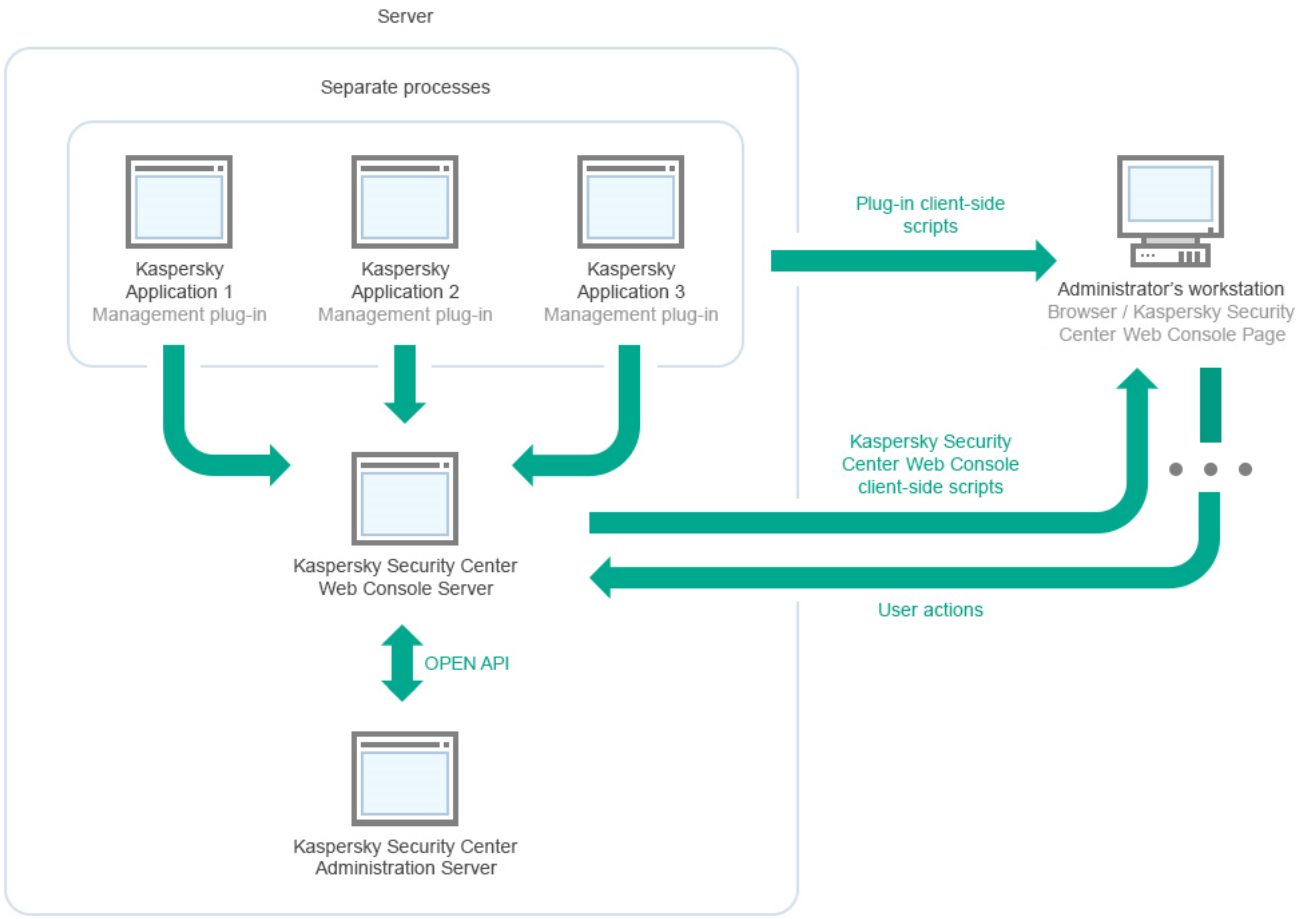


Diagrama de despliegue del Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console

Los complementos de administración para aplicaciones de Kaspersky instaladas en dispositivos protegidos (un complemento para cada aplicación) se despliegan junto con el servidor de Kaspersky Security Center 14 Web Console.

Como administrador, usted accede a Kaspersky Security Center 14 Web Console mediante un navegador en su estación de trabajo.

Cuando realiza acciones específicas en Kaspersky Security Center 14 Web Console, Kaspersky Security Center 14 Servidor de Web Console se comunica con el Servidor de administración de Kaspersky Security Center a través de OpenAPI. El servidor de Kaspersky Security Center 14 Web Console solicita la información requerida del Servidor de administración de Kaspersky Security Center y muestra los resultados de sus operaciones en Kaspersky Security Center 14 Web Console.

Puertos utilizados por Kaspersky Security Center 14 Web Console

La siguiente tabla enumera los puertos que deben estar abiertos en el dispositivo donde está instalado Kaspersky Security Center 14 Web Console Server (también conocido como Kaspersky Security Center 14 Web Console).

Puertos utilizados por Kaspersky Security Center 14 Web Console

Nombre de servicio	Número de puerto	Protocolo	Objetivo del puerto	Cob
KSCWebConsole	2001	HTTPS	Puerto API que se utiliza para recibir solicitudes del servicio	Ejecuc proces node.e

			KSCWebConsoleManagementService que se ejecuta en el mismo dispositivo	tanto Kasper Securi Cente Consc los compl de admini
KSCWebConsoleManagementService	2003	HTTPS	Puerto API que se utiliza para recibir solicitudes del servicio KSCWebConsole que se ejecuta en el mismo dispositivo	Actual de los compc de Kas Securi Cente Consc
Kaspersky OSMP KAS Service	3333	HTTPS	Puerto de punto final de autorización OAuth2.0	Identit Acces Manag
Kaspersky OSMP Facade Service	4004	HTTPS	Puerto del proveedor de identidad OAuth2.0	Identit Acces Manag
Kaspersky OSMP KAS Service	4444	HTTPS	Puerto del punto final de introspección de tokens OAuth2.0	Identit Acces Manag
KSCWebConsoleMessageQueue	8200	HTTP	Puerto API que se utiliza para generar certificados mediante HashiCorp Vault (para obtener más detalles, consulte el sitio web de HashiCorp Vault)	Instala Kasper Securi Cente Consc actuali de los compc de Kas Securi Cente Consc
KSCWebConsoleMessageQueue	4152	HTTPS	Puerto API del agente de mensajes que se utiliza para la comunicación entre los procesos de Kaspersky Security Center 14 Web Console y los complementos de administración	Interac entre Kasper Securi Cente Consc compl de admini

La siguiente tabla enumera los puertos que no tienen que estar abiertos en el dispositivo en el que está instalado Kaspersky Security Center 14 Web Console Server. Sin embargo, Kaspersky Security Center 14 Web Console utiliza estos puertos para Identity and Access Manager.

Puertos utilizados por Kaspersky Security Center 14 Web Console para Identity and Access Manager

Nombre	Número	Protocolo	Objetivo del puerto	Cobertura

de servicio	de puerto			
Kaspersky OSMP KAS Service	4445	HTTPS	Puerto principal de Identity and Access Manager que recibe la configuración de Kaspersky Security Center 14 Web Console para el puerto de punto final de autorización OAuth2.0 (para obtener más información sobre OAuth 2.0, consulte el sitio web de OAuth)	Identity and Access Manager
Kaspersky OSMP Facade Service	2444	HTTPS	Puerto para la configuración de Identity and Access Manager	Identity and Access Manager
Kaspersky OSMP Facade Service	2445	HTTPS	Puerto para la conexión de Kaspersky OSMP KAS Service a Kaspersky OSMP Facade Service	Identity and Access Manager

Escenario: Instalación y configuración inicial de Kaspersky Security Center 14 Web Console

Este escenario describe cómo instalar el Servidor de administración de Kaspersky Security Center 14 y la Kaspersky Security Center 14 Web Console, realizar la configuración inicial del Servidor de administración utilizando el Asistente de inicio rápido e instalar las aplicaciones de Kaspersky en los dispositivos administrados utilizando el Asistente de despliegue de la protección.

La instalación y configuración inicial de Kaspersky Security Center 14 Web Console sucede en etapas:

1. **Instalación de un sistema de gestión de bases de datos (DBMS)**

   Instale el DBMS que utilizará Kaspersky Security Center o utilice uno existente.

2. **Instalación del Servidor de administración, la Consola de administración y el Agente de red**

   La Consola de administración y la versión de servidor del Agente de red se instalan junto con el Servidor de administración.

   Durante la instalación del Servidor de administración de Kaspersky Security Center 14, especifique si desea instalar Kaspersky Security Center 14 Web Console en el mismo dispositivo. Si elige instalar ambos componentes en el mismo dispositivo, no tiene que instalar Kaspersky Security Center 14 Web Console por separado, ya que se instala automáticamente. Si desea instalar la Kaspersky Security Center 14 Web Console en un dispositivo diferente, después de instalar el Servidor de administración de Kaspersky Security Center 14, proceda a instalar la Kaspersky Security Center 14 Web Console.

3. **Instalación de Kaspersky Security Center 14 Web Console**

   Si no eligió instalar Kaspersky Security Center 14 Web Console junto con el Servidor de administración de Kaspersky Security Center en el paso anterior, instale Kaspersky Security Center 14 Web Console por separado. Puede instalar Kaspersky Security Center 14 Web Console en un dispositivo diferente o en el mismo dispositivo donde está instalado el Servidor de administración.

4. **Realizar la configuración inicial**

   Cuando la instalación del Servidor de administración se completa, en la primera conexión con el Servidor de administración, el Asistente de inicio rápido comienza automáticamente. Realice la configuración inicial del Servidor de administración según los requisitos existentes. Durante la etapa de configuración inicial, el Asistente usa la configuración predeterminada para crear las directivas y las tareas que son necesarias para desplegar la protección. Sin embargo, las configuraciones predeterminadas pueden no ser óptimas para las necesidades de su organización. Puede editar la configuración de directivas y tareas si es necesario.

5. **Licencias de Kaspersky Security Center (opcional)**

   El uso de Kaspersky Security Center con la funcionalidad básica de la Consola de Administración no requiere una licencia. Necesita una licencia comercial si desea usar una o varias de las funciones adicionales, que incluyen Administración de vulnerabilidades y parches, Administración de dispositivos móviles e Integración con los sistemas SIEM. Puede agregar una archivo clave o un código de activación para estas funciones en el paso correspondiente del Asistente de inicio rápido o manualmente.

6. **Detección de dispositivos de red**

   Esta etapa forma parte del Asistente de inicio rápido. También puede descubrir los dispositivos manualmente. Kaspersky Security Center recibe las direcciones y los nombres de todos los dispositivos detectados en la red. A continuación, puede usar Kaspersky Security Center para instalar aplicaciones y software de Kaspersky desde otros proveedores en los dispositivos detectados. Cada cierto tiempo, Kaspersky Security Center inicia una detección de dispositivos, lo que significa que si aparece alguna instancia nueva en la red, se la detectará automáticamente.

7. **Organización de dispositivos en grupos de administración**

   Esta etapa forma parte del Asistente de inicio rápido pero también puede mover los dispositivos detectados a grupos manualmente.

8. **Instalación del Agente de red y de aplicaciones de seguridad en dispositivos en red**

   El despliegue de la protección en una red empresarial implica la instalación del Agente de red y de aplicaciones de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) en dispositivos que el Servidor de administración ha detectado durante la detección de dispositivos.

   Para instalar las aplicaciones de forma remota, ejecute el Asistente de despliegue de la protección.

   Las aplicaciones de seguridad protegen los dispositivos frente a virus y otros programas que suponen una amenaza. El Agente de red garantiza la comunicación entre el dispositivo y el Servidor de administración. Los ajustes del Agente de red se configuran automáticamente de forma predeterminada.

   Antes de iniciar la instalación del Agente de red y las aplicaciones de seguridad en los dispositivos de la red, asegúrese de que pueda acceder a estos dispositivos (es decir, que estén encendidos).

9. **Despliegue de claves de licencia en dispositivos cliente**

   Despliegue claves de licencia en los dispositivos cliente para activar las aplicaciones de seguridad administradas en esos dispositivos.

10. **Instalación de Kaspersky Security for Mobile (opcional)**

    Si planea administrar dispositivos móviles corporativos, siga las instrucciones proporcionadas en la Ayuda de Kaspersky Security para dispositivos móviles para obtener información sobre la implementación de Kaspersky Endpoint Security for Android.

11. **Configuración de las directivas de aplicaciones de Kaspersky**

    Para aplicar diferentes configuraciones de aplicaciones a diferentes dispositivos, puede usar la administración de seguridad centrada en el dispositivo, la administración de seguridad centrada en el usuario o una combinación de estos dos enfoques. La administración de la seguridad centrada en el dispositivo se puede implementar mediante el uso de directivas y tareas. Solo puede aplicar tareas a aquellos dispositivos que cumplan condiciones específicas. Para establecer las condiciones para filtrar dispositivos, use selecciones de dispositivos y etiquetas.

12. **Supervisión del estado de protección de la red**

    Puede supervisar su red utilizando widgets en el panel, generar informes desde las aplicaciones de Kaspersky, configurar y ver selecciones de eventos recibidos de las aplicaciones en los dispositivos administrados y ver listas de notificaciones.

Instalación

Esta sección describe la instalación de Kaspersky Security Center y Kaspersky Security Center 14 Web Console.

Instalación de un sistema de administración de bases de datos

Instale el sistema de administración de bases de datos (DBMS) que utilizará Kaspersky Security Center. Puede escoger entre una de las versiones compatibles de Microsoft SQL Server, MySQL o MariaDB.

Para obtener información sobre cómo instalar el DBMS seleccionado, consulte su documentación.

Para un uso óptimo de MariaDB, debe configurar los ajustes recomendados.

Configurar el servidor MariaDB x64 para trabajar con Kaspersky Security Center 14

Kaspersky Security Center 14 es compatible con la versión 10.3 de MariaDB (compilación 10.3.22 y posteriores).

Si utiliza el servidor MariaDB para Kaspersky Security Center, active la compatibilidad con el almacenamiento InnoDB y MEMORY y con las codificaciones UTF-8 y UCS-2.

Configuración recomendada para el archivo my.ini

Para configurar el archivo my.ini:

1. Abra el archivo my.ini en un editor de textos.

2. Añada las siguientes líneas a la sección `[mysqld]` del archivo my.ini:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<value>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

El valor de `innodb_buffer_pool_size` no debe ser inferior al 80% del tamaño previsto de la base de datos KAV.

Se recomienda utilizar el valor del parámetro `innodb_flush_log_at_trx_commit=0`, porque los valores "1" o "2" afectan negativamente a la velocidad de funcionamiento de MariaDB.

Por defecto, los complementos del optimizador `join_cache_incremental`, `join_cache_hashed`, y `join_cache_bka` están habilitados. Si estos complementos no están habilitados, debe habilitarlos.

Para comprobar si los complementos del optimizador están habilitados:

1. En la consola del cliente MariaDB, ejecute el comando:

   ```
   SELECT @@optimizer_switch;
   ```

2. Compruebe que la salida contenga las siguientes líneas:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Si estas líneas están presentes y tienen el valor `on (activado)`, entonces los complementos del optimizador están habilitados.

   Si estas líneas faltan o tienen el valor `off (desactivado)`, haga lo siguiente:

   1. Abra el archivo my.ini en un editor de textos.

   2. Añada las siguientes líneas a la sección `[mysqld]` del archivo my.ini:

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

Los complementos `join_cache_incremental`, `join_cache_hash`, and `join_cache_bka` están habilitados.

Configurar el servidor MySQL x64 para que funcione con Kaspersky Security Center 14

Si utiliza el servidor MySQL para Kaspersky Security Center, active la compatibilidad del almacenamiento InnoDB y MEMORY, y las codificaciones UTF-8 y UCS-2.

Configuración recomendada para el archivo my.ini

Para configurar el archivo my.ini:

1. Abra el archivo my.ini en un editor de textos.

2. Añada las siguientes líneas a la sección `[mysqld]` del archivo my.ini:

   ```
   sort_buffer_size = 10M
   join_buffer_size = 20M
   tmp_table_size = 600M
   max_heap_table_size = 600M
   key_buffer_size = 200M
   innodb_buffer_pool_size = el valor real no debe ser inferior al 80 % del tamaño
   previsto de la base de datos KAV
   innodb_thread_concurrency = 20
   innodb_flush_log_at_trx_commit = 0 (en la mayoría de los casos, el servidor utiliza
   transacciones pequeñas)
   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
```

Se recomienda usar el valor del parámetro `innodb_flush_log_at_trx_commit=0`, debido a que los valores "1" o "2" afectan de modo negativo a la velocidad operativa de MySQL.

Instalación de Kaspersky Security Center (Instalación estándar)

Este procedimiento describe cómo instalar Kaspersky Security Center. Antes de la instalación, debe instalar un sistema de administración de bases de datos.

Instalar Kaspersky Security Center:

1. Bajo una cuenta con privilegios administrativos, ejecute el archivo ejecutable ksc_<número de compilación>_full_<idioma de localización>.exe
2. En la ventana de selección de la aplicación que se abre, haga clic en **Instalar Kaspersky Security Center**.

   Se inicia el Asistente de instalación del Servidor de administración de Kaspersky Security Center.
3. Comenzando con la página de bienvenida, continúe con el Asistente usando el botón **Siguiente**.
4. Si Microsoft.NET Framework no está instalado, instálelo.
5. Acepte los términos del Contrato de licencia y la Política de privacidad.
6. Seleccione el tipo de instalación. Para fines de evaluación, le recomendamos que mantenga el valor **Estándar** predeterminado.
7. Si desea instalar Kaspersky Security Center 14 Web Console en el mismo dispositivo, seleccione la casilla de verificación **Instalar Kaspersky Security Center 14 Web Console**.

   Si desactiva la casilla de verificación, puede instalar más adelante Kaspersky Security Center 14 Web Console por separado en el mismo o en otro dispositivo.
8. Seleccione el tamaño de su red. Para fines de evaluación, le recomendamos que mantenga el valor predeterminado **Menos de 100 dispositivos en la red**.
9. Seleccione el tipo del servidor de la base de datos que instaló antes.
10. Especifique los parámetros de conexión para el servidor de la base de datos que instaló antes.
11. Especifique los parámetros de autenticación para el servidor de la base de datos que instaló antes.
12. Haga clic en el botón **Instalar** para iniciar la instalación.
13. Una vez que la instalación finalice correctamente, elija si desea iniciar la Consola de administración inmediatamente después de cerrar el Asistente.

    Si elige abrir Kaspersky Security Center 14 Web Console, se abrirá la pantalla de inicio de sesión. Después, podrá realizar la configuración inicial del Servidor de administración utilizando el Asistente de inicio rápido.

Puede abrir Kaspersky Security Center 14 Web Console solo si ya está instalado. No puede abrir Kaspersky Security Center 14 Web Console si no la instaló durante la instalación de Kaspersky Security Center o por separado.

14. En la ventana de la Consola de administración que se abre, haga clic en el Servidor de administración instalado.

15. En la ventana del certificado del Servidor de administración que se abre, haga clic en el botón **Sí** para continuar.

El Asistente de inicio rápido del Servidor de administración se inicia si no lo ejecutó en la Consola de administración basada en la web.

Solución de problemas

Si la ventana del certificado del Servidor de administración no se abre y se muestran los errores de conexión, intente lo siguiente:

1. En Windows, abra **Servicios** (**Panel de control** → **Herramientas administrativas** → **Servicios**). Compruebe que se estén ejecutando los servicios del Agente de red de Kaspersky Security Center y del Servidor de administración de Kaspersky Security Center.

2. En Windows, abra el **Visor de eventos** (**Panel de control** → **Herramientas administrativas** → **Visor de eventos**) y luego seleccione **Registros de aplicaciones y servicios** → **Registro de eventos de Kaspersky**. Asegúrese de que el registro no contenga errores y contenga eventos como **Servidor de administración <número de la versión> se está ejecutando**.

Instalación de Kaspersky Security Center 14 Web Console

Esta sección describe cómo instalar el Servidor de Kaspersky Security Center 14 Web Console (también conocido como Kaspersky Security Center 14 Web Console) por separado. Antes de la instalación, debe instalar un sistema de administración de bases de datos y el Servidor de administración de Kaspersky Security Center. Puede instalar Kaspersky Security Center 14 Web Console en el mismo dispositivo donde está instalado Kaspersky Security Center o en uno diferente.

Para instalar Kaspersky Security Center 14 Web Console:

1. En una cuenta con privilegios administrativos, ejecute el archivo ejecutable ksc-web-console-<número de versión>.<número de compilación>.exe.

   Esto inicia el Asistente de instalación.

2. Seleccione un idioma para el Asistente de instalación.

3. En la ventana de bienvenida, haga clic en **Siguiente**.

4. En la ventana **Contrato de licencia**, lea y acepte las condiciones del Contrato de licencia de usuario final. La instalación continúa después de que usted acepte el EULA; si no lo hace, el botón **Siguiente** no estará disponible.

5. En la ventana **Carpeta de destino**, seleccione una carpeta donde Kaspersky Security Center 14 Web Console se instalará (de forma predeterminada, %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Si la carpeta no existe, se crea automáticamente durante la instalación.

   Puede cambiar la carpeta de destino con el botón **Examinar**.

6. En la ventana **Configuración de la conexión de Kaspersky Security Center 14 Web Console**, especifique la siguiente información:

   - La dirección de Kaspersky Security Center 14 Web Console (de forma predeterminada, 127.0.0.1).
   - El puerto que Kaspersky Security Center 14 Web Console utilizará para las conexiones entrantes, es decir, el puerto que da acceso a Kaspersky Security Center 14 Web Console desde un navegador (de forma predeterminada, 8080).

   Le recomendamos que deje la dirección y el número de puerto como están.

   Si lo desea, puede hacer clic en **Probar** para asegurarse de que el puerto seleccionado esté disponible.

   Si desea habilitar el registro de las actividades de Kaspersky Security Center 14 Web Console, seleccione la opción adecuada. Si no selecciona esta opción, los archivos de registro de Kaspersky Security Center 14 Web Console no se crearán.

   > Los certificados en el formato PFX no son compatibles con Kaspersky Security Center 14 Web Console. Para utilizar un certificado de este tipo, primero debe convertirlo al formato PEM compatible, utilizando una utilidad multiplataforma basada en OpenSSL, como OpenSSL para Windows.

7. En la ventana **Configuración de la cuenta**, especifique los nombres de la cuenta y contraseñas.

   Le recomendamos que utilice cuentas predeterminadas.

8. En la ventana **Certificado cliente**, seleccione una de las siguientes opciones:

   - **Generar un certificado nuevo**. Se recomienda esta opción si no tiene un certificado de navegador.
   - **Seleccione existente**. Puede seleccionar esta opción si ya tiene un certificado de navegador; en este caso, especifique su ruta.

9. En la ventana **Servidores de administración de confianza**, asegúrese que su Servidor de administración esté en la lista y haga clic en **Siguiente** para ir a la última ventana del instalador.

10. En la ventana **Identity and Access Manager DESACTIVADO**, especifique si desea instalar Identity and Access Manager (también denominado IAM). Si decide instalar Identity and Access Manager, especifique los siguientes números de puerto:

    - **Puerto de administrador KAS**. De forma predeterminada, se utiliza el puerto 4445 para recibir la configuración de Kaspersky Security Center 14 Web Console para el puerto de punto final de autorización OAuth2.0.
    - **Puerto de Facade**. De forma predeterminada, se utiliza el puerto 2444 para la configuración de Identity and Access Manager.
    - **Puerto de interacción Facade**. De forma predeterminada, el puerto 2445 se utiliza para la conexión de Kaspersky OSMP KAS Service a Kaspersky OSMP Facade Service.

    Si lo desea, puede cambiar los números de puerto predeterminados. No podrá cambiarlos en el futuro a través de Kaspersky Security Center 14 Web Console.

11. En la última ventana en el instalador, haga clic en **Instalar** para comenzar la instalación.

Una vez que la instalación se complete con éxito, aparece un acceso directo en el escritorio y puede iniciar sesión en Kaspersky Security Center 14 Web Console.

El Asistente de inicio rápido del Servidor de administración se inicia si no lo ejecutó en la Consola de administración basada en la Consola de administración de Microsoft.

Solución de problemas

Si Kaspersky Security Center 14 Web Console no aparece en su navegador en la URL que introdujo, intente lo siguiente:

1. Compruebe que haya especificado el nombre de host o la dirección IP correctos del dispositivo en el que está instalada la Kaspersky Security Center 14 Web Console.
2. Compruebe que el dispositivo que desea operar tenga acceso al dispositivo en el que está instalada Kaspersky Security Center 14 Web Console.
3. Verifique que la configuración del firewall en el dispositivo en el que está instalado Kaspersky Security Center 14 Web Console permita conexiones entrantes a través del puerto 8080 y para la aplicación node.exe.
4. En Windows, abra **Servicios**. Compruebe que el servicio de la Kaspersky Security Center 14 Web Console se esté ejecutando.
5. Compruebe que puede acceder a Kaspersky Security Center mediante la Consola de administración.
6. En Windows, abra el **Visor del evento**, y luego seleccione **Aplicaciones y registros de servicios** → **Registro de eventos de Kaspersky**. Asegúrese que el registro no contenga errores.

Instalación de Kaspersky Security Center 14 Web Console en plataformas Linux

En esta sección se describe la instalación del servidor Kaspersky Security Center 14 Web Console (también conocido como Kaspersky Security Center 14 Web Console) en dispositivos con sistema operativo Linux (consulte la lista de distribuciones de Linux compatibles).

Instalación de Kaspersky Security Center 14 Web Console en plataformas Linux

En esta sección se describe cómo instalar el servidor Kaspersky Security Center 14 Web Console (también denominado Kaspersky Security Center 14 Web Console) en dispositivos con sistema operativo Linux. Antes de la instalación, debe instalar un sistema de administración de bases de datos y el Servidor de administración de Kaspersky Security Center.

Utilice el archivo de instalación — ksc-web-console-[version_number] .deb o ksc-web-console-[version_number].x86_64.rpm — que corresponde a la distribución de Linux instalada en su dispositivo. El archivo de instalación debe descargarse del sitio web de Kaspersky.

Para instalar Kaspersky Security Center 14 Web Console:

1. Asegúrese de que el dispositivo en el que desea instalar Kaspersky Security Center 14 Web Console esté ejecutando una de las distribuciones de Linux compatibles.

2. Lea el Contrato de licencia de usuario final (EULA) que descargó junto con el archivo de instalación. Si no acepta los términos del Contrato de licencia, no instale la aplicación.

3. Cree un archivo de respuesta que contenga parámetros para conectar Kaspersky Security Center 14 Web Console al Servidor de administración. Nombre a este archivo ksc-web-console-setup.json y colóquelo en el siguiente directorio: /etc/ksc-web-console-setup.json.

   Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

   ```
   {
     "address": "127.0.0.1",
     "port": 8080,
     “trusted”:
   “127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server”,
     "acceptEula": true
   }
   ```

   Cuando instala Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto que no sea 8080, ya que el sistema operativo usa el puerto 8080.

   Kaspersky Security Center 14 Web Console no se puede actualizar usando el mismo archivo de instalación .rpm. Si desea cambiar la configuración en un archivo de respuesta y utilizar este archivo para volver a instalar la aplicación, primero debe eliminar la aplicación y luego volver a instalarla con el nuevo archivo de respuesta.

4. Con una cuenta con privilegios root, use la línea de comandos para ejecutar el archivo de instalación con la extensión .deb o .rpm, dependiendo de su distribución de Linux.

   - Para instalar o actualizar Kaspersky Security Center 14 Web Console desde un archivo .deb, ejecute el siguiente comando:
     ```
     $ sudo dpkg -i ksc-web-console-[version_number].deb
     ```
   - Para instalar Kaspersky Security Center 14 Web Console desde un archivo .rpm, ejecute el siguiente comando:
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[version_number].x86_64.rpm
     ```
   - Para actualizar desde una versión anterior de Kaspersky Security Center Web Console, ejecute uno de los siguientes comandos:
     - Para dispositivos que ejecutan un sistema operativo basado en RPM:
       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-[version_number].x86_64.rpm
       ```
     - Para dispositivos que ejecutan un sistema operativo basado en Debian:
       ```
       $ sudo dpkg -i ksc-web-console-[version_number].x86_64.deb
       ```

   Se empezará a desempaquetar el archivo de instalación. Espere hasta que finalice la instalación. Kaspersky Security Center 14 Web Console se instala en el siguiente directorio: /var/opt/kaspersky/ksc-web-console.

Cuando finalice la instalación, puede usar su navegador para abrir e iniciar sesión en Kaspersky Security Center 14 Web Console.

Parámetros de instalación de Kaspersky Security Center 14 Web Console

Para instalar el servidor Kaspersky Security Center 14 Web Console en dispositivos que ejecutan Linux, debe crear un archivo de respuesta en formato JSON, que contenga parámetros para conectar Kaspersky Security Center 14 Web Console al Servidor de administración.

Ejemplo de un archivo de respuesta que contiene el conjunto mínimo de parámetros, y la dirección y el puerto predeterminados:

```
{
  "address": "127.0.0.1",
  "port": 8080,
  “defaultLangId”: 1049,
  “enableLog”: false,
  “trusted”: “127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server”,
  “acceptEula”: true,
  “certPath”: “/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer”,
  “webConsoleAccount”: “Group1:User1”,
  “managementServiceAccount”: “Group2:User3”
}
```

Cuando instala Kaspersky Security Center 14 Web Console en el sistema operativo Linux ALT, debe especificar un número de puerto que no sea 8080, ya que el sistema operativo usa el puerto 8080.

En la siguiente tabla se describen los parámetros que se pueden especificar en un archivo de respuesta.

Parámetros para instalar Kaspersky Security Center 14 Web Console en dispositivos que ejecutan Linux

Parámetro	Descripción	Valores disponibles
`dirección`	Dirección del servidor Kaspersky Security Center 14 Web Console (obligatorio)	Valor de cadena.
`puerto`	Número de puerto que utiliza el servidor Kaspersky Security Center 14 Web Console para conectarse al Servidor de administración (obligatorio)	Valor numérico.
`defaultLangId`	Idioma de la interfaz de usuario (de forma predeterminada, `1033`)	Código numérico del idioma: • Alemán: `1031` • Inglés: `1033` • Español: `3082` • Español (México): `2058` • Francés: `1036`

		• Japonés: `1041` • Kazajo: `1087` • Polaco: `1045` • Portugués (Brasil): `1046` • Ruso: `1049` • Turco: `1055` • Chino simplificado: `4` • Chino tradicional: `31748` Si no se especifica ningún valor, se usa el idioma inglés.
`enableLog`	Activar o no activar el registro de actividad de Kaspersky Security Center 14 Web Console	Valor booleano: • `true` — el registro está activado (seleccionado de for predeterminada) • `false` — el registro está desactivado

`de confianza`	Lista de Servidores de administración de confianza con derecho a conectarse a Kaspersky Security Center 14 Web Console (obligatorio). Cada Servidor de administración debe estar definido con los siguientes parámetros:
	• Dirección de Servidor de administración
	• Puerto OpenAPI que utiliza Kaspersky Security Center 14 Web Console para conectarse al Servidor de administración (por defecto, 13299)
		Valor de cadena con el siguiente formato:
		`"server address|port|certificate path|server`
		Ejemplo:
		`"X.X.X.X|13299|/cert/server-1.cer|Server 1||Y.Y.Y.Y|13299|/cert/server-2.cer|Server 2`

	• Ruta al certificado del Servidor de administración • Nombre del Servidor de administración que se mostrará en la ventana de inicio de sesión Los parámetros se separan con barras verticales. Si se especifican varios Servidores de administración, sepárelos con dos barras verticales (plecas).	
`acceptEula`	Aceptar o no aceptar las condiciones del Contrato de licencia de usuario final (EULA) El archivo que contiene los términos del EULA se descarga junto con el archivo de instalación (obligatorio).	Valor booleano: • `true`: He leído, y entiendo y acepto completamente l Contrato de licencia de usuario final. • `false:` no acepto los términos del Contrato de licen (seleccionado por defecto).
`certDomain`	Si desea generar un nuevo certificado, use este parámetro para especificar el nombre de dominio para el que se generará el nuevo certificado.	Valor de cadena.
`certPath`	Si desea usar un certificado existente, use este parámetro para especificar la ruta al archivo del certificado	Valor de cadena. Especificar la ruta “`/var/opt/kaspersky/klnagent_srv/1093/cert/k` para utilizar el certificado existente. Para un certificado p especifique la ruta donde se almacena este certificado p
`keyPath`	Si desea usar un	Valor de cadena.

	certificado existente, use este parámetro para especificar la ruta al archivo clave.	
`webConsoleAccount`	Nombre de la cuenta sin privilegios para trabajar con Kaspersky Security Center 14 Web Console	Valor de cadena con el siguiente formato: `"nombre del grupo:nombre de usuario"`. Ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, se crea una nueva cuenta
`managementServiceAccount`	Nombre de la cuenta con privilegios para trabajar con Kaspersky Security Center 14 Web Console	Valor de cadena con el siguiente formato: `"nombre del grupo:nombre de usuario"`. Ejemplo: `"Grupo1:Usuario1"`. Si no se especifica ningún valor, se crea una nueva cuenta

Actualización de Kaspersky Security Center Web Console

Si desea utilizar una versión más reciente de Kaspersky Security Center Web Console sin eliminar la instancia instalada actualmente, puede utilizar el procedimiento de actualización estándar que se proporciona en el instalador de Kaspersky Security Center Web Console.

Para actualizar Kaspersky Security Center Web Console, siga estos pasos:

1. En una cuenta con derechos de administrador, ejecute el archivo ejecutable ksc-web-console-<número de compilación>.exe, donde <número de compilación> se refiere a una compilación de Kaspersky Security Center Web Console cuyo número es mayor que el de su instancia instalada actualmente.

2. En la ventana del Asistente de instalación que se abre, seleccione un idioma y luego haga clic en **Aceptar**.

3. En la ventana de bienvenida, seleccione la opción **Actualizar** y luego haga clic en **Siguiente**.

4. En la ventana **Contrato de licencia**, lea y acepte las condiciones del Contrato de licencia de usuario final. La instalación continúa después de que acepte el EULA; si no lo hace, el botón **Siguiente** no estará disponible.

5. Siga los pasos del Asistente de instalación hasta que finalice. Mientras avance, también podrá modificar la configuración de Kaspersky Security Center Web Console que especificó durante la instalación anterior. Cuando llegue al paso **Listo para modificar Kaspersky Security Center 14 Web Console**, haga clic en el botón **Actualizar**. Espere a que se aplique la nueva configuración y en el siguiente paso del Asistente de instalación, haga clic en **Finalizar**. También puede hacer clic en el enlace **Iniciar Kaspersky Security Center 14 Web Console en su navegador** para iniciar de inmediato la instancia actualizada de Kaspersky Security Center Web Console.

   La modificación de la configuración de Kaspersky Security Center Web Console durante la actualización solo está disponible en Kaspersky Security Center Web Console versión 12.2 o superior.

   Su instancia de Kaspersky Security Center Web Console está actualizada.

Certificados para trabajar con Kaspersky Security Center 14 Web Console:

La sección describe cómo emitir y reemplazar certificados para Kaspersky Security Center 14 Web Console y cómo renovar un certificado para el Servidor de administración si el Servidor interactúa con Kaspersky Security Center 14 Web Console.

Reemplazo del certificado para Kaspersky Security Center Web Console

La mayoría de los navegadores imponen un límite en el plazo de validez de un certificado. Para estar dentro de este límite, el plazo de validez del certificado de Kaspersky Security Center Web Console se limita a 397 días. Puede reemplazar un certificado existente recibido de una autoridad de certificación (CA) al emitir un nuevo certificado autofirmado de forma manual. Como alternativa, puede volver a emitir su certificado caducado de Kaspersky Security Center Web Console.

Si ya usa un certificado autofirmado, también puede volver a emitirlo al actualizar Kaspersky Security Center Web Console mediante el procedimiento estándar en el instalador (opción **Actualizar**).

Para emitir un nuevo certificado cuando instale Kaspersky Security Center Web Console por primera vez, siga estos pasos:

1. Ejecute la instalación de rutina de Kaspersky Security Center Web Console.
2. Cuando llegue al paso **Certificado de cliente** del Asistente de instalación, seleccione la opción **Generar un certificado nuevo** y luego haga clic en el botón **Siguiente**.
3. Continúe con los pasos restantes del Asistente de instalación hasta que finalice.

   Se emite un nuevo certificado para Kaspersky Security Center Web Console con un período de validez de 397 días.

Para volver a emitir el certificado caducado de Kaspersky Security Center Web Console, siga estos pasos:

1. Bajo una cuenta con derechos de administrador, ejecute el archivo de instalación ksc-web-console-<número de versión>.<número de compilación>.exe.
2. En la ventana del Asistente de instalación que se abre, seleccione un idioma y luego haga clic en **Aceptar**.
3. En la ventana de bienvenida, seleccione la opción **Volver a emitir certificado** y luego haga clic en **Siguiente**.
4. En el siguiente paso, espere hasta que se complete la reconfiguración de Kaspersky Security Center Web Console y luego haga clic en **Finalizar**.

   El certificado de Kaspersky Security Center Web Console se vuelve a emitir por otro período de validez de 397 días.

Si usa Identity and Access Manager, también debe volver a emitir todos los certificados TLS para los puertos que utiliza Identity and Access Manager. Kaspersky Security Center Web Console muestra una notificación cuando caduca un certificado. Debe seguir las instrucciones de notificación.

Reemplazar certificado para Kaspersky Security Center 14 Web Console

De forma predeterminada, cuando instala el Servidor de Kaspersky Security Center 14 Web Console, se genera automáticamente un certificado de navegador para la aplicación. Puede reemplazar el certificado generado automáticamente por uno personalizado.

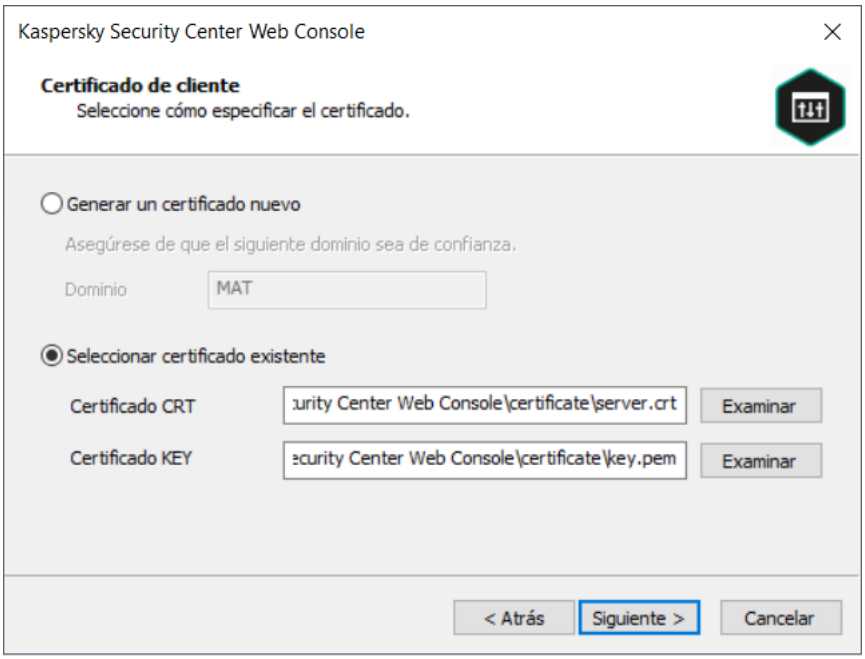
Para reemplazar el certificado de Kaspersky Security Center 14 Web Console Server por uno personalizado:

1. En el dispositivo donde está instalada Kaspersky Security Center 14 Web Console Server, ejecute el archivo ejecutable ksc-web-console-<número de versión>.<número de compilación>.exe en una cuenta con privilegios administrativos.

   Esto inicia el Asistente de instalación.

2. En la primera página del Asistente, seleccione la opción **Actualizar**.

3. En la página **Certificado de cliente** página, seleccione la opción **Seleccionar certificado existente** y especifique la ruta al certificado personalizado.



Especificar el certificado cliente

4. En la última página del Asistente, haga clic en **Modificar** para aplicar la nueva configuración.

5. Después de que la reconfiguración de la aplicación se complete correctamente, haga clic en el botón **Terminar**.

Kaspersky Security Center 14 Web Console funciona con el certificado especificado.

Especificación de certificados para Servidores de administración de confianza

El certificado del Servidor de administración existente se reemplaza automáticamente por uno nuevo antes de la fecha de vencimiento del certificado. También puede reemplazar el certificado existente del Servidor de administración por uno personalizado. Cada vez que se cambia el certificado, el nuevo certificado debe especificarse en la configuración de Kaspersky Security Center 14 Web Console. De lo contrario, Kaspersky Security Center 14 Web Console no podrá conectarse al Servidor de administración.

Si Kaspersky Security Center 14 Web Console y el Servidor de administración están instalados en el mismo dispositivo, Kaspersky Security Center 14 Web Console recibe el nuevo certificado automáticamente. Si Kaspersky Security Center 14 Web Console está instalado en un dispositivo diferente, debe especificar la ruta de acceso local al nuevo certificado del Servidor de administración.

Para especificar un nuevo certificado para el Servidor de administración:

1. En el dispositivo donde está instalado el Servidor de administración, copie el archivo de certificado a, por ejemplo, un dispositivo de almacenamiento masivo.

   De forma predeterminada, el archivo del certificado se almacena en la siguiente carpeta:

   - Para Windows: ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - Para Linux: /var/opt/kaspersky/klnagent_srv/1093/cert/

2. En el dispositivo donde está instalada Kaspersky Security Center 14 Web Console, coloque el archivo de certificado en una carpeta local.

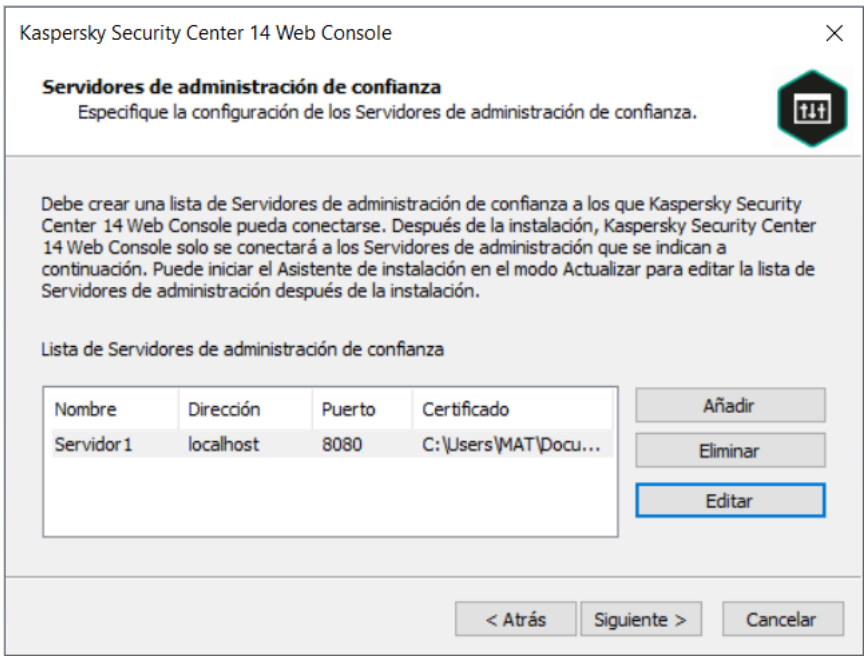
3. Ejecute el archivo de instalación ksc-web-console-<número de versión>.<número de compilación>.exe en una cuenta con privilegios administrativos.

   Esto inicia el Asistente de instalación.

4. En la primera página del Asistente, seleccione la opción **Actualizar**.

5. En la página **Tipo de modificación**, seleccione la opción **Editar configuración de conexión**.

6. En la página **Servidores de administración de confianza**, seleccione el Servidor de administración requerido y haga clic en el botón **Editar**.



Especificar los Servidores de administración de confianza

7. En la página que se abre, haga clic en **Examinar** y especifique la ruta al nuevo archivo de certificado.

8. En la última página del Asistente, haga clic en **Modificar** para aplicar la nueva configuración.

9. Después de que la reconfiguración de la aplicación se complete correctamente, haga clic en el botón **Terminar**.

10. Inicie sesión en Kaspersky Security Center 14 Web Console.

Kaspersky Security Center 14 Web Console funciona con el certificado especificado.

Conversión de un certificado PFX al formato PEM

Para utilizar un certificado PFX en Kaspersky Security Center 14 Web Console, primero debe convertirlo al formato PEM mediante cualquier utilidad multiplataforma conveniente basada en OpenSSL.

Para convertir un certificado PFX al formato PEM en el sistema operativo Windows:

1. En una utilidad multiplataforma basada en OpenSSL, ejecute los siguientes comandos:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys -out server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes -out key.pem
   ```

   Como resultado, obtiene una clave pública como archivo .crt y una clave privada como archivo .pem protegido por contraseña.

2. Asegúrese de que los archivos .crt y .pem se generen en la misma carpeta donde se almacena el archivo .pfx.

3. Si el archivo .crt o .pem contiene los atributos bag, elimine estos atributos utilizando cualquier editor de texto conveniente y guarde el archivo.

4. Reinicie el servicio de Windows.

5. Kaspersky Security Center 14 Web Console no es compatible con certificados protegidos con contraseña. Por tanto, ejecute el siguiente comando en una utilidad multiplataforma basada en OpenSSL para eliminar una contraseña del archivo .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > No use el mismo nombre para los archivos .pem de entrada y salida.

   Como resultado, el nuevo archivo .pem se descifra. No tiene que introducir una contraseña para usarlo.

Los archivos .crt y .pen están listos para usarse, por lo que puede especificarlos en el instalador de Kaspersky Security Center 14 Web Console.

Para convertir un certificado PFX al formato PEM en el sistema operativo Linux:

1. En una utilidad multiplataforma basada en OpenSSL, ejecute los siguientes comandos:

   ```
   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. Asegúrese de que el archivo de certificado y la clave privada se generen en el mismo directorio donde está almacenado el archivo .pfx.

3. Kaspersky Security Center 14 Web Console no es compatible con certificados protegidos con contraseña. Por tanto, ejecute el siguiente comando en una utilidad multiplataforma basada en OpenSSL para eliminar una contraseña del archivo .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

No use el mismo nombre para los archivos .pem de entrada y salida.

Como resultado, el nuevo archivo .pem se descifra. No tiene que introducir una contraseña para usarlo.

Los archivos .crt y .pen están listos para usarse, por lo que puede especificarlos en el instalador de Kaspersky Security Center 14 Web Console.

Migración a Kaspersky Security Center Cloud Console

Puede realizar la migración de Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console. Después de eso, obtiene acceso al Servidor de administración y al sistema de administración de bases de datos (DBMS), que están alojados en la infraestructura de Kaspersky. No necesita un servidor físico ni un DBMS; el mantenimiento de ambos está a cargo de los expertos de Kaspersky.

Puede migrar sus dispositivos administrados con un sistema operativo Windows, Linux o macOS bajo el control de Kaspersky Security Center Cloud Console. Si su red incluye una jerarquía de Servidores de administración, puede guardarla en Kaspersky Security Center Cloud Console. Además, puedes transferir lo siguiente:

- Tareas y políticas de aplicaciones administradas
- Tareas globales
- Selecciones de dispositivos personalizados
- Estructura del grupo de administración y dispositivos incluidos
- Las etiquetas asignadas a los dispositivos de migración

Después de finalizar la migración, puede administrar los dispositivos mediante Kaspersky Security Center Cloud Console. Al mismo tiempo, los objetos transferidos se conservan y el Agente de red se reinstala en todos los dispositivos administrados.

Para obtener información sobre cómo realizar la migración y una lista de los requisitos previos, consulte la *Ayuda de Kaspersky Security Center Cloud Console*.

Iniciar sesión en Kaspersky Security Center 14 Web Console y cerrar sesión

Puede iniciar sesión en Kaspersky Security Center 14 Web Console después de instalar el Servidor de administración y el Servidor de Web Console. Debe conocer la dirección web del Servidor de administración y el número de puerto especificado durante la instalación (de forma predeterminada, el puerto es 8080). En su navegador, JavaScript debe estar habilitado.

Para iniciar sesión en Kaspersky Security Center 14 Web Console:

1. En su navegador, vaya a <dirección web del Servidor de administración>:<Número de puerto>.

   Se muestra la página de inicio de sesión.

2. Si agregó varios servidores de confianza, en la lista Servidores de administración, seleccione el Servidor de administración al que desea conectarse.

   Si solo agregó un Servidor de administración, solo se mostrarán los campos Inicio de sesión y Contraseña.

3. Inicie sesión con el nombre de usuario y la contraseña del administrador local.

   Si el Servidor de administración no responde o si ha introducido credenciales incorrectas, se mostrará un mensaje de error.

4. Después de iniciar sesión, se muestra el panel de control, que contiene el idioma y el tema que usó la última vez.

Puede navegar por Kaspersky Security Center 14 Web Console y usarlo para trabajar con Kaspersky Security Center.

Para cerrar sesión en Kaspersky Security Center 14 Web Console:

1. Haga clic en su nombre de usuario en la esquina superior derecha de la pantalla.

2. En el menú desplegable, seleccione **Salir**.

Kaspersky Security Center 14 Web Console se cierra y se muestra la página de inicio de sesión.

Identity and Access Manager en Kaspersky Security Center 14 Web Console

Esta sección proporciona información sobre Identity and Access Manager (también conocido como IAM).

Acerca de Identity and Access Manager

Identity and Access Manager (también conocido como IAM) es un componente de Kaspersky Security Center 14 Web Console que le permite utilizar un inicio de sesión único (SSO) entre Kaspersky Security Center 14 Web Console y la interfaz web de Kaspersky Industrial CyberSecurity for Networks. IAM utiliza el protocolo OAuth 2.0 para garantizar la autorización de Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center 14 Web Console.

En este caso, Kaspersky Industrial CyberSecurity for Networks, al que se accede a través de Kaspersky Security Center 14 Web Console, lo denomina *servidor de recursos*, y Kaspersky Security Center 14 Web Console y la interfaz web de Kaspersky Industrial CyberSecurity for Networks lo denomina como *clientes OAuth 2.0*. Un servidor de recursos es un programa que trabaja con varios usuarios y requiere autorización. El cliente utiliza un *token* para la autorización en el servidor de recursos. Un token es una secuencia única de bytes. Cuando caduca un token, se vuelve a emitir automáticamente. IAM actúa como un único servidor de autorización para múltiples clientes OAuth 2.0.

Puede instalar IAM al instalar Kaspersky Security Center 14 Web Console. Puede habilitarlo en cualquier otro momento en la configuración de Kaspersky Security Center 14 Web Console. Si se instala un servidor de Kaspersky Industrial CyberSecurity o una interfaz web de Kaspersky Industrial CyberSecurity en un dispositivo administrado por el mismo Servidor de administración, IAM detecta este programa y se muestra una notificación en Kaspersky Security Center 14 Web Console que informa de esto. Puede registrar Kaspersky Industrial CyberSecurity for Networks y utilizar SSO luego tanto para Kaspersky Security Center 14 Web Console como para la interfaz web de Kaspersky Industrial CyberSecurity for Networks.

Si cierra la sesión de Kaspersky Security Center 14 Web Console, finalizará su sesión en la interfaz web de Kaspersky Industrial CyberSecurity for Networks y tendrá que volver a iniciar sesión en Kaspersky Security Center 14 Web Console.

Activación de Identity and Access Manager: escenario

Requisitos previos

Antes de empezar, asegúrese de que tiene acceso a Kaspersky Industrial CyberSecurity for Networks versión 3.1 o superior.

Etapas

La habilitación del Identity and Access Manager (también denominado IAM) se realiza por etapas:

1. **Comprobación de los puertos necesarios**

   Asegúrese de que los puertos 3333, 4004 y 4444 están abiertos en el dispositivo donde está instalado Kaspersky Security Center 14 Web Console. Estos puertos son necesarios para utilizar OAuth 2.0. Si lo desea, puede cambiar los números de puerto predeterminados en la ventana de configuración de Kaspersky Security Center 14 Web Console.

   Además de los puertos 3333, 4004 y 4444, Kaspersky Security Center 14 Web Console también utiliza los puertos 4445, 2444 y 2445 para diversos fines.

2. **Instalación del Identity and Access Manager**

   Durante la instalación de Kaspersky Security Center 14 Web Console, especifique que desea instalar Identity and Access Manager. Si no lo ha hecho, ejecute de nuevo el Asistente de instalación de Kaspersky Security Center 14 Web Console.

3. **Configuración del Identity and Access Manager**

   En la ventana de configuración de Kaspersky Security Center 14 Web Console, asegúrese de que el botón de alternancia **Identity and Access Manager DESACTIVADO** esté activado. También especifique el nombre DNS del dispositivo donde está instalado Kaspersky Security Center 14 Web Console: las aplicaciones cliente se conectarán a este dispositivo.

4. **Especificación de la configuración de los tokens**

   En la ventana de configuración de Kaspersky Security Center 14 Web Console, especifique la duración de los tokens y el tiempo de espera de autorización que utilizará Identity and Access Manager. Puede utilizar los valores predeterminados, o puede especificar sus propios valores según sus necesidades.

5. **Concesión de certificados**

   Si prefiere utilizar los certificados generados por el Servidor de administración, en la ventana de configuración de Kaspersky Security Center 14 Web Console, descargue los certificados raíz para los puertos utilizados por IAM y distribúyalos a las estaciones de trabajo de los usuarios de Kaspersky Security Center 14 Web Console. De lo contrario, los navegadores de los usuarios mostrarán mensajes de error al intentar conectarse a Kaspersky Security Center 14 Web Console.

6. **Registro de los servidores de Kaspersky Industrial CyberSecurity for Networks y las interfaces web de Kaspersky Industrial CyberSecurity for Networks**

   Cuando se instala IAM, Kaspersky Security Center 14 Web Console muestra un mensaje que dice que se espera el registro de un servidor (o varios servidores) de Industrial CyberSecurity for Networks y una o más interfaces web de Kaspersky Industrial CyberSecurity for Networks. Haga clic en este mensaje para registrar su servidor (o varios servidores) e interfaz web (o varias interfaces web) de Kaspersky Industrial CyberSecurity for Networks.

Resultados

Después de completar este escenario, podrá utilizar SSO e IAM para Kaspersky Industrial CyberSecurity for Networks y Kaspersky Security Center 14 Web Console.

Configuración de Identity and Access Manager en Kaspersky Security Center 14 Web Console

Para configurar Identity and Access Manager según sus necesidades:

1. En Kaspersky Security Center 14 Web Console, vaya a la sección **Configuración de la consola → Integración**.
2. En la sección **Instalar Identity and Access Manager**, asegúrese de que Identity and Access Manager esté activado.
3. Haga clic en el enlace **Configuración** en la línea **Nombre de la red del dispositivo con Identity and Access Manager**.
4. Especifique el nombre DNS del dispositivo en el que se ha instalado Identity and Access Manager. Las aplicaciones cliente se conectarán a este dispositivo.
5. Si lo desea, cambie la configuración predeterminada de los tokens, la configuración del certificado y los números de puerto al hacer clic en el enlace **Configuración** en el grupo de configuración correspondiente.

Identity and Access Manager está activado y funciona según sus necesidades.

Registro de la interfaz web de Kaspersky Industrial CyberSecurity for Networks en Kaspersky Security Center 14 Web Console

Para comenzar a trabajar con la interfaz web de Kaspersky Industrial CyberSecurity for Networks a través de Kaspersky Security Center 14 Web Console, primero debe registrarla en Kaspersky Security Center 14 Web Console.

Para registrar la interfaz web de Kaspersky Industrial CyberSecurity for Networks:

1. Asegúrese de que se haga lo siguiente:
   - Ha descargado e instalado el complemento web de Kaspersky Industrial CyberSecurity for Networks. Sin embargo, puede hacerlo más adelante mientras espera que el servidor de Kaspersky Industrial CyberSecurity for Networks se sincronice con el Servidor de administración.
   - Ha completado el Escenario de preparación para el uso de la tecnología de inicio de sesión único (SSO).
   - La configuración necesaria en la interfaz web de Kaspersky Industrial CyberSecurity for Networks se especifica en la página de Kaspersky Security Center. Para obtener más información, consulte la Ayuda en línea de Kaspersky Industrial CyberSecurity for Networks.
   - Ha iniciado sesión en Kaspersky Security Center 14 Web Console con una cuenta de administrador.
   - IAM esté configurado.
2. Mueva el dispositivo donde está instalado el servidor de Kaspersky Industrial CyberSecurity for Networks del grupo de dispositivos no asignados al grupo de dispositivos administrados:
   a. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DISPOSITIVOS NO ASIGNADOS**.

b. Seleccione la casilla de verificación junto al dispositivo donde está instalado el servidor de Kaspersky Industrial CyberSecurity for Networks.

c. Haga clic en el botón **Mover a un grupo**.

d. En la jerarquía de grupos de administración, seleccione la casilla de verificación junto al grupo de dispositivos administrados.

e. Haga clic en el botón **Mover**.

3. Vaya a las propiedades del dispositivo donde está instalado el servidor de Kaspersky Industrial CyberSecurity for Networks.

4. En la página de propiedades del dispositivo, en la sección **General**, seleccione la opción **No desconectar del Servidor de administración** y, a continuación, haga clic en el botón **Guardar**.

5. En la página de propiedades del dispositivo, seleccione la sección **Aplicaciones**.

6. En la sección **Aplicaciones**, seleccione Agente de red de Kaspersky.

7. Si el estado actual de la aplicación es *Detenido*, espere hasta que cambie a *En ejecución*.

   Esto puede tardar hasta 15 minutos. Si aún no ha instalado el complemento web de Kaspersky Industrial CyberSecurity for Networks, puede hacerlo ahora, mientras espera.

8. En el menú principal, vaya a la sección **Configuración de la consola → Integración**.

   En el campo **Solicitudes de registro**, se muestra una solicitud pendiente.

9. Haga clic en el enlace **Configuración** en el campo **Solicitudes de registro**.

10. En la lista de clientes registrados que se abre, seleccione la casilla de verificación junto al nombre del servidor Kaspersky Industrial CyberSecurity for Networks, que tiene el estado *Pendiente* y, a continuación, haga clic en el botón **Aprobar**.

    Si no desea registrar el servidor de Kaspersky Industrial CyberSecurity for Networks, puede hacer clic en el botón Rechazar y volver a esta lista más adelante.

    Después de hacer clic en el botón **Aprobar**, el estado cambia a *Aprobado* y luego a *Listo*. Si el estado no cambia, puede hacer clic en el botón Actualizar.

11. Cierre la lista de clientes registrados y asegúrese de que el valor en el campo **Clientes registrados** haya aumentado.

12. Para añadir el widget de Kaspersky Industrial CyberSecurity for Networks en el panel de control:

    a. **SUPERVISIÓN E INFORMES → PANEL**.

    b. En el panel de control, haga clic en el botón **Añadir o restaurar un widget web**.

    c. En el menú del widget que se abre, seleccione **Otro**.

    d. Seleccione el widget de Kaspersky Industrial CyberSecurity for Networks.

    Ahora puede pasar a la interfaz web de Kaspersky Industrial CyberSecurity for Networks mediante el enlace del widget.

Después de completar el procedimiento de registro, un nuevo botón, **Kaspersky Security Center**, aparece en la página de inicio de sesión de la interfaz web de Kaspersky Industrial CyberSecurity for Networks. Puede hacer clic en este botón para iniciar sesión en la interfaz web de Kaspersky Industrial CyberSecurity for Networks con sus credenciales de Kaspersky Security Center.

Duración de los tokens y tiempo de espera de la autorización para Identity and Access Manager

Al configurar el Identity and Access Manager (también conocido como IAM), debe especificar los ajustes para la duración del token y el tiempo de espera de la autorización. La configuración predeterminada está diseñada para reflejar tanto las normas de seguridad como la carga del servidor. Sin embargo, puede cambiar estos ajustes de acuerdo con las políticas de su organización.

IAM vuelve a emitir automáticamente un token cuando está a punto de caducar.

La siguiente tabla muestra la configuración predeterminada de la vida útil de los tokens.

Configuración de la vida útil de los tokens

Token	Duración predeterminada (en segundos)	Descripción
Token de identidad (id_token)	86400	Token de identidad utilizado por el cliente OAuth 2.0 (es decir, Kaspersky Security Center 14 Web Console o Kaspersky Industrial CyberSecurity Console). IAM envía al cliente el token de identificación que contiene información sobre el usuario (es decir, el perfil de usuario).
Token de acceso (access_token)	86400	Token de acceso utilizado por el cliente OAuth 2.0 para acceder al servidor de recursos en nombre del propietario del recurso identificado por IAM.
Token de actualización (refresh_token)	172800	El cliente OAuth 2.0 utiliza este token para volver a emitir el token de identidad y el token de acceso.

La siguiente tabla muestra los tiempos de espera para auth_code y login_consent_request.

Configuración del tiempo de espera de la autorización

Configuración	Tiempo de espera predeterminado (en segundos)	Descripción
Código de autorización (auth_code)	3600	Tiempo de espera para intercambiar el código por el token. El cliente OAuth 2.0 envía este código al servidor de recursos y obtiene a cambio el token de acceso.
Tiempo de espera de la solicitud de consentimiento de inicio de sesión (login_consent_request)	3600	Tiempo de espera para delegar los derechos del usuario al cliente OAuth 2.0.

Para más información sobre los tokens, consulte el sitio web de OAuth.

Descarga y distribución de los certificados IAM

De forma predeterminada, el Identity and Access Manager utiliza los certificados generados por el Servidor de administración para conceder a los navegadores el acceso a Kaspersky Security Center 14 Web Console. Sin embargo, si lo desea, puede utilizar certificados personalizados. Sea cual sea el certificado que utilice, debe asegurarse de que todas las estaciones de trabajo desde las que los usuarios de Kaspersky Security Center 14 Web Console accedan a Kaspersky Security Center 14 Web Console confíen en este certificado.

Para descargar y distribuir certificados:

1. En Kaspersky Security Center 14 Web Console, vaya a la sección **Configuración de la consola** → **Integración**.
2. Para cada certificado, haga clic en el enlace **Configuración** bajo el grupo de configuración correspondiente y, a continuación, realice una de las siguientes acciones:
   - Si desea utilizar el certificado que el Servidor de administración generó durante la instalación de Kaspersky Security Center 14 Web Console:
     1. Seleccione **Certificado generado por el Servidor de administración en la ventana de propiedades del certificado** que se abre.
     2. Haga clic en el botón **Descargar** para descargar el certificado.
     3. Distribuya el certificado descargado a todas las estaciones de trabajo desde las que los usuarios de Kaspersky Security Center 14 Web Console acceden a Kaspersky Security Center 14 Web Console.
   - Si tiene un certificado que quiere utilizar:
     1. Seleccione **Certificado TLS personalizado** en la ventana de propiedades del certificado que se abre.
     2. Seleccione el archivo del certificado y la clave privada.
     3. Haga clic en el botón **Aceptar**.
     4. Distribuya el certificado a todas las estaciones de trabajo desde las que los usuarios acceden a Kaspersky Security Center 14 Web Console o Kaspersky Industrial CyberSecurity Console.

Los certificados otorgan a los usuarios acceso a Kaspersky Security Center 14 Web Console y a Kaspersky Industrial CyberSecurity Console.

Debe volver a emitir todos los certificados a tiempo. Los certificados generados por el Servidor de administración se deben volver a generar manualmente. Los certificados generados por el instalador de Kaspersky Security Center 14 Web Console se deben volver a generar con el instalador.

Desactivación de Identity and Access Manager

Si lo desea, puede desactivar Identity and Access Manager (también conocido como IAM).

Para deshabilitar IAM,

En la ventana de configuración de Kaspersky Security Center 14 Web Console, cambie el botón de alternancia de IAM a desactivado.

Puede activar IAM en cualquier otro momento.

Si actualiza Kaspersky Security Center 14 Web Console a través del instalador y especifica que no desea instalar IAM, se actualizará Kaspersky Security Center 14 Web Console y no se instalará IAM. Se eliminará toda la información sobre la integración con Kaspersky Industrial CyberSecurity for Networks de su equipo, así como los archivos de configuración de IAM y los archivos de registro.

Configuración de la autenticación de dominio mediante los protocolos NTLM y Kerberos

Kaspersky Security Center 14 le permite utilizar la autenticación de dominio en OpenAPI mediante los protocolos NTLM y Kerberos. El uso de la autenticación de dominio le permite a un usuario de Windows habilitar la autenticación segura en Kaspersky Security Center 14 Web Console sin tener que volver a introducir la contraseña en la red corporativa (inicio de sesión único).

La autenticación de dominio en OpenAPI sobre el protocolo Kerberos tiene las siguientes restricciones:

- El usuario de Kaspersky Security Center 14 Web Console debe estar autenticado en Active Directory mediante el protocolo Kerberos. El usuario debe tener un Ticket Granting Ticket de Kerberos válido (también conocido como TGT). Un TGT se emite automáticamente cuando se autentica en el dominio.
- Debe configurar la autenticación Kerberos en el navegador. Para obtener más información, consulte la documentación del navegador que está utilizando.

Si desea utilizar la autenticación de dominio mediante protocolos Kerberos, su red debe cumplir las siguientes condiciones:

- El Servidor de administración debe ejecutarse con el nombre de la cuenta de dominio.
- El servidor Kaspersky Security Center Web Console debe instalarse en el mismo dispositivo donde está instalado el Servidor de administración.
- Debe especificar los siguientes nombres de servicio principal (SPN) para la cuenta del Servidor de administración:
  - “https/<servidor.fqnd.nombre>”
  - “https/<servidor>”

  Aquí,<server> es el nombre de red del dispositivo del Servidor de administración, y <server.fqnd.name> es el nombre FQDN del dispositivo del Servidor de administración.
- Al conectarse a la Consola de administración o a Kaspersky Security Center Web Console, la dirección del Servidor de administración debe especificarse exactamente como la dirección para la que está registrado el Nombre principal del servicio (SPN). Puede especificar <serverhost.find.name> o <serverhost>.
- Para un inicio de sesión sin contraseña, el proceso del navegador en el que Kaspersky Security Center Web Console está abierto como navegador debe ejecutarse bajo una cuenta de dominio.

Los protocolos Kerberos y NTLM solo son compatibles con OpenAPI para Kaspersky Security Center 14. No son compatibles con OpenAPI para Kaspersky Security Center Linux.

Instalación inicial de Kaspersky Security Center 14 Web Console

Esta sección describe los pasos que debe seguir después de la instalación de Kaspersky Security Center Web Console 14 para realizar su configuración inicial.

Asistente de inicio rápido (Kaspersky Security Center 14 Web Console)

Esta sección proporciona información sobre del Asistente de inicio rápido del Servidor de administración.

> El Asistente requiere acceso a Internet. Si su Servidor de administración no tiene acceso a Internet, le recomendamos que realice todos los pasos del Asistente de forma manual, a través de la interfaz de Kaspersky Security Center 14 Web Console.

Kaspersky Security Center le permite ajustar una selección mínima de parámetros de configuración para crear un sistema centralizado de administración para proteger su red contra amenazas de seguridad. Esta configuración se realiza mediante el Asistente de inicio rápido. Cuando el Asistente se está ejecutando, puede realizar los siguientes cambios en la aplicación:

- Añadir archivos claves o ingresar códigos de activación que se pueden distribuir automáticamente a los dispositivos de grupos de administración.
- Configurar la interacción con Kaspersky Security Network (KSN). Si ha permitido el uso de KSN, el Asistente habilita el servicio de Servidor proxy de KSN, lo que garantiza la conexión entre KSN y los dispositivos.
- Configurar el envío de notificaciones por correo electrónico sobre eventos que tienen lugar durante el funcionamiento del Servidor de administración y las aplicaciones administradas (para que el envío de notificaciones sea correcto, el servicio de mensajería se debe ejecutar en el Servidor de administración y en todos los dispositivos destinatarios).
- Crear una directiva de protección para estaciones de trabajo y servidores, así como tareas del análisis antivirus, tareas de descarga de actualizaciones y tareas de copia de seguridad de datos, para el nivel superior de la jerarquía de dispositivos administrados.

  > El Asistente de inicio rápido crea directivas de únicamente para las aplicaciones cuya carpeta **Dispositivos administrados** no contiene directivas. El Asistente de inicio rápido no crea ninguna tarea si ya existe alguna tarea con el mismo nombre en el nivel superior de jerarquía de los dispositivos administrados.

La aplicación automáticamente solicita que se ejecute el Asistente de inicio rápido tras la instalación del Servidor de administración la primera vez que se realiza la conexión con él. También puede iniciar el Asistente de inicio rápido manualmente en cualquier momento.

Para iniciar manualmente el Asistente de inicio rápido, haga lo siguiente:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Control de aplicaciones**.

3. Haga clic en **Iniciar Asistente de inicio rápido**.

El Asistente le solicita a realizar la configuración inicial del Servidor de administración. Siga las instrucciones del Asistente. Avance a través del Asistente utilizando el botón **Siguiente**.

Paso 1. Especificar la configuración de la conexión a Internet

Especificar la configuración del acceso a Internet de Kaspersky Security Center.

Seleccione la casilla **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si se selecciona esta casilla, los campos están disponibles para introducir la configuración. Especifique la configuración siguiente para la conexión con el servidor proxy:

- **Dirección**
- **Número de puerto**
- No utilizar el servidor proxy para direcciones locales

  No se utilizará un servidor proxy para conectarse a los dispositivos de la red local.

- Autenticación del servidor proxy

  Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  Este campo de entrada está disponible si la casilla **Usar servidor proxy** está seleccionada.

- Nombre de usuario (este campo está disponible si la casilla de verificación **Autenticación del servidor proxy** está seleccionada)

  La cuenta de usuario en la que se establece la conexión al servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

- Contraseña (este campo está disponible si la casilla de verificación **Autenticación del servidor proxy** está seleccionada)

  La contraseña configurada por el usuario bajo cuya cuenta se establece la conexión del servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

  Para ver la contraseña introducida, mantenga pulsado el botón **Mostrar** todo el tiempo que sea necesario.

Paso 2. Descarga de actualizaciones requeridas

Las actualizaciones necesarias se descargan de los servidores de Kaspersky automáticamente.

Paso 3. Selección de los alcances y plataformas de protección

Seleccione los alcances de protección y las plataformas que están en uso en su red. Cuando selecciona estas opciones, especifica los filtros para los complementos de administración de aplicaciones y los paquetes de distribución en los servidores de Kaspersky que puede descargar para instalar en los dispositivos cliente en su red. Seleccione las opciones:

- Áreas

  Puede seleccionar los siguientes alcances de protección:

  - **Estaciones de trabajo**. Seleccione esta opción si desea proteger las estaciones de trabajo en su red. La estación de trabajo está seleccionada de forma predeterminada.
  - **Servidores de archivos y almacenamiento**. Seleccione esta opción si desea proteger los servidores de archivos en su red.
  - **Dispositivos móviles**. Seleccione esta opción si desea proteger los dispositivos móviles pertenecientes a la empresa o a los empleados de la empresa. Si selecciona esta opción pero no ha proporcionado una licencia con la función de administración de dispositivos móviles, se muestra un mensaje que le informa sobre la necesidad de proporcionar una licencia con la función de administración de dispositivos móviles. Si no proporciona una licencia, no podrá usar la función de dispositivo móvil.
  - **Virtualización**. Seleccione esta opción si desea proteger las máquinas virtuales en su red.
  - **Kaspersky Anti-Spam**. Seleccione esta opción si desea proteger los servidores de correo electrónico de su organización del correo no deseado, el fraude y la entrega de malware.

- Sistemas operativos

  Puede seleccionar las siguientes plataformas:

  - Microsoft Windows
  - Linux
  - macOS
  - Android

Después de seleccionar los alcances y plataformas de protección, los complementos de administración y los paquetes de distribución para las aplicaciones de Kaspersky comenzarán a descargarse automáticamente.

Paso 4. Seleccionar el cifrado en las soluciones

La ventana **Cifrado en soluciones** se muestra solo si ha seleccionado **Estaciones de trabajo** como alcance de protección y **Microsoft Windows** como plataforma.

Kaspersky Endpoint Security para Windows incluye una herramienta de cifrado para la información almacenada en los dispositivos cliente. La aplicación administrada incluye herramientas de cifrado que tienen el Estándar de cifrado avanzado (AES) implementado con una longitud de clave de 256 o 56 bits. La descarga y el uso del paquete de distribución con una longitud de clave de 256 bits deben realizarse de conformidad con las leyes y regulaciones aplicables. Para descargar un paquete de distribución de Kaspersky Endpoint Security para Windows válido para las necesidades de su organización, consulte la legislación del país donde se encuentran los dispositivos cliente de su organización. En la ventana **Cifrado en soluciones**, seleccione uno de los siguientes tipos de cifrado:

- Cifrado fuerte. Este tipo de cifrado utiliza una longitud de clave de 256 bits.
- Cifrado ligero. Este tipo de cifrado utiliza una longitud de clave de 56 bits.

Paso 5. Configurar la instalación de los complementos para las aplicaciones administradas

Seleccione complementos para instalar aplicaciones administradas. Se muestra una lista de complementos ubicados en los servidores de Kaspersky. La lista se filtra de acuerdo con las opciones seleccionadas en el paso anterior del Asistente. Por defecto, una lista completa incluye complementos de todos los idiomas. Para mostrar solo el complemento de un idioma específico, utilice el filtro. La lista de complementos incluye las siguientes columnas:

- **Nombre**

  Se seleccionan los complementos que dependen de los componentes y las plataformas que haya seleccionado en el paso anterior.

- **Versión**

  La lista incluye complementos de todas las versiones colocadas en los servidores de Kaspersky. De forma predeterminada, se seleccionan los complementos de las últimas versiones.

- **Idioma**

  De forma predeterminada, el idioma de localización de un complemento está definido por el idioma de Kaspersky Security Center que ha seleccionado en la instalación. Puede especificar otros idiomas en la lista desplegable **Mostrar el idioma de localización de la Consola de administración o**.

Una vez seleccionados los complementos, haga clic en **Siguiente** para iniciar la instalación.

Paso 6. Instalar los complementos seleccionados

El Asistente de inicio rápido instala automáticamente los complementos que ha seleccionado en el paso anterior. Para instalar algunos complementos, debe aceptar las condiciones del EULA. Lea el texto del EULA, seleccione la casilla de verificación **Acepto usar Kaspersky Security Network** y haga clic en el botón **Instalar**. Si no acepta las condiciones del EULA, el complemento no se instala.

Cuando todos los complementos seleccionados están instalados, el Asistente de inicio rápido lo lleva automáticamente al siguiente paso.

Paso 7. Descargar los paquetes de distribución y crear los paquetes de instalación

Seleccione los paquetes de distribución que desea descargar.

Las actualizaciones de aplicaciones administradas pueden requerir la instalación de una versión mínima específica de Kaspersky Security Center.

Después de seleccionar un tipo de cifrado para Kaspersky Endpoint Security para Windows, se muestra una lista de paquetes de distribución de ambos tipos de cifrado. En la lista, se selecciona un paquete de distribución con el tipo de cifrado seleccionado. Puede seleccionar los paquetes de distribución de cualquier tipo de cifrado. El idioma del paquete de distribución corresponde al idioma de Kaspersky Security Center. Si no existe un paquete de distribución de Kaspersky Endpoint Security para Windows para el idioma de Kaspersky Security Center, se selecciona el paquete de distribución en inglés.

Para finalizar la descarga de algunos paquetes de distribución, debe aceptar el EULA. Cuando hace clic en el botón **Aceptar**, se muestra el texto del EULA. Para continuar con el siguiente paso del Asistente, debe aceptar las condiciones del EULA y las condiciones de la Política de privacidad de Kaspersky. Si no acepta las condiciones, se cancela la descarga del paquete.

Después de haber aceptado las condiciones del EULA y las condiciones de la Política de privacidad de Kaspersky, la descarga de los paquetes de distribución continúa. Más tarde, usará paquetes de instalación para implementar aplicaciones de Kaspersky en dispositivos cliente.

Paso 8. Configuración de Kaspersky Security Network

Especifique la configuración para transmitir la información sobre las operaciones de Kaspersky Security Center a la base de conocimientos de Kaspersky Security Network. Seleccione una de las siguientes opciones:

- **Acepto usar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos cliente transferirán automáticamente su información de operación a Kaspersky Security Network. La participación en Kaspersky Security Network garantiza actualizaciones más rápidas de bases de datos que contienen información sobre virus y otras amenazas, y asegura una respuesta más rápida ante amenazas de seguridad emergentes.

- **No acepto usar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se desactivará el uso de Kaspersky Security Network.

Paso 9. Selección del método de activación de la aplicación

Seleccione una de las siguientes opciones de activación de Kaspersky Security Center:

- **Introducir su código de activación**

  El *código de activación* es una secuencia única de 20 caracteres alfanuméricos. Introduzca un código de activación para añadir una clave que active Kaspersky Security Center. Recibirá el código de activación a través de la dirección de correo electrónico que especificó después de adquirir Kaspersky Security Center.

  Para activar la aplicación con un código de activación, necesita disponer de acceso a Internet a fin de establecer conexión con los servidores de activación de Kaspersky.

  Si ha seleccionado esta opción de activación, puede activar la opción **Desplegar clave de licencia automáticamente en dispositivos administrados**.

  Si esta opción está activada, la clave de licencia se desplegará automáticamente en los dispositivos administrados.

  Si esta opción está desactivada, puede desplegar después la clave de licencia en los dispositivos administrados en el nodo **Licencias de Kaspersky** del árbol de la Consola de administración.

- **Especifique un archivo clave**

  Un *archivo clave* es un archivo con la extensión .key que Kaspersky le proporciona. Sirve para añadir archivo clave que active la aplicación.

  Recibirá su archivo clave a través de la dirección de correo electrónico que especificó después de adquirir Kaspersky Security Center.

  Para activar la aplicación con un archivo clave, no hace falta conectarse a los servidores de activación de Kaspersky.

  Si ha seleccionado esta opción de activación, puede activar la opción **Desplegar clave de licencia automáticamente en dispositivos administrados**.

  Si esta opción está activada, la clave de licencia se desplegará automáticamente en los dispositivos administrados.

  Si esta opción está desactivada, puede desplegar después la clave de licencia en los dispositivos administrados en el nodo **Licencias de Kaspersky** del árbol de la Consola de administración.

- **Posponer la activación de aplicaciones**

  La aplicación funcionará con una funcionalidad básica, sin Administración de dispositivos móviles y sin administración de vulnerabilidades y parches.

Si decide posponer la activación de la aplicación, puede agregar una clave de licencia más adelante en cualquier momento en **OPERACIONES → LICENCIAS**.

Cuando trabaja con Kaspersky Security Center desplegado desde una AMI de pago o para un SKU facturado mensualmente según el uso, no puede especificar un archivo clave ni introducir un código.

Paso 10. Especificar la configuración de administración de actualizaciones de terceros

Este paso no se muestra si no tiene la licencia de Administración de vulnerabilidades y parches y ya existe la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Para actualizaciones de software de terceros, seleccione una de las siguientes opciones:

- **Buscar actualizaciones requeridas**

  La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea.

  Esta opción está seleccionada de forma predeterminada.

- **Buscar e instalar las actualizaciones requeridas**

  Las tareas *Buscar vulnerabilidades y actualizaciones requeridas* y *Instalar actualizaciones requeridas y reparar vulnerabilidades* se crean automáticamente, si no tiene ninguna.

  Esta opción solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

Para las actualizaciones de Windows Update, seleccione una de las siguientes opciones:

- **Utilizar los orígenes de actualización definidos en la directiva del dominio**

  Los dispositivos cliente descargarán las actualizaciones de Windows Update de acuerdo con la configuración de su directiva de dominio. La directiva del Agente de red se crea automáticamente si no tiene una.

- **Utilizar el Servidor de administración como servidor WSUS**

  Los dispositivos cliente descargarán las actualizaciones de Windows Update del Servidor de administración. La tarea *Realizar la sincronización de Windows Update* y la directiva del Agente de red se crean automáticamente, si no tiene ninguna.

  Esta opción solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

Paso 11. Crear una configuración de protección de red básica

Puede consultar la lista de directivas y tareas que se crean.

Espere a que se complete la creación de directivas y tareas antes de ir al paso siguiente del Asistente.

Paso 12. Configuración de notificaciones por correo electrónico

Configure la entrega de notificaciones sobre eventos registrados durante el funcionamiento de aplicaciones Kaspersky en los dispositivos cliente. Estos parámetros servirán de configuración predeterminada de las directivas de la aplicación.

Para configurar la entrega de notificaciones sobre eventos que ocurren en aplicaciones de Kaspersky, use la configuración siguiente:

- **Destinatarios (direcciones de correo electrónico)**

  Las direcciones de correo electrónico de usuarios a quien la aplicación enviará notificaciones. Puede introducir una o más direcciones; si introduce más de una dirección, sepárelas con un punto y coma.

- **Dirección del servidor SMTP**

  La dirección o direcciones de los servidores de correo de su organización.

  Si introduce más de una dirección, sepárelas con un punto y coma. Puede usar los siguientes valores:

  - Dirección IPv4 o IPv6
  - Nombre de la red de Windows (nombre NetBIOS) del dispositivo
  - Nombre DNS del servidor SMTP

- **Puerto del servidor SMTP**

  Número del puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

- **Utilizar autenticación ESMTP**

  Activa la compatibilidad con autenticación de ESMTP. Cuando la casilla está seleccionada, en los campos **Nombre de usuario** y **Contraseña**, puede especificar la configuración de la autorización de ESMTP. De forma predeterminada, esta casilla está vacía y los parámetros de autenticación ESMTP no están disponibles.

- **Usar TLS**

Puede especificar la configuración de TLS para la conexión con un servidor SMTP:

- **No usar TLS**

Puede seleccionar esta opción si desea desactivar el cifrado de mensajes de correo electrónico.

- **Utilizar TLS si es compatible con el servidor SMTP**

Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.

- **Usar siempre TLS, comprobar la validez del certificado del servidor**

Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse con el servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si selecciona el valor **Usar siempre TLS, comprobar la validez del certificado del servidor**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

Puede especificar certificados para una conexión TLS al hacer clic en el enlace **Especificar certificados**:

- Busque un archivo de certificado para el servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo en el Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

- Busque un archivo de certificado para el cliente:

Puede utilizar un certificado que haya recibido de cualquier fuente, por ejemplo, de cualquier autoridad de certificación confiable. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

  - Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Ambos archivos no dependen el uno del otro y, por ende, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

  - Contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y su clave privada. Cuando se cargue el archivo, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

Puede probar la nueva configuración de la notificación por correo electrónico haciendo clic en el botón **Enviar mensaje de prueba**.

Paso 13. Realizar una encuesta de red

El Servidor de administración realiza un sondeo inicial. Durante el sondeo, se muestra una barra de progreso. Cuando se completa la encuesta, el enlace **Ver dispositivos detectados** queda disponible. Puede hacer clic en este enlace para ver los dispositivos de red detectados por el Servidor de administración. Para volver al Asistente de inicio rápido, presione la tecla **Escape**.

Paso 14. Cierre el Asistente de inicio rápido

En la página de finalización del Asistente de inicio rápido, seleccione la casilla **Ejecutar Asistente de despliegue de la protección** si desea iniciar la instalación automática de aplicaciones antivirus y/o el Agente de red en dispositivos en su red.

Para cerrar el Asistente, haga clic en el botón **Finalizar**.

Conexión de dispositivos fuera de la oficina

Esta sección describe cómo conectar los dispositivos fuera de la oficina (es decir, los dispositivos administrados que se encuentran fuera de la red principal) al Servidor de administración.

Escenario: conexión de dispositivos fuera de la oficina a través de una puerta de enlace de conexión

Este escenario describe cómo conectar dispositivos administrados que se encuentran fuera de la red principal al Servidor de administración.

Requisitos previos

El escenario tiene los siguientes requisitos previos:

- Una zona desmilitarizada (DMZ) está organizada en la red de su organización.
- El Servidor de administración de Kaspersky Security Center está desplegado en la red corporativa.

Etapas

Este escenario avanza en etapas:

1. **Seleccionar un dispositivo cliente en la DMZ**

   Este dispositivo se utilizará como puerta de enlace de conexión. El dispositivo que seleccione debe cumplir los requisitos de las puertas de enlace de conexión.

2. **Instalación de Agente de red con la función de puerta de enlace de conexión**

   Le recomendamos que utilice una instalación local para instalar el Agente de red en el dispositivo seleccionado.

   De forma predeterminada, el archivo de instalación se encuentra en: \\<server name>\KLSHARE\PkgInst\NetAgent_<version number>

En la ventana **Puerta de enlace de conexión** del Asistente de instalación del Agente de red, seleccione **Usar el Agente de red como puerta de enlace de conexión en DMZ**. Este modo activa simultáneamente la función de puerta de enlace de conexión e indica al Agente de red que espere las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración.

También puede instalar el Agente de red en un dispositivo Linux y configurar el Agente de red para que funcione como puerta de enlace de conexión, pero preste atención a la lista de limitaciones del Agente de red que se ejecuta en dispositivos Linux.

3. **Permitir conexiones en firewalls en la puerta de enlace de conexión**

   Para asegurarse de que el Servidor de administración pueda realmente conectarse a la puerta de enlace de conexión en la DMZ, permita conexiones al puerto TCP 13000 en todos los firewalls entre el Servidor de administración y la puerta de enlace de conexión.

   Si la puerta de enlace de conexión no tiene una dirección IP real en Internet, sino que se encuentra detrás de Network Address Translation (NAT), configure una regla para reenviar las conexiones a través de NAT.

4. **Creación de un grupo de administración para dispositivos externos**

   Cree un nuevo grupo en el grupo de **Dispositivos administrados**. Este grupo nuevo contendrá dispositivos administrados externos.

5. **Conexión de la puerta de enlace de conexión a un Servidor de administración.**

   La puerta de enlace de conexión que ha configurado queda a la espera de que el Servidor de administración se conecte. Sin embargo, el Servidor de administración no enumera el dispositivo con la puerta de enlace de conexión entre los dispositivos administrados. Esto se debe a que la puerta de enlace de conexión no ha intentado establecer una conexión con el Servidor de administración. Por lo tanto, necesita un procedimiento especial para asegurarse de que el Servidor de administración inicie una conexión con la puerta de enlace de conexión.

   Haga lo siguiente:

   1. Añada la puerta de enlace de conexión como punto de distribución.
   2. Mueva la puerta de enlace de conexión del grupo **Dispositivos no asignados** al grupo que ha creado para dispositivos externos.

   La puerta de enlace de conexión queda conectada y configurada.

6. **Conexión de equipos de escritorio externos al Servidor de administración:**

   Por lo general, los equipos de escritorio externos no se mueven dentro del perímetro. Por lo tanto, debe configurarlos para que se conecten al Servidor de administración a través de la puerta de enlace al instalar el Agente de red.

7. **Configuración de actualizaciones para equipos de escritorio externos**

   Si las actualizaciones de las aplicaciones de seguridad están configuradas para descargarse del Servidor de administración, los equipos externos descargan las actualizaciones a través de la puerta de enlace de conexión. Esto tiene dos desventajas:

   - Se trata de tráfico innecesario, que ocupa el ancho de banda del canal de comunicación de Internet de la empresa.
   - Esta no es necesariamente la forma más rápida de obtener actualizaciones. Es muy probable que sea más barato y rápido que los equipos externos reciban actualizaciones de los servidores de actualización de Kaspersky.

   Haga lo siguiente:

   1. Mueva todos los equipos externos al grupo de administración independiente que ha creado.

2. Excluya al grupo con dispositivos externos de la tarea de actualización.

3. Cree una tarea de actualización aparte para el grupo con dispositivos externos.

8 **Conexión de equipos portátiles que viajan al Servidor de administración**

Los equipos portátiles que viajan a veces están dentro de la red, y otras fuera. Para una gestión eficaz, necesita que se conecten al Servidor de administración de forma diferente según su ubicación. Para un uso eficiente del tráfico, también necesitan recibir actualizaciones de diferentes fuentes según su ubicación.

Necesita configurar reglas para usuarios fuera de la oficina: perfiles de conexión y descripciones de ubicación de red. Cada regla define la instancia del Servidor de administración al que deben conectarse los equipos portátiles que viajan, según su ubicación y según el Servidor de administración desde el cual deben recibir actualizaciones.

Acerca de la conexión de dispositivos fuera de la oficina

Algunos de los dispositivos administrados que siempre están fuera de la red principal (por ejemplo, los equipos en las sucursales regionales de una empresa; quioscos, cajeros automáticos y terminales instalados en varios puntos de venta; equipos en las oficinas en casa de los empleados) no se pueden conectar directamente al Servidor de administración. Algunos dispositivos viajan fuera del perímetro de vez en cuando (por ejemplo, ordenadores portátiles de usuarios que visitan sucursales regionales o la oficina de un cliente).

Con todo, es necesario monitorizar y gestionar la protección de los dispositivos fuera de la oficina: recibir información real sobre su estado de protección y mantener actualizadas las aplicaciones de seguridad. Esto es necesario porque, por ejemplo, si un dispositivo de este tipo se ve comprometido mientras está lejos de la red principal, podría convertirse en una plataforma para propagar amenazas tan pronto como se conecte a la red principal. Para conectar dispositivos fuera de la oficina al Servidor de administración, puede utilizar dos métodos:

- Puerta de enlace de conexión en la zona desmilitarizada (DMZ)

  Consulte el esquema de tráfico de datos: Servidor de administración en LAN, dispositivos administrados en Internet, puerta de enlace de conexión en uso

- Servidor de administración en DMZ

  Consulte el esquema de tráfico de datos: Servidor de administración en DMZ, dispositivos administrados en Internet

Una puerta de enlace de conexión en la DMZ

Un método recomendado para conectar dispositivos fuera de la oficina al Servidor de administración es organizar una DMZ en la red de la organización e instalar una puerta de enlace de conexión en la DMZ. Los dispositivos externos se conectarán a la puerta de enlace de conexión y el Servidor de administración dentro de la red iniciará la conexión con los dispositivos a través de la puerta de enlace de conexión.

En comparación con el otro método, este es más seguro:

- No es necesario abrir el acceso al Servidor de administración desde fuera de la red.

- Una puerta de enlace de conexión comprometida no representa un alto riesgo para la seguridad de los dispositivos de red. Una puerta de enlace de conexión en realidad no administra nada por sí misma y no establece ninguna conexión.

Además, una puerta de enlace de conexión no requiere muchos recursos de hardware.

Sin embargo, este método tiene un proceso de configuración más complicado:

- Para hacer que un dispositivo actúe como puerta de enlace de conexión en la DMZ, debe instalar el Agente de red y conectarlo al Servidor de administración de una manera específica.
- No podrá utilizar la misma dirección para conectarse al Servidor de administración en todas las situaciones. Desde fuera del perímetro, no solo deberá utilizar una dirección diferente (dirección de puerta de enlace de conexión), sino también un modo de conexión diferente: a través de una puerta de enlace de conexión.
- También debe definir diferentes configuraciones de conexión para ordenadores portátiles en diferentes ubicaciones.

Servidor de administración en la DMZ

Otro método es instalar un único Servidor de administración en la DMZ.

Esta configuración es menos segura que el otro método. Para administrar ordenadores portátiles externos en este caso, el Servidor de administración debe aceptar conexiones desde cualquier dirección en Internet. Seguirá administrando todos los dispositivos en la red interna, pero desde la DMZ. Por lo tanto, un servidor comprometido podría causar una enorme cantidad de daños, a pesar de la baja probabilidad de que ocurra tal evento.

El riesgo se reduce en gran medida si el Servidor de administración en la DMZ no administra dispositivos en la red interna. Una configuración de este tipo puede utilizarla, por ejemplo, un proveedor de servicios para administrar los dispositivos de los clientes.

Es posible que desee utilizar este método en los siguientes casos:

- Si está familiarizado con la instalación y configuración del Servidor de administración y no desea realizar otro procedimiento para instalar y configurar una puerta de enlace de conexión.
- Si necesita gestionar más dispositivos. La capacidad máxima del Servidor de administración es de 100.000 dispositivos, mientras que una puerta de enlace de conexión puede admitir hasta 10.000 dispositivos.

Esta solución también tiene posibles dificultades:

- El Servidor de administración requiere más recursos de hardware y una base de datos más.
- La información sobre los dispositivos se almacenará en dos bases de datos no relacionadas (para el Servidor de administración dentro de la red y otra en la DMZ), lo que complica el la monitorización.
- Para administrar todos los dispositivos, el Servidor de administración debe ser parte de una jerarquía, lo que complica no solo la monitorización, sino también la administración. Una instancia del Servidor de administración secundario impone limitaciones a las posibles estructuras de los grupos de administración. Debe decidir cómo y qué tareas y directivas distribuir a una instancia del Servidor de administración secundario.
- Configurar dispositivos externos para usar el Servidor de administración en la DMZ desde afuera y usar el Servidor de administración principal desde adentro no es más simple que configurarlos para usar una conexión condicional a través de una puerta de enlace.
- Altos riesgos de seguridad. Una instancia del Servidor de administración comprometida hace más fácil comprometer ordenadores portátiles administrados. Si esto sucede, los piratas informáticos solo necesitan esperar a que uno de los ordenadores portátiles regrese a la red corporativa para poder continuar con su ataque contra la red de área local.

Conexión de equipos de escritorio externos al Servidor de administración:

Los equipos de escritorio que siempre están fuera de la red principal (por ejemplo, los equipos en las sucursales regionales de la empresa; quioscos, cajeros automáticos y terminales instalados en varios puntos de venta; equipos en las oficinas en casa de los empleados) no se pueden conectar directamente al Servidor de administración. Deben conectarse al Servidor de administración a través de una puerta de enlace de conexión que esté instalada en la zona desmilitarizada (DMZ). Esta configuración se realiza al instalar el Agente de red en esos equipos.

Para conectar equipos de escritorio externos al Servidor de administración:

1. Cree un paquete nuevo de instalación personalizada para el Agente de red.
2. Abra las propiedades del paquete de instalación creado y vaya a la sección **Configuración** → **Avanzado**; luego, elija la opción **Conectar con el Servidor de administración usando un puerta de enlace de conexión**.

   El ajuste **Conectar con el Servidor de administración usando un puerta de enlace de conexión** es incompatible con el ajuste **Usar el Agente de red como puerta de enlace de conexión en DMZ**. No puede habilitar estas dos configuraciones al mismo tiempo.

3. En el campo **Dirección de la puerta de enlace de conexión**, especifique la dirección pública de la puerta de enlace de conexión.

   Si la puerta de enlace de conexión se encuentra detrás de un sistema de traducción de direcciones de red (NAT) y no tiene su propia dirección pública, configure una regla de puerta de enlace NAT para reenviar conexiones desde la dirección pública a la dirección interna de la puerta de enlace de conexión.

4. Cree un paquete de instalación independiente basado en el paquete de instalación creado.
5. Entregue el paquete de instalación independiente a los equipos de destino de forma electrónica o mediante una unidad extraíble.
6. Instale Agente de red desde el paquete independiente.

Los equipos de escritorio externos quedan conectados al Servidor de administración.

Acerca de los perfiles de conexión para usuarios fuera de la oficina

Puede que los usuarios "fuera de la oficina" de equipos portátiles (en adelante, también denominados "dispositivos") deban cambiar el método de conexión a un Servidor de administración o cambiar entre Servidores de administración según la ubicación actual del dispositivo en la red empresarial.

Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

Uso de diferentes direcciones de un único Servidor de administración

Los dispositivos con el Agente de red instalado pueden conectarse al Servidor de administración ya sea mediante la intranet de la organización o por Internet. Esta situación puede requerir que el Agente de red utilice direcciones diferentes para la conexión con el Servidor de administración: la dirección del Servidor de administración externa para la conexión a Internet y la dirección del Servidor de administración interna para la conexión a la intranet.

Para ello, añada un perfil para la conexión al Servidor de administración desde Internet en las propiedades de la política del Agente de red (en la sección **Configuración de la aplicación → Red → Perfiles de conexión → Perfiles de conexión al Servidor de administración**). En la ventana de creación de perfil, desactive la opción **Usar solo para recibir actualizaciones** y asegúrese de que esté seleccionada la opción **Sincronizar la configuración de la conexión con la configuración del Servidor de administración especificada para este perfil**. Si usa una puerta de enlace de conexión para acceder al Servidor de administración (por ejemplo, en una configuración de Kaspersky Security Center como la que se describe en Acceso a Internet: el Agente de red como puerta de enlace en DMZ), debe especificar la dirección de la puerta de enlace de conexión en el campo correspondiente del perfil de conexión.

Cambio entre Servidores de administración según la red actual

Si la organización tiene varias oficinas con Servidores de administración diferentes y algunos de los dispositivos con el Agente de red instalado se mueven entre ellas, necesita el Agente de red para la conexión con el Servidor de administración de la red local en la oficina donde se ubica el dispositivo actualmente.

En este caso, cree un perfil de conexión al Servidor de administración en las propiedades de la directiva del Agente de red para cada una de las oficinas, excepto para la oficina principal donde se encuentra el Servidor de administración principal. Especifique las direcciones de los Servidores de administración en los perfiles de conexión y active o desactive la opción **Usar solo para recibir actualizaciones**:

- Seleccione la opción si necesita que el Agente de red se sincronice con el Servidor de administración principal, mientras el Servidor local se usa solo para descargar actualizaciones.
- Desactive esta opción si es necesario que el Agente de red sea completamente administrado por el Servidor de administración local.

Después de esto, debe configurar las condiciones de conmutación a los perfiles recientemente creados: al menos, una condición para cada una de las oficinas, excepto la oficina principal. El objetivo de cada condición consiste en la detección de elementos que sean específicos del entorno de red de una oficina. Si una condición es verdadera, se activa el perfil correspondiente. Si ninguna de las condiciones es verdadera, el Agente de red cambia al Servidor de administración principal.

Creación de un perfil de conexión para usuarios fuera de la oficina

El perfil de conexión del Servidor de Administración sólo está disponible en dispositivos con Windows y macOS.

Para crear un perfil que permita a los usuarios fuera de la oficina conectar el Agente de red al Servidor de administración:

1. Si desea crear un perfil de conexión para un grupo de dispositivos administrados, abra la directiva del Agente de red de este grupo. Para ello, realice las siguientes acciones:
   a. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
   b. Haga clic en el vínculo de la ruta actual.
   c. En la ventana que se abre, seleccione un grupo de administración requerido.
      Después de eso, se cambia la ruta actual.

d. Agregue la directiva del Agente de red para el grupo de dispositivos administrados. Si ya lo ha creado, haga clic en el nombre de la directiva del Agente de red para abrir las propiedades de la directiva.

2. Si desea crear un perfil de conexión para un dispositivo administrado específico, haga lo siguiente:

   a. En el menú principal, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.

   b. Haga clic en el nombre del dispositivo administrado.

   c. En la ventana de propiedades del dispositivo que se abre, vaya a la pestaña **Aplicaciones**.

   d. Haga clic en el nombre de la directiva del Agente de red a la que solo se aplica el dispositivo administrado seleccionado.

3. En la ventana de propiedades que se abre, vaya a **Configuración de la aplicación** → **Red** → **Perfiles de conexión.**

4. En la sección **Perfiles de conexión al Servidor de administración**, haga clic en el botón **Añadir**.

   De forma predeterminada, la lista de perfiles de conexión contiene los perfiles <Modo sin conexión> y <Servidor de administración principal>. No se puede modificar ni eliminar el perfiles.

   El perfil <Modo sin conexión> no especifica ningún Servidor para la conexión. Por lo tanto, el Agente de red, cuando se cambia a ese perfil, no intenta conectarse a ningún Servidor de administración mientras las aplicaciones instaladas en dispositivos cliente se ejecutan bajo directivas fuera de la oficina. El perfil <Modo sin conexión> puede utilizarse si los dispositivos están desconectados de la red.

   El perfil <Servidor de administración principal> indica para la conexión el Servidor de administración que se seleccionó durante la instalación del Agente de red. El perfil <Servidor de administración principal> se aplica cuando un dispositivo se conecta de nuevo al Servidor de administración maestro después de que se ejecutara en una red externa durante algún tiempo.

5. En la ventana **Configurar perfil** que se abre, configure el perfil de conexión:

   - **Configurar perfil**

     En el campo de entrada se puede ver o cambiar el nombre del perfil de conexión.

   - **Dirección del Servidor de administración**

     La Dirección del Servidor de administración al cual el dispositivo cliente debe conectarse durante la activación del perfil.

   - **Número de puerto**

     Número de puerto que se utiliza en la conexión.

   - **Puerto SSL**

     Número de puerto para la conexión mediante el protocolo SSL.

   - **Usar conexión SSL**

Si esta opción está activada, la conexión se establece a través de un puerto seguro, utilizando el protocolo SSL.

Esta opción está activada de forma predeterminada. Le recomendamos que no desactive esta opción para que su conexión siga siendo segura.

- Seleccione la opción **Usar servidor proxy** si desea usar un servidor proxy al conectarse a Internet. Si esta opción está seleccionada, los campos están disponibles para introducir la configuración. Especifique la configuración siguiente para la conexión con el servidor proxy:

  - Dirección

    Dirección del servidor proxy utilizado para la conexión de Kaspersky Security Center con Internet.

  - Número de puerto

    Número del puerto a través del cual se establecerá la conexión proxy de Kaspersky Security Center.

  - Autenticación del servidor proxy

    Si se selecciona esta casilla, en los campos de entrada se podrán especificar las credenciales para la autenticación del servidor proxy.

  - Nombre de usuario

    La cuenta de usuario en la que se establece la conexión al servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

  - Contraseña

    La contraseña configurada por el usuario bajo cuya cuenta se establece la conexión del servidor proxy (este campo está disponible si la casilla **Autenticación del servidor proxy** está seleccionada).

    Para ver la contraseña introducida, mantenga pulsado el botón **Mostrar** todo el tiempo que sea necesario.

- Dirección de la puerta de enlace de conexión

  Dirección de la puerta de enlace a través de la que se conectan los dispositivos cliente al Servidor de administración.

- Activar modo Fuera de la oficina cuando el Servidor de administración no esté disponible

  Seleccione esta casilla para permitir que las aplicaciones instaladas en un dispositivo cliente usen perfiles de directiva para dispositivos en modo fuera de la oficina, así como directivas fuera de la oficina, en cualquier intento de conexión si el Servidor de administración no está disponible. Si no se ha definido una directiva fuera de la oficina en la aplicación, se utilizará la directiva activa.

  Si esta opción está desactivada, las aplicaciones utilizarán las directivas activas.

  De forma predeterminada, esta casilla está en blanco.

- Usar solo para recibir actualizaciones

  Si esta opción está activada, el perfil lo utilizarán las aplicaciones instaladas en el dispositivo cliente solo para descargar actualizaciones. Para otras operaciones, la conexión al Servidor de administración será establecida con los parámetros de conexión iniciales definidos durante la instalación del Agente de red.

  Esta opción está activada de forma predeterminada.

- Sincronizar la configuración de la conexión con la configuración del Servidor de administración especificada para este perfil

  Si esta opción está activada, el Agente de red se conecta al Servidor de administración usando la configuración especificada en las propiedades del perfil.

  Si esta opción está desactivada, el Agente de red se conectará al Servidor de administración usando la configuración original especificada durante la instalación.

  Esta opción está disponible si la opción **Usar solo para recibir actualizaciones** está desactivada.

  Esta opción está desactivada de forma predeterminada.

Se crea un perfil para la conexión del Agente de red al Servidor de administración para usuarios fuera de la oficina. Cuando el Agente de red se conecta al Servidor de administración con este perfil, las aplicaciones instaladas en un dispositivo cliente utilizarán las directivas para estos dispositivos en modo fuera de la oficina, o bajo directivas fuera de la oficina.

Acerca del cambio del Agente de red a otro Servidor de administración

Kaspersky Security Center ofrece la opción de cambiar el Agente de red de un dispositivo cliente a otros Servidores de administración si cambian los siguientes parámetros de la red:

- **Condición para dirección del servidor DHCP**: si cambia la dirección IP del servidor Protocolo de configuración dinámica de host (DHCP) de la red.
- **Condición para dirección predeterminada de la puerta de enlace de conexión**: si cambia la dirección de la puerta de enlace principal de la red.
- **Condición para dominio DNS**: si cambia el sufijo DNS de la subred.
- **Condición para dirección del servidor DNS**: si cambia la dirección IP del servidor DNS de la red.
- **Condición para dirección del servidor WINS**: si cambia la dirección IP del servidor WINS de la red. Esta configuración solo está disponible para dispositivos que ejecutan Windows.
- **Condición para solvencia de nombre** - Si cambia el nombre DNS o NetBIOS del dispositivo cliente.
- **Condición para subred**: cambia la dirección de la subred y la máscara.
- **Condición para accesibilidad del dominio de Windows**: cambia el estado del dominio de Windows al que está conectado un dispositivo cliente. Esta configuración solo está disponible para dispositivos que ejecutan Windows.
- **Condición para accesibilidad de dirección de conexión SSL** - El dispositivo cliente puede o no puede (según la opción que seleccione) establecer una conexión SSL con un servidor específico (nombre:puerto). Para cada servidor, puede especificar adicionalmente un certificado SSL. En este caso, el Agente de red verifica el

certificado del servidor además de verificar la capacidad de conexión SSL. Si el certificado no coincide, la conexión falla.

Esta función solo es compatible con los Agentes de red instalados en dispositivos que ejecutan Windows o macOS.

Los parámetros iniciales de la conexión del Agente de red al Servidor de administración se definen durante la instalación del Agente de red. A continuación, si se han creado las reglas de cambio del Agente de red a otros Servidores de administración, el Agente de red responde a los cambios en la configuración de red del siguiente modo:

- Si la configuración de la red cumple con una de las reglas creadas, el Agente de red se conecta con el Servidor de administración que se especifique en ella. Las aplicaciones instaladas en los dispositivos cliente cambian a las directivas fuera de la oficina siempre y cuando así lo contemple una regla.
- Si ninguna de las reglas es aplicable, el Agente de red restaura la configuración predeterminada de la conexión al Servidor de administración especificado durante la instalación. Las aplicaciones instaladas en los dispositivos cliente restablecen las directivas activas.
- Si no se puede acceder al Servidor de administración, el Agente de red utiliza las directivas fuera de la oficina.

El Agente de red cambia a la directiva fuera de la oficina solo si la opción **Activar modo Fuera de la oficina cuando el Servidor de administración no esté disponible** está activada en la configuración de la directiva del Agente de red.

Los parámetros de conexión del Agente de red al Servidor de administración se guardan en un perfil de conexión. En el perfil de conexión, puede crear reglas de cambio de dispositivos cliente a directivas fuera de la oficina, así como configurar el perfil de modo que pueda utilizarse únicamente para descargar actualizaciones.

Creación de una regla de cambio de Agente de red por ubicación de red

El cambio de Agente de red por ubicación de red está disponible solo en dispositivos que ejecutan Windows y macOS.

Para crear una regla de cambio del Agente de red de un Servidor de administración a otro si la configuración de red cambia:

1. Si desea crear una regla para un grupo de dispositivos administrados, abra la directiva del Agente de red de este grupo. Para ello, realice las siguientes acciones:
   a. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
   b. Haga clic en el vínculo de la ruta actual.
   c. En la ventana que se abre, seleccione un grupo de administración requerido.
      Después de eso, se cambia la ruta actual.
   d. Agregue la directiva del Agente de red para el grupo de dispositivos administrados. Si ya lo ha creado, haga clic en el nombre de la directiva del Agente de red para abrir las propiedades de la directiva.
2. Si desea crear una regla para un dispositivo administrado específico, haga lo siguiente:

a. En el menú principal, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.

b. Haga clic en el nombre del dispositivo administrado.

c. En la ventana de propiedades del dispositivo que se abre, vaya a la pestaña **Aplicaciones**.

d. Haga clic en el nombre de la directiva del Agente de red a la que solo se aplica el dispositivo administrado seleccionado.

3. En la ventana de propiedades que se abre, vaya a **Configuración de la aplicación** → **Red** → **Perfiles de conexión.**

4. En la sección **Configuración de la ubicación de red**, haga clic en el botón **Añadir**.

5. En la ventana que se abre, configure la descripción de la ubicación de la red y la regla de cambio. Especifique la configuración de la descripción de la ubicación de la red siguiente:

- Descripción

  El nombre de una descripción de la ubicación de la red no puede contener más de 255 caracteres, ni contener símbolos especiales, como ("*<>?\/:|).

- Utilizar perfil de conexión

  En la lista desplegable se puede especificar el perfil de conexión que utiliza un Agente de red para conectarse al Servidor de administración. Este perfil se utilizará cuando las condiciones de la descripción de la ubicación de la red se cumplan. El perfil de conexión contiene la configuración para la conexión de Agente de red con el Servidor de administración; también define cuando los dispositivos cliente deben cambiar a directivas fuera de la oficina. El perfil solo se utiliza para descargar actualizaciones.

- Descripción activada

  Marque esta casilla para activar el uso de la nueva descripción de ubicación de red.

6. Seleccione las condiciones para la regla de cambio de Agente de red:

- **Condición para dirección del servidor DHCP**: si cambia la dirección IP del servidor Protocolo de configuración dinámica de host (DHCP) de la red.
- **Condición para dirección predeterminada de la puerta de enlace de conexión**: si cambia la dirección de la puerta de enlace principal de la red.
- **Condición para dominio DNS**: si cambia el sufijo DNS de la subred.
- **Condición para dirección del servidor DNS**: si cambia la dirección IP del servidor DNS de la red.
- **Condición para dirección del servidor WINS**: si cambia la dirección IP del servidor WINS de la red. Esta configuración solo está disponible para dispositivos que ejecutan Windows.
- **Condición para solvencia de nombre** - Si cambia el nombre DNS o NetBIOS del dispositivo cliente.
- **Condición para subred**: cambia la dirección de la subred y la máscara.

- **Condición para accesibilidad del dominio de Windows**: cambia el estado del dominio de Windows al que está conectado un dispositivo cliente. Esta configuración solo está disponible para dispositivos que ejecutan Windows.

- **Condición para accesibilidad de dirección de conexión SSL** - El dispositivo cliente puede o no puede (según la opción que seleccione) establecer una conexión SSL con un servidor específico (nombre:puerto). Para cada servidor, puede especificar adicionalmente un certificado SSL. En este caso, el Agente de red verifica el certificado del servidor además de verificar la capacidad de conexión SSL. Si el certificado no coincide, la conexión falla.

Las condiciones de una regla se combinan mediante el operador lógico AND. Para activar una regla de cambio por la descripción de la ubicación de la red, se deben cumplir todas las condiciones de cambio de reglas.

7. En la sección de condiciones, especifique cuándo debe cambiarse el Agente de red a otro Servidor de administración. Para ello, haga clic en el botón **Añadir** y luego configure el valor de la condición.

   Además, la opción **Corresponde, al menos, con un valor de la lista** está activada de forma predeterminada. Puede desactivar esta opción si desea que la condición se cumpla con todos los valores especificados.

8. Guarde sus cambios.

Se creará una nueva regla de cambio por la descripción de la ubicación de la red, según la cual, siempre que se cumplan las condiciones, el Agente de red utilizará el perfil de conexión especificado en la regla para conectarse al Servidor de administración.

Asistente de despliegue de la protección

Puede usar el Asistente de despliegue de la protección para instalar aplicaciones Kaspersky. El Asistente de despliegue de la protección permite la instalación remota de aplicaciones mediante paquetes de instalación creados previamente o directamente desde un paquete de distribución.

El Asistente de despliegue de la protección realiza las siguientes acciones:

- Descarga un paquete de instalación para la instalación de la aplicación (si no se creó antes). El paquete de instalación se encuentra en **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**. Puede usar este paquete de instalación para la instalación de la aplicación en el futuro.

- Crea y ejecuta una tarea de instalación remota para dispositivos específicos o para un grupo de administración. La tarea de instalación remota recién creada se almacena en la sección **Tareas**. Más tarde podrá iniciar esta tarea manualmente. El tipo de tarea es **Instalar aplicación en remoto**.

Si desea instalar Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, instale el paquete insserv-compat primero para configurar el Agente de red.

Iniciar Asistente de despliegue de la protección

Para iniciar manualmente el Asistente de despliegue de la protección,

En la ventana principal de la aplicación, haga clic en **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → ASISTENTE DE DESPLIEGUE DE LA PROTECCIÓN**.

Comienza el Asistente de despliegue de la protección. Avance a través del Asistente utilizando el botón **Siguiente**.

Paso 1. Seleccionar paquete de instalación

Seleccione el paquete de instalación de la aplicación que desea instalar.

Si el paquete de instalación de la aplicación requerida no está en la lista, haga clic en el botón **Añadir** y luego seleccione la aplicación de la lista.

Paso 2. Seleccionar un método para la distribución de archivos claves o códigos de activación

Seleccione un método para la distribución de la archivo clave o el código de activación:

- **No añadir la clave de licencia al paquete de instalación**

  La clave se distribuye automáticamente a todos los dispositivos con los que es compatible:
  - Si se ha activado la distribución automática en las propiedades de la clave.
  - Si se ha creado la tarea **Agregar clave**.

- **Añadir clave de licencia al paquete de instalación**

  La clave se distribuye a dispositivos junto con el paquete de instalación.

  No recomendamos que distribuya la clave con este método porque en el repositorio de paquetes está activado el acceso de lectura compartido.

Si el paquete de instalación ya incluye un archivo clave o un código de activación, se muestra esta ventana, pero solo contiene la información de la clave de licencia.

Paso 3. Seleccionar versión del Agente de red

Si seleccionó el paquete de instalación de una aplicación que no sea el agente de red, también debe instalar el agente de red, que conecta la aplicación con el Servidor de administración de Kaspersky Security Center.

Seleccione la última versión del agente de red.

Paso 4. Selección de dispositivos

Especifique una lista de dispositivos en los que se instalará la aplicación:

- **Instalar en dispositivos administrados**

  Si se selecciona esta opción, la tarea de instalación remota se creará para un grupo de dispositivos.

- **Seleccionar dispositivos para la instalación**

  La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

Paso 5. Especificar la configuración de tarea de instalación remota

En la página **Configuración de tarea Instalación remota**, especifique la configuración de la instalación remota de la aplicación.

En el grupo de ajustes **Forzar la descarga del paquete de instalación**, especifique cómo los archivos necesarios para la instalación de la aplicación se distribuirán a los dispositivos cliente:

- **Usando el Agente de red**

  Si esta opción está habilitada, el Agente de red instalado en dispositivos cliente entrega los paquetes de instalación a dichos dispositivos cliente.

  Si esta opción está deshabilitada, los paquetes de instalación se entregan mediante las herramientas de Microsoft Windows.

  Recomendamos que habilite esta opción si la tarea se ha asignado a dispositivos que tienen instalados Agentes de red.

  Esta opción está activada de forma predeterminada.

- **Usando los recursos del sistema operativo mediante puntos de distribución**

  Si esta opción está habilitada, los paquetes de instalación se transmiten a los dispositivos cliente mediante herramientas del sistema operativo a través de los puntos de distribución. Se puede seleccionar esta opción si existe al menos un punto de distribución en la red.

  Si la opción **Usando el Agente de red** está habilitada, los archivos se entregan mediante herramientas del sistema operativo solo si los recursos del Agente de red no están disponibles.

  De forma predeterminada, esta opción está habilitada para tareas de instalación remotas creadas en un Servidor de administración virtual.

- **Usando los recursos del sistema operativo mediante el Servidor de administración**

Si esta opción está habilitada, los archivos se transmitirán a dispositivos cliente mediante herramientas de Microsoft Windows a través del Servidor de administración. Puede activar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

Esta opción está activada de forma predeterminada.

Defina la configuración adicional:

- **No reinstalar la aplicación si ya se encuentra instalada**

  Si esta opción está habilitada, la aplicación seleccionada no se volverá a instalar si ya está instalada en el dispositivo cliente.

  Si esta opción está deshabilitada, la aplicación se instalará igualmente.

  Esta opción está activada de forma predeterminada.

- **Asignar instalación del paquete en las directivas de grupo de Active Directory**

  Si esta opción está habilitada, se instalará un paquete de instalación mediante las directivas de grupo del Active Directory.

  Esta opción está disponible si se ha seleccionado el paquete de instalación del Agente de red.

  Esta opción está desactivada de forma predeterminada.

Paso 6. Administración del reinicio

Especifique la acción para realizar si el sistema operativo debe reiniciarse cuando instale la aplicación:

- **No reiniciar el dispositivo**

  Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- **Reiniciar el dispositivo**

  Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  Si esta opción está desactivada, la solicitud se muestra solo una vez.

- **Reiniciar después de (min)**

  Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

Paso 7. Eliminar aplicaciones incompatibles antes de la instalación

Este paso solo está presente si se conoce que la aplicación que despliega es incompatible con otras aplicaciones.

Seleccione esta opción si desea que Kaspersky Security Center elimine automáticamente aplicaciones que sean incompatibles con la aplicación que despliegue.

También se muestra la lista de aplicaciones incompatibles.

Si no selecciona esta opción, la aplicación solo se instalará en dispositivos que no tengan aplicaciones incompatibles.

Paso 8. Mover dispositivos móviles a dispositivos administrados

Especifique si los dispositivos deben moverse a un grupo de administración después de la instalación del Agente de red.

- **No mover dispositivos**

  Los dispositivos permanecen en los grupos en los que se localizan actualmente. Los dispositivos que no se han localizado en ningún grupo permanecen sin asignar.

- **Mover dispositivos no asignados al grupo**

  Los dispositivos se mueven al grupo de administración que seleccione.

La opción **No mover dispositivos** está preseleccionada. Por razones de seguridad, quizá quiera mover los dispositivos manualmente.

Paso 9. Selección de cuentas para acceder a dispositivos

Si es necesario, agregue las cuentas que se utilizarán para iniciar la tarea de instalación remota:

- **No es necesaria una cuenta (Agente de red instalado)**

  Si se selecciona esta opción, no tiene que especificar la cuenta bajo la que se ejecutará el instalador de aplicación. La tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

  Si el Agente de red no se ha instalado en dispositivos cliente, esta opción no está disponible.

- **Se necesita una cuenta (para la instalación sin Agente de red)**

  Si se selecciona esta opción, puede especificar la cuenta bajo la que se ejecutará el instalador de aplicación. Puede especificar la cuenta de usuario si el Agente de red no se ha instalado en los dispositivos para los cuales está asignada la tarea.

  Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que se asignó esta tarea. En este caso, todas las cuentas que se han agregado se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

  Si no se agrega ninguna cuenta, la tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

Paso 10. Inicio de la instalación

Esta página es el último paso del Asistente. En este paso, la tarea **Tarea de instalación remota** se ha creado y configurado correctamente.

La opción **Ejecutar tarea después de que finalice el Asistente** no está seleccionada de forma predeterminada. Si selecciona esta opción, la tarea **Tarea de instalación remota** comenzará inmediatamente después de que complete el Asistente. Si no selecciona esta opción, la tarea **Tarea de instalación remota** no comenzará. Más tarde podrá iniciar esta tarea manualmente.

Haga clic en **Aceptar** para completar el paso final del Asistente de despliegue de la protección.

Configuración del Servidor de administración

Esta sección describe el proceso de configuración y las propiedades del Servidor de administración de Kaspersky Security Center.

Configuración de la conexión de Kaspersky Security Center 14 Web Console al Servidor de administración

Para configurar los puertos de conexión del Servidor de administración:

1. En la parte superior de la pantalla, haga clic en el icono de la **Configuración** ( ) al lado del nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Puertos de conexión**.

La aplicación muestra la configuración de conexión principal del servidor seleccionado.

En versiones anteriores de Kaspersky Security Center, la Consola de administración se conectaba al Servidor de administración mediante el puerto SSL TCP 13291, así como el puerto SSL TCP 13000. Desde Kaspersky Security Center 10 Service Pack 2, los puertos SSL usados por la aplicación se separan de forma estricta y cualquier uso indebido de puertos es imposible:

- El puerto SSL TCP 13291 solo puede ser utilizado por la Consola de administración.
- El puerto SSL TCP 13000 solo puede ser utilizado por el Agente de red, un Servidor de administración secundario y el Servidor de administración principal en DMZ.
- El puerto TCP 14000 solo puede ser utilizado para conectar la Consola de administración, los puntos de distribución y los Servidores de administración secundarios así como para recibir datos desde dispositivos cliente.

Visualización del registro de conexiones con el Servidor de administración

El historial de conexiones e intentos de conexión con el Servidor de administración durante su funcionamiento se puede guardar en un archivo de registro. La información en el archivo le permite rastrear no solo las conexiones desde su infraestructura de red, sino también los intentos no autorizados de acceder al servidor.

Para registrar los eventos de conexión al Servidor de administración:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Puertos de conexión**.

3. Active la opción **Registrar eventos de conexión del Servidor de administración**.

Todos los eventos adicionales de la conexión con el Servidor de administración, los resultados de autenticación y los errores de SSL se guardarán en el archivo %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Configuración del número máximo de eventos en el repositorio de eventos

En la sección **Repositorio de eventos** de la ventana de propiedades del Servidor de administración, puede editar la configuración del almacenamiento de eventos en la base de datos del Servidor de administración limitando el número de registros de eventos o el tiempo de almacenamiento de los registros. Cuando especifica el número máximo de eventos, la aplicación calcula una cantidad aproximada de espacio de almacenamiento requerido para el número especificado. Puede usar este cálculo aproximado para evaluar si tiene suficiente espacio libre en el disco para evitar el desbordamiento de la base de datos. La capacidad predeterminada de la base de datos del Servidor de administración es de 400.000 eventos. La capacidad máxima recomendada de la base de datos es 45 millones de eventos.

Si el número de eventos en la base de datos llega al valor máximo especificado por el administrador, la aplicación elimina los eventos más antiguos sobrescribiéndolos con los nuevos. Cuando el Servidor de administración elimina eventos antiguos, no puede guardar eventos nuevos en la base de datos. Durante este período de tiempo, la información sobre los eventos que fueron rechazados se escribe en el Registro de eventos de Kaspersky. Los nuevos eventos se ponen en cola y luego se guardan en la base de datos una vez que se completa la operación de eliminación.

Para limitar la cantidad de eventos que se pueden almacenar en el repositorio de eventos en el Servidor de administración:

1. En la parte superior de la pantalla, haga clic en el icono de la **Configuración** ( ) al lado del nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Repositorio de eventos**.

3. Especifique el número máximo de eventos almacenados en la base de datos.

4. Haga clic en el botón **Guardar**.

El número de eventos que se pueden almacenar en la base de datos está limitado al valor especificado.

Configuración de conexión de dispositivos con protección de UEFI

El *dispositivo con protección de UEFI* es un dispositivo con Kaspersky Anti-Virus for UEFI integrado al nivel de BIOS. La protección integrada garantiza la seguridad del dispositivo a partir del momento en que se inicia el sistema, mientras la protección en dispositivos sin el software integrado solo comienza a funcionar después de que se inicie la aplicación de seguridad. Kaspersky Security Center admite la administración de estos dispositivos.

Para modificar la configuración de conexión de dispositivos con protección de UEFI:

En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.

Se abre la ventana Propiedades del Servidor de administración.

1. En la pestaña **Control de aplicaciones**, seleccione la sección **Puertos adicionales**.
2. Modifique la configuración relevante:
   - **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

     Los dispositivos con protección de UEFI pueden conectarse al Servidor de administración.

   - **Puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS**

     Puede cambiar el número de puerto si la opción **Abrir puerto para dispositivos con protección de UEFI y dispositivos con KasperskyOS** está activada. El número de puerto predeterminado es el 13294.
3. Haga clic en el botón **Guardar**.

Los dispositivos con protección de UEFI pueden conectarse ahora al Servidor de administración.

Creación de una jerarquía de Servidores de administración: adición de un Servidor de administración secundario

Adición de un Servidor de administración secundario (operación realizada en el futuro Servidor de administración principal)

Puede añadir un Servidor de administración como Servidor de administración secundario y establecer así una jerarquía "principal/secundario".

Para añadir un Servidor de administración secundario que se pueda conectar mediante Kaspersky Security Center 14 Web Console:

1. Asegúrese de que el puerto 13000 del futuro Servidor de administración principal esté disponible para la recepción de conexiones desde los Servidores de administración secundarios.
2. En el futuro Servidor de administración principal, haga clic en el icono de **configuración** ().
3. En la página de propiedades que se abre, seleccione la pestaña **Servidores de administración**.
4. Seleccione la casilla de verificación junto al nombre del grupo de administración al que desea agregar el Servidor de administración.
5. En la línea del menú, haga clic en **Conectar Servidor de administración secundario**.

   Se inicia el Asistente del Servidor de administración secundario de conexión.
6. En la primera página del Asistente, complete los siguientes campos:

- Nombre a mostrar del Servidor de administración secundario

  Un nombre con el que se mostrará en la jerarquía el Servidor de administración secundario. Si lo desea, puede introducir la dirección IP como nombre, o puede usar un nombre como, por ejemplo, "Servidor secundario para el grupo 1".

- Dirección del Servidor de administración secundario (opcional)

  Especifique la dirección IP o el nombre de dominio del Servidor de administración secundario.

- Puerto SSL del Servidor de administración

  Especifique el número del puerto de SSL en el Servidor de administración principal. El número de puerto predeterminado es el 13000.

- Puerto API del Servidor de administración

  Especifique el número del puerto en el Servidor de administración principal para recibir conexiones de OpenAPI. El número de puerto predeterminado es el 13299.

- Conectar Servidor de administración principal a Servidor de administración secundario en DMZ

  Seleccione esta opción si el Servidor de administración secundario está en una zona desmilitarizada (DMZ).

- Usar servidor proxy

  Seleccione esta opción si utiliza un servidor proxy para conectarse al Servidor de administración secundario.

  En este caso, también tiene que especificar la siguiente configuración del servidor proxy:

  - **Dirección**
  - **Nombre de usuario**
  - **Contraseña**

7. Siga las instrucciones adicionales del Asistente.

Cuando el Asistente concluye, se crea la jerarquía "principal/secundario". El Servidor de administración principal empieza a aceptar conexiones del Servidor de administración secundario utilizando el puerto 13000. Se reciben y aplican las tareas y directivas del Servidor de administración principal. El Servidor de administración secundario se muestra en el Servidor de administración principal, en el grupo de administración donde se añadió.

Adición de un Servidor de administración secundario (operación realizada en el futuro Servidor de administración secundario)

Si no pudo conectarse al futuro Servidor de administración secundario (por ejemplo, debido a que estaba temporalmente desconectado o no estaba disponible para la conexión), aún puede añadir un Servidor de administración secundario.

Para añadir en calidad de secundario un Servidor de administración que no esté disponible para conectarse mediante Kaspersky Security Center 14 Web Console, haga lo siguiente:

1. Envíe el archivo de certificado del futuro Servidor de administración principal al administrador del sistema de la oficina donde se encuentra el supuesto Servidor de administración secundario. (por ejemplo, puede escribir el archivo en un dispositivo externo, como una unidad flash o enviarlo por correo electrónico.)

   El archivo de certificado se encuentra en el futuro Servidor de administración principal, en %ALLUSERSPROFILE %\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Solicite al administrador del sistema a cargo del futuro Servidor de administración secundario que haga lo siguiente:

   a. Haga clic en el icono de la **Configuración** ( ).

   b. En la página de propiedades que se abre, vaya a la sección **Jerarquía de Servidores de administración** de la pestaña **Control de aplicaciones**.

   c. Seleccione la opción **Este Servidor de administración es secundario en la jerarquía**.

   d. En el campo **Dirección del Servidor de administración principal**, especifique el nombre de la red del futuro Servidor de administración principal.

   e. Seleccione el archivo guardado anteriormente con el certificado del futuro Servidor de administración principal haciendo clic en **Examinar**.

   f. Si es necesario, seleccione la casilla **Conectar Servidor de administración principal a Servidor de administración secundario en DMZ**.

   g. Si la conexión con el futuro Servidor de administración secundario se realiza a través de un servidor proxy, seleccione la opción **Usar servidor proxy** y especifique la configuración de la conexión.

   h. Haga clic en **Guardar**.

Se construye la jerarquía "principal/secundario". El Servidor de administración principal comienza recibiendo conexión de Servidor de administración secundario utilizando el puerto 13000. Se reciben y aplican las tareas y directivas del Servidor de administración principal. El Servidor de administración secundario se muestra en el Servidor de administración principal, en el grupo de administración donde se añadió.

Visualización de la lista de Servidores de administración secundarios

Para ver la lista de los Servidores de administración secundarios (incluido el virtual), haga lo siguiente:

En la ventana principal de la aplicación, haga clic en el nombre del Servidor de administración ubicado junto al icono de **Configuración** ( ).

Se muestra la lista desplegable de los Servidores de administración secundarios (incluidos los virtuales).

Puede ir a cualquiera de estos Servidores de administración haciendo clic en su nombre.

Los grupos de administración también se muestran, pero están en gris y no están disponibles para su administración en este menú.

Eliminación de una jerarquía de Servidores de administración

Si ya no desea tener una jerarquía de Servidores de administración, puede desconectarlos de esta jerarquía.

Para eliminar una jerarquía de Servidores de administración:

1. En la parte superior de la pantalla, haga clic en el icono de la **Configuración** ( ) al lado del nombre del Servidor de administración principal.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. En el grupo de administración del que desea eliminar el Servidor de administración secundario, seleccione el Servidor de administración secundario.
4. En la línea del menú, haga clic en **Eliminar**.
5. En la ventana que se abre, haga clic en **Aceptar** para eliminar el Servidor de administración secundario.

El Servidor de administración principal anterior y el Servidor de administración secundario anterior ahora son independientes el uno del otro. La jerarquía ya no existe.

Mantenimiento del Servidor de administración

El mantenimiento del Servidor de administración le permite reducir el volumen de la base de datos y mejorar el rendimiento y la fiabilidad del funcionamiento de la aplicación. Le recomendamos realizar un mantenimiento del Servidor de administración por lo menos una vez a la semana.

El mantenimiento del Servidor de administración se lleva a cabo a través de la tarea especializada. La aplicación realiza las acciones siguientes durante el mantenimiento del Servidor de administración:

- Comprueba la base de datos en busca de errores.
- Reorganiza los índices de la base de datos.
- Actualiza las estadísticas de la base de datos.
- Reduce la base de datos (si es necesario).

La tarea Mantenimiento del Servidor de administración no admite MariaDB. Si se utiliza este DBMS en su red, los administradores deberán mantener MariaDB por su cuenta.

La tarea Mantenimiento del Servidor de administración se crea automáticamente al instalar Kaspersky Security Center. Si la tarea Mantenimiento del Servidor de administración se elimina, puede crearla manualmente.

Para crear la tarea Mantenimiento del Servidor de administración:

1. En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en el botón **Añadir**.

   Se inicia Asistente para añadir tarea.
3. En la ventana **Nueva tarea** del Asistente, seleccione **Mantenimiento del Servidor de administración** como tipo de tarea y haga clic en el botón **Siguiente**.
4. Siga el resto de instrucciones del Asistente.

La nueva tarea creada se muestra en la lista de tareas. Solo se puede ejecutar una tarea de Mantenimiento del Servidor de administración por Servidor de administración. Si ya se ha creado una tarea de Mantenimiento del Servidor de administración para un Servidor de administración, no se puede crear otra tarea de Mantenimiento del Servidor de administración de este tipo.

Configuración de la interfaz

Puede configurar la interfaz de Kaspersky Security Center 14 Web Console para mostrar y ocultar secciones y elementos de la interfaz, según las funciones que se utilicen.

Para configurar la interfaz de Kaspersky Security Center 14 Web Console de acuerdo con el conjunto de funciones utilizado actualmente:

1. En la ventana principal de la aplicación, haga clic en el menú de la cuenta.
2. En el menú desplegable, seleccione **Opciones de interfaz**.
3. En la ventana **Opciones de interfaz** que se abre, habilite o deshabilite la opción **Mostrar protección y cifrado de datos**.
4. Hacer clic en **Guardar**.

La consola muestra la sección **PROTECCIÓN Y CIFRADO DE DATOS**.

Administración de Servidores de administración virtuales

En esta sección, se describen las siguientes acciones para administrar Servidores de administración virtuales:

- Crear Servidores de administración virtual
- Activar y desactivar Servidores de administración virtual
- Eliminar Servidores de administración virtual
- Cambio del Servidor de administración de los dispositivos cliente

Creación de un Servidor de administración virtual

Puede crear Servidores de administración virtuales y añadirlos a grupos de administración.

Para crear y añadir un Servidor de administración virtual:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.

2. En la página que se abre, vaya a la pestaña **Servidores de administración**.

3. Seleccione el grupo de administración al que quiere añadir el Servidor de administración virtual.
   El Servidor de administración virtual administrará los dispositivos del grupo seleccionado (incluidos los subgrupos).

En la línea del menú, haga clic en **Nuevo Servidor de administración virtual**.

1. En la página que se abre, defina las propiedades del nuevo Servidor de administración virtual:

   - **Nombre del Servidor de administración virtual**.

   - **Dirección de conexión del Servidor de administración**

     Puede especificar el nombre o la dirección IP de su Servidor de administración.

2. En la lista de usuarios, seleccione al administrador del Servidor de administración virtual.

   Si lo desea, puede editar una de las cuentas existentes antes de asignarle la función de administrador o crear una nueva cuenta de usuario.

3. Haga clic en **Guardar**.

El nuevo Servidor de administración virtual se crea, se añade al grupo de administración y se muestra en la pestaña **Servidores de administración**.

Activación y desactivación de un Servidor de administración virtual

Cuando crea un nuevo Servidor de administración virtual, está activado de forma predeterminada. Puede activarlo o desactivarlo nuevamente en cualquier momento. Activar o desactivar un Servidor de administración virtual equivale a apagar o encender un Servidor de administración físico.

Activación y desactivación de un Servidor de administración virtual:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración.

2. En la página que se abre, vaya a la pestaña **Servidores de administración**.

3. Seleccione el Servidor de administración virtual que desea activar o desactivar.

4. En la línea del menú, haga clic en el botón **Activar/Desactivar Servidor de administración virtual**.

El estado del Servidor de administración virtual cambia a activado o desactivado, según cuál haya sido su estado anterior. El estado actualizado se muestra junto al nombre del Servidor de administración.

Eliminación de un Servidor de administración virtual

Cuando elimina un Servidor de administración virtual, también se eliminarán todos los objetos creados en el Servidor de administración, incluidas las directivas y las tareas. Los dispositivos administrados de los grupos de administración que estaban administrados por el Servidor de administración virtual se eliminarán de los grupos de administración. Para devolver los dispositivos en la administración de Kaspersky Security Center, ejecute el sondeo de red y luego mueva los dispositivos encontrados del grupo de Dispositivos no asignados a los grupos de administración.

Para eliminar un Servidor de administración virtual:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración.
2. En la página que se abre, vaya a la pestaña **Servidores de administración**.
3. Seleccione el Servidor de administración virtual que desea eliminar.
4. En la línea del menú, haga clic en el botón **Eliminar**.

Se elimina el Servidor de administración virtual.

Cambio del Servidor de administración de los dispositivos cliente

Se puede cambiar el Servidor de administración que administra los dispositivos cliente por otro con la tarea **Cambiar Servidor de administración**. Después de finalizar la tarea, los dispositivos cliente seleccionados se pondrán bajo la administración del Servidor de administración que especifique. Puede cambiar la administración de dispositivos entre los siguientes servidores de administración:

- Servidor de administración primario y uno de sus Servidores de administración virtuales
- Dos Servidores de administración virtuales del mismo Servidor de administración principal

Para cambiar el Servidor de administración que gestiona los dispositivos cliente a otro servidor:

1. En la ventana principal de la aplicación, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Cambiar Servidor de administración**.
4. Especifique el nombre para la tarea que está creando.

   El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Seleccionar dispositivos a los que se asignará la tarea.
6. Seleccione el Servidor de administración que desea utilizar para administrar los dispositivos seleccionados.
7. Especifique la configuración de la cuenta:
   - Cuenta predeterminada

La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

- **Cuenta**

  Cuenta bajo la que se ejecuta la tarea.

- **Contraseña**

  La contraseña de la cuenta bajo la cual la tarea se ejecutará.

8. Si en la página **Finalizar la creación de tareas**, activa la opción **Abrir los detalles de la tarea cuando se complete la creación**, puede modificar la configuración de tarea predeterminada. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

9. Haga clic en el botón **Finalizar**.

   La tarea se crea y se muestra en la lista de tareas.

10. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

11. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea que se ajuste a sus necesidades.

12. Haga clic en el botón **Guardar**.

    La tarea se crea y se configura.

13. Ejecute la tarea creada.

Tras completarse la tarea, los dispositivos cliente para los que se la creó se ponen bajo la administración del Servidor de administración especificado en los parámetros de tarea.

Activar la protección de la cuenta de modificaciones no autorizadas

Puede habilitar una opción adicional para proteger una cuenta de usuario de modificaciones no autorizadas. Si esta opción está activada, la modificación de la configuración de la cuenta de usuario requiere la autorización del usuario con derechos de modificación.

Para habilitar o deshabilitar la protección de la cuenta contra modificaciones no autorizadas:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.

2. Haga clic en el nombre de la cuenta de usuario interna en la que desea especificar la protección de la cuenta frente a modificaciones no autorizadas.

3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.

4. En la pestaña **Protección de cuenta**, seleccione la opción **Solicitar autenticación para verificar el permiso para modificar las cuentas de usuario** si desea solicitar credenciales cada vez que se cambia o modifica la configuración de la cuenta. De lo contrario, seleccione la opción **Permitir a los usuarios modificar esta cuenta sin autenticación adicional**.

5. Haga clic en el botón **Guardar**.

La protección de la cuenta contra modificaciones no autorizadas está activada para una cuenta de usuario.

Verificación en dos pasos

Esta sección describe cómo puede usar la verificación en dos pasos para reducir el riesgo de acceso no autorizado a Kaspersky Security Center 14 Web Console.

Escenario: Configurar la verificación en dos pasos para todos los usuarios

Este escenario describe cómo activar la verificación en dos pasos para todos los usuarios y cómo excluir las cuentas de usuario de la verificación en dos pasos. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para otros usuarios, la aplicación abre primero la ventana para habilitar la verificación en dos pasos para su cuenta. Este escenario también describe cómo activar la verificación en dos pasos para su propia cuenta.

> Si habilitó la verificación en dos pasos para su cuenta, puede proceder a activar la verificación en dos pasos para todos los usuarios.

Requisitos previos

Antes de empezar:

- Asegúrese de que su cuenta de usuario tenga derechos de Modificar ACL de objeto del área funcional **Funciones generales: Permisos de usuario** para modificar la configuración de seguridad de las cuentas de otros usuarios.

- Asegúrese de que los demás usuarios del Servidor de administración instalen una aplicación de autenticación en sus dispositivos.

Etapas

La activación de la verificación en dos pasos para todos los usuarios se realiza en etapas:

1. **Instalación de una aplicación de autenticación en un dispositivo**

   Puede instalar Google Authenticator, Microsoft Authenticator o cualquier otra aplicación de autenticación que admita el algoritmo de contraseña única basada en tiempo.

2. **Sincronización de la hora de la aplicación de autenticación con la hora del dispositivo en el que está instalado el Servidor de administración**

   Asegúrese de que la hora establecida en la aplicación de autenticación esté sincronizada con la hora del Servidor de administración.

3. **Activación de la verificación en dos pasos para su cuenta y recepción de la clave secreta de su cuenta**

   Instrucciones:

   - Para la consola de administración basada en MMC: Activación de la verificación en dos pasos de su propia cuenta
   - Para Kaspersky Security Center 14 Web Console: Activación de la verificación en dos pasos para su propia cuenta

   Después de activar la verificación en dos pasos para su cuenta, puede activar la verificación en dos pasos para todos los usuarios.

4. **Activación de la verificación en dos pasos para todos los usuarios**

   Los usuarios que tengan activada la verificación en dos pasos deben usarla para iniciar sesión en el Servidor de administración.

   Instrucciones:

   - Para la consola de administración basada en MMC: Activar la verificación en dos pasos para todos los usuarios
   - Para Kaspersky Security Center 14 Web Console: Activar la verificación en dos pasos para todos los usuarios

5. **Modificar el nombre de un emisor del código de seguridad**

   Si tiene varios Servidores de administración con nombres similares, es posible que deba cambiar los nombres de los emisores del código de seguridad para reconocer mejor los diferentes Servidores de administración.

   Instrucciones:

   - Para la consola de administración basada en MMC: Modificar el nombre del emisor de un código de seguridad
   - Para Kaspersky Security Center 14 Web Console: Modificar el nombre de un emisor de código de seguridad

6. **Exclusión de las cuentas de usuario para las que no necesita activar la verificación en dos pasos**

   Si es necesario, puede excluir usuarios de la verificación en dos pasos. Los usuarios con cuentas excluidas no tienen que utilizar la verificación en dos pasos para iniciar sesión en el Servidor de administración.

   Instrucciones:

   - Para la consola de administración basada en MMC: Excluir cuentas de la verificación en dos pasos
   - Para Kaspersky Security Center 14 Web Console: Excluir cuentas de la verificación en dos pasos

Resultados

Una vez completado este escenario:

- La verificación en dos pasos queda activada para su cuenta.
- La verificación en dos pasos queda activada para todas las cuentas de usuario del Servidor de administración, excepto para las cuentas de usuario que fueron excluidas.

Acerca de la verificación en dos pasos

Kaspersky Security Center proporciona verificación en dos pasos para los usuarios de Kaspersky Security Center 14 Web Console. Cuando la verificación en dos pasos está activada para su propia cuenta, cada vez que inicie sesión en Kaspersky Security Center 14 Web Console, debe introducir su nombre de usuario, contraseña y un código de seguridad adicional de un solo uso. Si usa la autenticación de dominio para su cuenta, basta con ingresar un código de seguridad adicional de un solo uso. Para recibir un código de seguridad de un solo uso, debe tener una aplicación de autenticación en su equipo o dispositivo móvil.

Un código de seguridad tiene un identificador denominado *nombre del emisor*. El nombre del emisor del código de seguridad se utiliza como un identificador del Servidor de administración en la aplicación de autenticación. Puede cambiar el nombre del emisor del código de seguridad. El nombre del emisor del código de seguridad tiene un valor predeterminado que es el mismo que el nombre del Servidor de administración. El nombre del emisor se utiliza como un identificador del Servidor de administración en la aplicación de autenticación. Si cambia el nombre del emisor del código de seguridad, debe volver a emitir una nueva clave secreta y pasarla a la aplicación de autenticación. Los códigos de seguridad son de un solo uso y válidos por hasta 90 segundos (el tiempo exacto puede variar).

Cualquier usuario que tenga activada la verificación en dos pasos puede volver a emitir su propia clave secreta. Cuando un usuario se autentica con la clave secreta reemitida y la usa para iniciar sesión, el Servidor de administración guarda la nueva clave secreta de la cuenta de usuario. Si un usuario introduce la clave secreta de forma incorrecta al formulario de autenticación, el Servidor de administración no guarda la nueva clave secreta y conserva la validez de la clave secreta vigente para la autenticación posterior.

Cualquier software de autenticación que admita el algoritmo de contraseña de un solo uso basado en tiempo (TOTP) se puede utilizar como aplicación de autenticación, por ejemplo, Google Authenticator. Para generar el código de seguridad, debe sincronizar la hora configurada en la aplicación de autenticación con la hora configurada del Servidor de administración.

Una aplicación de autenticación genera el código de seguridad de la siguiente manera:

1. El Servidor de administración genera una clave secreta especial y un código QR.
2. Usted pasa la clave secreta generada o el código QR a la aplicación de autenticación.
3. La aplicación de autenticación genera un código de seguridad de un solo uso que usted pasa a la ventana de autenticación del Servidor de administración.

Insistimos en recomendarle que instale una aplicación de autenticación en más de un dispositivo móvil. Guarde la clave secreta (o el código QR) y conservelos en un lugar seguro. Esto le ayudará a restaurar el acceso a Kaspersky Security Center 14 Web Console si pierde el acceso a su dispositivo móvil.

Para proteger el uso de Kaspersky Security Center, puede habilitar la verificación en dos pasos para su propia cuenta y habilitar la verificación en dos pasos para todos los usuarios.

Puede excluir cuentas de la verificación en dos pasos. Esto puede ser necesario para las cuentas de servicio que no pueden recibir un código de seguridad para la autenticación.

La verificación en dos pasos funciona según las siguientes reglas:

- Solo una cuenta de usuario que tenga los derechos Modificar objeto ACL en el área funcional **Funciones generales: Permisos de usuario** puede activar la verificación en dos pasos para todos los usuarios.
- Solo un usuario que haya habilitado la verificación en dos pasos para su propia cuenta puede habilitar la opción de verificación en dos pasos para todos los usuarios.
- Solo un usuario que haya habilitado la verificación en dos pasos para su propia cuenta puede excluir otras cuentas de usuario de la lista de verificación en dos pasos habilitada para todos los usuarios.
- Un usuario puede activar la verificación en dos pasos solo para su propia cuenta.
- Una cuenta de usuario que tiene el derecho Modificar las LCA de objetos en el área funcional **Características generales: permisos de usuario** y está conectado a Kaspersky Security Center 14 Web Console mediante la verificación en dos pasos puede deshabilitar la verificación en dos pasos: a) para cualquier otro usuario solo si la verificación en dos pasos para todos los usuarios está deshabilitada; b) para un usuario excluido de la lista de verificación en dos pasos que esté habilitada para todos los usuarios.
- Cualquier usuario que haya iniciado sesión en Kaspersky Security Center 14 Web Console mediante la verificación en dos pasos puede volver a emitir su clave secreta.
- Puede habilitar la opción de verificación en dos pasos para todos los usuarios para el Servidor de administración con el que está trabajando en un momento dado. Si activa esta opción en el Servidor de administración, también activa esta opción para las cuentas de usuario de sus Servidores de administración virtuales y no activa la verificación en dos pasos para las cuentas de usuario de los Servidores de administración secundarios.

Si la verificación en dos pasos está activada para una cuenta de usuario en el Servidor de administración de Kaspersky Security Center versión 13 o posterior, el usuario no podrá conectarse a las versiones 12, 12.1 o 12.2 de Kaspersky Security Center Web Console.

Activar la verificación en dos pasos para su propia cuenta

Puede activar la verificación en dos pasos solo para su propia cuenta.

Antes de activar la verificación en dos pasos para su cuenta, asegúrese de que haya una aplicación de autenticación instalada en su dispositivo móvil. Asegúrese de que la hora establecida en la aplicación de autenticación esté sincronizada con la hora establecida del dispositivo en el que se instaló el Servidor de administración.

Para activar la verificación en dos pasos en una cuenta de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Haga clic en el nombre de su cuenta.
3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.
4. En la pestaña **Protección de cuenta**:
   - Seleccione la opción **Solicitar nombre de usuario, contraseña y código de seguridad (verificación en dos pasos)** si desea habilitar la verificación en dos pasos para una cuenta de usuario:

- En la ventana de verificación en dos pasos que se abre, introduzca la clave secreta en la aplicación de autenticación o escanee el código QR y reciba un código de seguridad por única vez.

  Puede especificar la clave secreta en la aplicación de autenticación manualmente o escanear el código QR con su dispositivo móvil.

- En la ventana de verificación en dos pasos, especifique el código de seguridad generado por la aplicación de autenticación y luego haga clic en el botón **Comprobar y aplicar**.

5. Haga clic en el botón **Guardar**.

La verificación en dos pasos queda activada para su cuenta.

Activación de la verificación en dos pasos para todos los usuarios

Puede activar la verificación en dos pasos para todos los usuarios del Servidor de administración si su cuenta tiene el derecho Modificar ACL de objetos en el área funcional **Funciones generales: Permisos de usuario** y si está autenticado mediante la verificación en dos pasos. Si no habilitó la verificación en dos pasos para su cuenta antes de habilitarla para todos los usuarios, la aplicación abre la ventana para habilitar la verificación en dos pasos para su propia cuenta.

Para activar la verificación en dos pasos para todos los usuarios:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de la autenticación** de la ventana de propiedades, deslice el botón de alternancia de la opción **verificación en dos pasos para todos los usuarios** a la posición "activada".

La verificación en dos pasos queda activada para todos los usuarios. A partir de ahora, los usuarios del Servidor de Administración, incluidos los usuarios que se agregaron después de activar la verificación en dos pasos, tienen que configurar la verificación en dos pasos para sus cuentas. La excepción son los usuarios cuyas cuentas estén excluidas de la verificación en dos pasos.

Desactivación de la verificación en dos pasos de una cuenta de usuario

Puede desactivar la verificación en dos pasos para su propia cuenta, así como para la cuenta de cualquier otro usuario.

Puede desactivar la verificación en dos pasos de la cuenta de otro usuario si su cuenta tiene el derecho Modificar LCA de objeto del área funcional **Características generales: Permisos de usuario**.

Para desactivar la verificación en dos pasos de una cuenta de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.

2. Haga clic en el nombre de la cuenta de usuario interno para la que desea desactivar la verificación en dos pasos. Esta puede ser su propia cuenta o la cuenta de cualquier otro usuario.

3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.

4. En la pestaña **Protección de cuenta**, seleccione la opción **Solicitar solo nombre de usuario y contraseña** si desea desactivar la verificación en dos pasos para una cuenta de usuario.

5. Haga clic en el botón **Guardar**.

La verificación en dos pasos queda desactivada para la cuenta de usuario.

Desactivar la verificación en dos pasos para todos los usuarios

Puede desactivar la verificación en dos pasos para todos los usuarios si la verificación en dos pasos está activada para su cuenta y su cuenta tiene el derecho Modificar LCA de objetos en el área funcional **Características generales: permisos de usuario**. Si la verificación en dos pasos no está habilitada para su cuenta, debe activar la verificación en dos pasos para su cuenta antes de desactivarla para todos los usuarios.

Para desactivar la verificación en dos pasos para todos los usuarios:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Seguridad de la autenticación** de la ventana de propiedades, deslice el botón de alternancia de la opción **verificación en dos pasos para todos los usuarios** a la posición "desactivada".

3. Introduzca las credenciales de su cuenta en la ventana de autenticación.

La verificación en dos pasos queda desactivada para todos los usuarios.

Exclusión de cuentas de la verificación en dos pasos

Puede excluir cuentas de usuario de la verificación en dos pasos si tiene el derecho Modificar LCA de objeto en el área funcional **Características generales: permisos de usuario**.

Si una cuenta de usuario se excluye de la lista de verificación en dos pasos para todos los usuarios, este usuario no tiene que utilizar la verificación en dos pasos.

> Puede ser necesario excluir cuentas de la verificación en dos pasos para las cuentas de servicio que no pueden pasar el código de seguridad durante la autenticación.

Si desea excluir algunas cuentas de usuario de la verificación en dos pasos, haga lo siguiente:

1. Debe realizar un sondeo de Active Directory para actualizar la lista de usuarios del Servidor de administración si desea excluir cuentas de Active Directory.

2. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

3. En la pestaña **Seguridad de la autenticación** de la ventana de propiedades, en la tabla de exclusiones de la verificación de dos pasos, haga clic en el botón **Añadir**.

4. En la ventana que se abre:

   a. Seleccione las cuentas de usuario que desea excluir.

   b. Haga clic en el botón **Aceptar**.

Las cuentas de usuario seleccionadas se excluyen de la verificación en dos pasos.

Generar una nueva clave secreta

Puede generar una nueva clave secreta para una verificación en dos pasos para su cuenta solo si está autorizado mediante la verificación en dos pasos.

Para generar una nueva clave secreta para una cuenta de usuario, haga lo siguiente:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES → USUARIOS**.

2. Haga clic en el nombre de la cuenta de usuario para la que desea generar una nueva clave secreta para la verificación en dos pasos.

3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.

4. En la pestaña **Protección de cuenta**, haga clic en el enlace **Generar una nueva clave secreta**.

5. En la ventana de verificación en dos pasos que se abre, especifique una nueva clave de seguridad generada por la aplicación de autenticación.

6. Haga clic en el botón **Comprobar y aplicar**.

Se genera una nueva clave secreta para el usuario.

Si pierde su dispositivo móvil, puede instalar una aplicación de autenticación en otro dispositivo móvil y generar una nueva clave secreta para restaurar el acceso a Kaspersky Security Center 14 Web Console.

Modificar el nombre de un emisor del código de seguridad

Puede tener varios identificadores (se denominan emisores) para diferentes Servidores de administración. Puede cambiar el nombre de un emisor de código de seguridad en el caso de que, por ejemplo, el Servidor de administración ya utilice un nombre similar de emisor de código de seguridad para otro Servidor de administración. De forma predeterminada, el nombre del emisor del código de seguridad es el mismo que el del Servidor de administración.

> Después de cambiar el nombre del emisor del código de seguridad, debe volver a emitir una nueva clave secreta y pasarla a la aplicación de autenticación.

Para especificar un nuevo nombre de emisor del código de seguridad:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Protección de cuenta**.

3. En la pestaña **Protección de cuenta**, haga clic en el enlace **Editar**.

   Se abre la sección **Editar emisor del código de seguridad.**

4. Especifique el nuevo nombre de emisor de código de seguridad.

5. Haga clic en el botón **Aceptar**.

Se especifica un nuevo nombre de emisor de código de seguridad para el Servidor de administración.

Creación de copias de seguridad y restauración de los datos del Servidor de administración

La copia de seguridad de datos permite trasladar un Servidor de administración de un dispositivo a otro sin perder los datos. Mediante la copia de seguridad, puede restaurar datos cuando traslada la base de datos de un Servidor de administración a otro dispositivo o cuando se pasa a una nueva versión de Kaspersky Security Center.

Puede crear una copia de seguridad de los datos del Servidor de administración mediante uno de los siguientes métodos:

- Creando y ejecutando una tarea de creación de copias de seguridad de datos mediante la Consola de administración.
- Ejecutando la utilidad klbackup en el dispositivo que tenga instalado el Servidor de administración. La utilidad se incluye en el kit de distribución de Kaspersky Security Center. Después de la instalación del Servidor de administración, la utilidad se ubica en la raíz de la carpeta de destino especificada durante la instalación de la aplicación.

Los siguientes datos se guardan en la copia de seguridad del Servidor de administración:

- Base de datos del Servidor de administración (directivas, tareas, parámetros de la aplicación, eventos guardados en el Servidor de administración).
- Información de configuración de la estructura de los grupos de administración y los dispositivos cliente.
- Repositorio de paquetes de distribución de aplicaciones para la instalación remota.
- Certificado del Servidor de administración.

La recuperación de datos del Servidor de administración solo es posible mediante la utilidad klbackup.

Creación de una tarea de copia de seguridad

Las tareas de creación de copias de seguridad son tareas del Servidor de administración creadas por el Asistente de inicio rápido. Si se ha eliminado una tarea de creación de copias de seguridad creada por el Asistente de inicio rápido, puede crear una manualmente.

Para crear una tarea de creación de copias de seguridad de los datos del Servidor de administración:

1. En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en el botón **Añadir**.

   Se inicia **Asistente para añadir tarea**.
3. En la ventana **Nueva tarea** del Asistente, seleccione el tipo de tarea **Copia de seguridad de los datos del Servidor de administración**.
4. Siga el resto de instrucciones del Asistente.

Solo se puede crear un ejemplar de la tarea **Copia de seguridad de los datos del Servidor de administración**. Si la tarea de creación de copias de seguridad de los datos del Servidor de administración ya se ha creado, no aparecerá en la ventana de selección de tipo de tarea del Asistente para crear tareas de copia de seguridad.

Despliegue de aplicaciones de Kaspersky a través de Kaspersky Security Center 14 Web Console

Esta sección describe cómo desplegar aplicaciones de Kaspersky en dispositivos cliente de su organización por medio de Kaspersky Security Center 14 Web Console.

Escenario: Despliegue de aplicaciones de Kaspersky a través de Kaspersky Security Center 14 Web Console

Este escenario explica cómo desplegar aplicaciones de Kaspersky mediante Kaspersky Security Center 14 Web Console. Puede utilizar el Asistente de inicio rápido y el Asistente de despliegue de la protección, o puede completar todos los pasos necesarios manualmente.

Requisitos previos

Las siguientes aplicaciones están disponibles para el despliegue a través de Kaspersky Security Center 14 Web Console:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux

El despliegue de las aplicaciones de Kaspersky se realiza en etapas:

1. **Descargar complemento de administración para la aplicación**

   Esta etapa forma parte del Asistente de inicio rápido. Si elige no ejecutar el Asistente, descargue el complemento para Kaspersky Endpoint Security para Windows manualmente.

Si planea administrar dispositivos móviles corporativos, siga las instrucciones proporcionadas en la Ayuda de Kaspersky Security para dispositivos móviles para descargar e instalar los complementos de administración de Kaspersky Endpoint Security for Android.

2. **Descarga y creación de paquetes de instalación**

Esta etapa forma parte del Asistente de inicio rápido.

El Asistente de inicio rápido le permite descargar el paquete de instalación con el complemento de administración. Si no seleccionó esta opción al ejecutar el Asistente o si no lo hizo, debe descargar el paquete manualmente.

Si no puede instalar las aplicaciones de Kaspersky mediante Kaspersky Security Center en algunos dispositivos, (por ejemplo, en dispositivos de empleados remotos) puede crear paquetes de instalación independientes para las aplicaciones. Si utiliza paquetes independientes para instalar aplicaciones de Kaspersky, no tiene que crear y ejecutar una tarea de instalación remota, ni crear y configurar tareas para Kaspersky Endpoint Security para Windows.

3. **Creación, configuración y ejecución de la tarea de instalación remota**

Para Kaspersky Endpoint Security para Windows, esta etapa es parte del Asistente de despliegue de la protección, que se inicia automáticamente una vez que el Asistente de inicio rápido ha finalizado. Si decide no ejecutar el Asistente de despliegue de la protección, debe crear esta tarea manualmente y configurarla manualmente.

También puede crear manualmente varias tareas de instalación remotas para grupos de administración diferentes o selecciones de dispositivos diferentes. Puede desplegar diferentes versiones de una aplicación en estas tareas.

Asegúrese de que se hayan detectado todos los dispositivos en su red; a continuación, ejecute la tarea (o tareas) de instalación remota.

> Si desea instalar Agente de red en dispositivos con el sistema operativo SUSE Linux Enterprise Server 15, instale el paquete insserv-compat primero para configurar el Agente de red.

4. **Creación y configuración de tareas para la aplicación administrada**

La *tarea Instalar actualización* de Kaspersky Endpoint Security para Windows debe estar configurada.

Esta etapa forma parte del Asistente de inicio rápido: la tarea se crea y configura automáticamente con la configuración predeterminada. Si no ejecutó el Asistente, debe crear esta tarea manualmente y configurarlas manualmente. Si utiliza el Asistente de inicio rápido, asegúrese de que la programación de la tarea cumpla con sus requisitos. (De forma predeterminada, el inicio programado para la tarea se establece en **Manualmente**, pero es posible que desee elegir otra opción).

Otras aplicaciones de Kaspersky podrían tener otras tareas predeterminadas. Por favor, consulte la documentación de las aplicaciones correspondientes para más información.

Asegúrese de que la programación para cada tarea que crea que cumpla con sus requisitos.

5. **Instalación de Kaspersky Security for Mobile (opcional)**

Si planea administrar dispositivos móviles corporativos, siga las instrucciones proporcionadas en la Ayuda de Kaspersky Security para dispositivos móviles para obtener información sobre la implementación de Kaspersky Endpoint Security for Android.

6. **Creación de directivas**

Cree la directiva para cada aplicación manualmente o (en el caso de Kaspersky Endpoint Security para Windows) a través del Asistente de inicio rápido. Puede utilizar la configuración predeterminada de la directiva; también puede modificar la configuración predeterminada de la directiva de acuerdo con sus necesidades en cualquier momento.

7. **Verificación de los resultados**

Asegúrese de que el despliegue se completó correctamente: tiene directivas y tareas para cada aplicación y estas aplicaciones están instaladas en los dispositivos administrados.

Resultados

Al completar el escenario se obtienen los siguientes resultados:

- Se crean todas las directivas y tareas necesarias para las aplicaciones seleccionadas.
- Los horarios de las tareas se configuran de acuerdo a sus necesidades.
- Las aplicaciones seleccionadas se despliegan o programan para desplegarse en los dispositivos cliente seleccionados.

La adquisición de complementos para aplicaciones de Kaspersky

Para desplegar una aplicación Kaspersky, como Kaspersky Endpoint Security para Windows, debe descargar el complemento de administración de la aplicación.

Para descargar un complemento de administración para una aplicación de Kaspersky:

1. En la lista desplegable **Configuración de la consola**, seleccione **Complementos web**.
2. En la ventana que se abre, haga clic en el botón **Añadir**.

   Se muestra una lista de complementos disponibles.
3. En la lista de complementos disponibles, seleccione el complemento que desea descargar (por ejemplo, Kaspersky Endpoint Security 11 para Windows) haciendo clic en su nombre.

   Se muestra una página de descripción del complemento.
4. En la página de descripción del complemento, haga clic en **Instalar complemento**.
5. Cuando la instalación se haya completado, haga clic en **Aceptar**.

El complemento de administración se descarga con la configuración predeterminada y se muestra en la lista de complementos de administración.

Puede añadir complementos y actualizar los complementos descargados desde un archivo. Puede descargar complementos de administración y complementos de administración web de la Página web del Servicio de soporte técnico de Kaspersky.

Para descargar o actualizar complementos desde un archivo, siga estos pasos:

1. En la lista desplegable **Configuración de la consola**, seleccione **Complementos web**.
2. Especifique el archivo del complemento y la firma del archivo:
   - Haga clic en **Añadir desde archivo** para descargar un complemento desde un archivo.
   - Haga clic en **Actualizar desde archivo** para descargar la actualización de un complemento desde un archivo.

3. Especifique el archivo y la firma del archivo.

4. Descargue los archivos especificados.

El complemento de administración se descarga del archivo y se muestra en la lista de complementos de administración.

Descargar y crear paquetes de instalación para aplicaciones de Kaspersky

Puede crear paquetes de instalación para aplicaciones de Kaspersky desde los servidores web de Kaspersky si su Servidor de administración tiene acceso a Internet.

Para descargar y crear un paquete de instalación para una aplicación de Kaspersky:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**.
   - En el menú principal, vaya a **OPERACIONES → REPOSITORIOS → PAQUETES DE INSTALACIÓN**.

   También puede ver las notificaciones sobre los nuevos paquetes para las aplicaciones de Kaspersky en la lista de notificaciones en pantalla. Si hay notificaciones sobre un nuevo paquete, puede hacer clic en el enlace junto a la notificación y pasar a la lista de paquetes de instalación disponibles.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en **Añadir**.

   Se inicia el Asistente de nuevo paquete. Avance a través del Asistente utilizando el botón **Siguiente**.

3. En la primera página del Asistente, seleccione la opción **Crear un paquete de instalación para una aplicación de Kaspersky**.

   Aparece una lista con los paquetes de instalación disponibles en los servidores web de Kaspersky. La lista contiene paquetes de instalación solo para aquellas aplicaciones que son compatibles con la versión actual de Kaspersky Security Center.

4. Haga clic en el nombre de un paquete de instalación, por ejemplo, Kaspersky Endpoint Security para Windows (11.1.0).

   Se abrirá una ventana con información sobre el paquete de instalación.

5. Lea la información y haga clic en el botón **Descargar y crear paquete de instalación**.

   Si un paquete de distribución no se puede convertir en un paquete de instalación, se mostrará el botón **Descargar el paquete de distribución** en lugar de **Descargar y crear paquete de instalación**.

   Se inicia la descarga del paquete de instalación en el Servidor de administración. Puede cerrar la ventana del Asistente o continuar con el siguiente paso de la instrucción. Si cierra la ventana del Asistente, el proceso de descarga continuará en segundo plano.

   Si desea realizar un seguimiento del proceso de descarga de un paquete de instalación:

   a. En el menú principal, vaya a **OPERACIONES → REPOSITORIOS → PAQUETES DE INSTALACIÓN → En curso ()**.

b. Siga el progreso de la operación en la columna **Progreso de la descarga** y la columna **Estado de la descarga** de la tabla.

Cuando se completa el proceso, el paquete de instalación se añade a la lista en la pestaña **Descargados**. Si el proceso de descarga se detiene y el estado de descarga cambia a **Aceptar EULA**, haga clic en el nombre del paquete de instalación y luego continúe con el siguiente paso de la instrucción.

Si el tamaño de los datos contenidos en el paquete de distribución seleccionado excede el límite actual, se muestra un mensaje de error. Puede cambiar el valor límite y luego continuar con la creación del paquete de instalación.

6. Para algunas aplicaciones de Kaspersky, durante el proceso de descarga se muestra el botón **Mostrar el EULA**. Si se muestra, haga lo siguiente:

   a. Haga clic en el botón **Mostrar el EULA** para leer el Contrato de licencia de usuario final (EULA).

   b. Lea el EULA que se muestra en la pantalla y haga clic en **Aceptar**.

   La descarga continúa después de que acepte el EULA. Si hace clic en **Rechazar**, la descarga se detiene.

7. Cuando la descarga se haya completado, haga clic en el botón **Cerrar**.

El paquete de instalación seleccionado se descarga a la carpeta compartida del Servidor de administración, en la subcarpeta de Paquetes. Una vez descargado, el paquete de instalación se muestra en la lista de paquetes de instalación.

Cambio del límite del tamaño de los datos del paquete de instalación personalizada

El tamaño total de los datos desempaquetados durante la creación de un paquete de instalación personalizado es limitado. El límite predeterminado es de 1 GB.

Si intenta cargar un archivo que contiene datos que exceden el límite actual, se muestra un mensaje de error. Es posible que tenga que aumentar este valor límite al crear paquetes de instalación a partir de paquetes de distribución grandes.

Para cambiar el valor límite del tamaño del paquete de instalación personalizado:

1. Abra el registro del sistema del dispositivo del Servidor de administración (por ejemplo, localmente, mediante el comando `regedit` del menú **Iniciar** → **Ejecutar**).

2. Vaya al subárbol HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlag

3. Haga clic derecho en el subárbol y luego seleccione **Nuevo** → **Valor DWORD (32 bits)**.

   Se crea una nueva clave DWORD.

4. Asigne a la clave el nombre MaxArchivePkgSize.

5. Haga doble clic en la nueva clave DWORD para editarla.

6. Establezca el valor límite requerido:

a. Seleccione cualquier base: hexadecimal o decimal.

b. Especifique el número de bytes correspondientes a la base seleccionada.

Por ejemplo, si el límite requerido es de 2 GB, puede especificar el valor decimal 2147483648 o el valor hexadecimal 0x80000000.

7. Haga clic en **Aceptar**.

Se cambia el límite del tamaño de los datos del paquete de instalación personalizada.

Descarga de paquetes de distribución para aplicaciones de Kaspersky

En Kaspersky Security Center 14 Web Console, puede descargar y guardar paquetes de distribución para las aplicaciones de Kaspersky. Puede usar los paquetes de distribución para instalar las aplicaciones manualmente, sin usar Kaspersky Security Center.

Para descargar y guardar paquetes de distribución para aplicaciones de Kaspersky:

1. En la pestaña **Operaciones**, seleccione **aplicaciones de Kaspersky → Versiones de aplicación actuales**.

   Se abrirá la lista de paquetes de distribución, complementos y parches disponibles. Kaspersky Security Center muestra solo los elementos que son compatibles con su versión actual.

2. En la lista, haga clic en el nombre del paquete que desea descargar.

   Se abre la descripción del paquete.

3. Lea la descripción y haga clic en el botón **Descargar y crear paquete de instalación**.

   Si un paquete de distribución no se puede convertir en un paquete de instalación, se mostrará el botón **Descargar el paquete de distribución** en lugar de **Descargar y crear paquete de instalación**.

   Se inicia la descarga del paquete de instalación en el Servidor de administración.

El paquete de instalación o distribución seleccionado se descarga a la carpeta compartida del Servidor de administración, en la subcarpeta de **Packages**. Después de descargarlo, el paquete de instalación se muestra en la lista de paquetes de instalación.

Comprobación de la correcta instalación de Kaspersky Endpoint Security para Windows

Para asegurarse de que ha desplegado correctamente las aplicaciones de Kaspersky, como Kaspersky Endpoint Security:

1. Con Kaspersky Security Center 14 Web Console, asegúrese de tener lo siguiente:

   - Una directiva para Kaspersky Endpoint Security y/u otras aplicaciones de seguridad que utilice.
   - Tareas para Kaspersky Endpoint Security para Windows: tarea Análisis antivirus rápido y tarea *Instalar actualización* (si utiliza Kaspersky Endpoint Security para Windows).
   - Las tareas para otras aplicaciones de seguridad que utiliza.

2. En uno de los dispositivos administrados seleccionados para la instalación, asegúrese de lo siguiente:

   - Kaspersky Endpoint Security u otra aplicación de seguridad de Kaspersky está instalada.
   - En Kaspersky Endpoint Security, la Protección frente a amenazas en archivos, la Protección frente a amenazas web y la Protección frente a amenazas en el correo coinciden con la directiva que creó para este dispositivo.
   - El servicio Kaspersky Endpoint Security se puede detener e iniciar manualmente.
   - Las tareas de grupo se pueden detener e iniciar manualmente.

Crear paquetes de instalación independientes.

Usted y los usuarios de dispositivos de su organización pueden utilizar paquetes de instalación independientes para instalar aplicaciones en dispositivos de forma manual.

Un paquete de instalación independiente es un archivo ejecutable (installer.exe) que puede almacenar en el servidor web, en una carpeta compartida, enviar por correo electrónico o transferir al dispositivo cliente de otra manera. En el dispositivo cliente, el usuario puede ejecutar el archivo recibido localmente para instalar una aplicación sin utilizar Kaspersky Security Center. Puede crear paquetes de instalación independientes de aplicaciones de Kaspersky y de aplicaciones de terceros para plataformas Windows, macOS y Linux. Para crear un paquete de instalación independiente para una aplicación de terceros, debe crear un paquete de instalación personalizada.

Asegúrese de que el paquete de instalación independiente no esté disponible para personas no autorizadas.

Para crear un paquete de instalación independiente:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**.
   - En el menú principal, vaya a **OPERACIONES → REPOSITORIOS → PAQUETES DE INSTALACIÓN**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. En la lista de paquetes de instalación, seleccione un paquete de instalación y, encima de la lista, haga clic en el botón **Desplegar**.

3. Seleccione la opción **Mediante un paquete independiente**.

   Se inicia el Asistente para crear paquete de instalación independiente. Avance a través del Asistente utilizando el botón **Siguiente**.

4. En la primera página del Asistente, asegúrese de seleccionar la opción **Instalar Agente de red junto con esta aplicación** si desea instalar el Agente de red junto con la aplicación seleccionada.

   Esta opción está activada de forma predeterminada. Le recomendamos que active esta opción si no sabe si el Agente de red está instalado en el dispositivo. Si el Agente de red ya está instalado en el dispositivo, una vez que instale el paquete de instalación independiente con el Agente de red, este último se actualizará a la versión más reciente.

   Si desactiva esta opción, el Agente de red no se instalará en el dispositivo y este quedará no administrado.

Si la aplicación seleccionada ya cuenta con un paquete de instalación independiente en el Servidor de administración, el Asistente se lo informa. En este caso, debe seleccionar una de las siguientes acciones:

- **Crear un paquete de instalación independiente**. Seleccione esta opción si, por ejemplo, desea crear un paquete de instalación independiente para una nueva versión de la aplicación y también conservar un paquete de instalación independiente que haya creado para una versión de la aplicación anterior. El nuevo paquete de instalación independiente se ubicará en otra carpeta.

- **Utilizar paquete de instalación independiente existente**. Seleccione esta opción si desea utilizar un paquete de instalación independiente existente. El proceso para crear paquetes no se iniciará.

- **Crear de nuevo un paquete de instalación independiente existente**. Seleccione esta opción si desea volver a crear un paquete de instalación independiente para la misma aplicación. El paquete de instalación independiente se ubicará en la misma carpeta.

5. En la página del Asistente **Mover a lista de dispositivos administrados**, la opción **No mover dispositivos** está activada de forma predeterminada. Si no desea mover el dispositivo cliente a ningún grupo de administración después de la instalación del Agente de red, deje activada esta opción.

   Si desea mover el dispositivo cliente después de la instalación del Agente de red, seleccione la opción **Mover dispositivos no asignados a este grupo** y especifique el grupo de administración al que desea mover el dispositivo cliente. De manera predeterminada, el dispositivo se mueve al grupo de **Dispositivos administrados**.

6. En la página siguiente del Asistente, cuando haya finalizado el proceso de creación del paquete de instalación independiente, haga clic en el botón **FINALIZAR**.

   Asistente para crear paquete de instalación independiente se cierra.

Se crea el paquete de instalación independiente y se lo ubica en la subcarpeta PkgInst de la carpeta compartida del Servidor de administración. Puede ver la lista de paquetes independientes si hace clic en el botón **Ver la lista de paquetes independientes** que se encuentra encima de la lista de paquetes de instalación.

Ver la lista de paquetes de instalación independientes

Puede ver la lista de paquetes de instalación independiente y las propiedades de cada paquete de instalación independiente.

Para ver la lista de paquetes de instalación independientes para todos los paquetes de instalación:

Encima de la lista, haga clic en el botón **Ver la lista de paquetes independientes**.

En la lista de paquetes de instalación independientes, se muestran las siguientes propiedades:

- **Nombre del paquete**. Nombre del paquete de instalación independiente que se forma automáticamente como el nombre de la aplicación incluida en el paquete y la versión de la aplicación.

- **Nombre de la aplicación**. Nombre de la aplicación que se incluye en el paquete de instalación independiente.

- **Versión de la aplicación**.

- **Nombre del paquete de instalación del Agente de red**. La propiedad se muestra solo si el Agente de red está incluido en el paquete de instalación independiente.

- **Versión del Agente de red**. La propiedad se muestra solo si el Agente de red está incluido en el paquete de instalación independiente.

- **Tamaño**. Tamaño de RAM, en MB.
- **Grupo**. Nombre del grupo al que se mueve el dispositivo cliente después de la instalación del Agente de red.
- **Creado**. Fecha y hora de la creación del paquete de instalación independiente.
- **Modificado**. Fecha y hora de la modificación del paquete de instalación independiente.
- **Ruta**. Ruta completa a la carpeta donde se ubica el paquete de instalación independiente.
- **Dirección web**. Dirección web de la ubicación del paquete de instalación independiente.
- **Archivo hash**. La propiedad se utiliza para certificar que el paquete de instalación independiente no fue modificado por terceros y que un usuario tiene el mismo archivo que usted creó y transfirió al usuario.

Para ver la lista de paquetes de instalación independientes para determinados paquetes de instalación:

Seleccione el paquete de instalación en la lista y, encima de esta, haga clic en el botón **Ver la lista de paquetes independientes**.

En la lista de paquetes de instalación independientes puede:

- Publicar un paquete de instalación independiente en el servidor web si hace clic en el botón **Publicar**. El paquete de instalación independiente publicado queda disponible para que lo descarguen los usuarios a quienes ha enviado el enlace a dicho paquete.
- Cancelar la publicación de un paquete de instalación independiente en el servidor web si hace clic en el botón **Anular la publicación**. El paquete de instalación independiente que no se publica estará disponible solo para que usted y otros administradores lo descarguen.
- Descargar un paquete de instalación independiente en su dispositivo haciendo clic en el botón **Descargar**.
- Enviar un correo electrónico con el enlace a un paquete de instalación independiente si hace clic en el botón **Enviar por correo electrónico**.
- Eliminar un paquete de instalación independiente haciendo clic en el botón **Eliminar**.

Crear paquetes de instalación personalizada

Puede utilizar paquetes de instalación personalizada para hacer lo siguiente:

- Para instalar cualquier aplicación (como un editor de texto) en un dispositivo cliente, por ejemplo, mediante una tarea.
- Para crear un paquete de instalación independiente.

Un paquete de instalación personalizada es una carpeta con un conjunto de archivos. La fuente para crear un paquete de instalación personalizada es un *archivo de almacenamiento*. El archivo de almacenamiento contiene un archivo o archivos que deben incluirse en el paquete de instalación personalizada. Al crear un paquete de instalación personalizada, puede especificar parámetros de línea de comandos, por ejemplo, para instalar la aplicación en modo silencioso.

Si tiene una clave de licencia activa para la función Administración de vulnerabilidades y parches (VAPM), puede convertir su configuración de instalación predeterminada para el paquete de instalación personalizada relevante y usar los valores recomendados por los expertos de Kaspersky. La configuración se convierte automáticamente durante la creación del paquete de instalación personalizada solo si el archivo ejecutable correspondiente está incluido en la base de datos de Kaspersky de aplicaciones de terceros.

Para crear un paquete de instalación personalizada:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**.
   - En el menú principal, vaya a **OPERACIONES → REPOSITORIOS → PAQUETES DE INSTALACIÓN**.

   Se muestra una lista de paquetes de instalación disponibles en el Servidor de administración.

2. Haga clic en **Añadir**.

   Se inicia el Asistente de nuevo paquete. Avance a través del Asistente utilizando el botón **Siguiente**.

3. En la primera página del Asistente, seleccione la opción **Crear un paquete de instalación a partir de un archivo**.

4. En la siguiente página del Asistente, especifique el nombre del paquete y haga clic en el botón **Examinar**.

   Se abre una ventana **Abrir** estándar de Windows en el navegador que le permite escoger un archivo para crear el paquete de instalación.

5. Seleccione un archivo de almacenamiento ubicado en los discos disponibles.

   Puede cargar un archivo comprimido ZIP, CAB, TAR o TAR.GZ. No es posible crear un paquete de instalación desde un archivo SFX (archivo autoextraíble).

   Si desea que la configuración se convierta durante la instalación del paquete, asegúrese de que la casilla de verificación **Convertir la configuración a los valores recomendados para las aplicaciones reconocidas por Kaspersky Security Center una vez que finalice el Asistente** esté seleccionada y luego haga clic en **Siguiente**.

   Se inicia la carga de archivos al Servidor de administración de Kaspersky Security Center 14.

   Si habilitó el uso de la configuración de instalación recomendada, Kaspersky Security Center 14 verifica si el archivo ejecutable está incluido en la base de datos de Kaspersky de aplicaciones de terceros. Si la verificación se realiza correctamente, recibirá una notificación que le informará que se reconoce el archivo. La configuración se convierte y se crea el paquete de instalación personalizada. No se requieren más acciones. Haga clic en el botón **Finalizar** para cerrar el Asistente.

6. En la página siguiente del Asistente, seleccione un archivo (de la lista de archivos extraídos del archivo de almacenamiento seleccionado) y especifique los parámetros de la línea de comandos de un archivo ejecutable.

   Puede especificar parámetros de línea de comandos para instalar la aplicación desde el paquete de instalación en modo silencioso. La especificación de los parámetros de la línea de comandos es opcional.

   Se inicia el proceso para crear el paquete de instalación.

   El Asistente le informa cuando finaliza el proceso.

Si no se crea el paquete de instalación, se muestra el mensaje adecuado.

7. Haga clic en el botón **Finalizar** para cerrar el Asistente.

El paquete de instalación que ha creado se descarga en la subcarpeta Paquetes de la carpeta compartida del Servidor de administración. Después de la descarga, el paquete de instalación aparece en la lista de paquetes de instalación.

En la lista de paquetes de instalación disponibles en el Servidor de administración, al hacer clic en el enlace con el nombre de un paquete de instalación personalizado, puede hacer lo siguiente:

- Ver las siguientes propiedades de un paquete de instalación:
  - **Nombre**. Nombre del paquete de instalación personalizado.
  - **Origen**. Nombre del proveedor de la aplicación.
  - **Aplicación**. Nombre de la aplicación empaquetada en el paquete de instalación personalizado.
  - **Versión**. Versión de la aplicación.
  - **Idioma**. Idioma de la aplicación empaquetada en el paquete de instalación personalizado.
  - **Tamaño (MB)**. Tamaño del paquete de instalación.
  - **Sistema operativo**. Tipo de sistema operativo para el que está destinado el paquete de instalación.
  - **Creado**. Fecha de creación del paquete de instalación.
  - **Modificado**. Fecha de modificación del paquete de instalación.
  - **Tipo**. Tipo del paquete de instalación.
- Cambiar el nombre del paquete y los parámetros de la línea de comandos. Esta función está disponible únicamente para los paquetes que no se crean sobre la base de las aplicaciones de Kaspersky.

Si ha convertido la configuración de instalación del paquete a los valores recomendados para el proceso de creación del paquete personalizado, pueden aparecer dos secciones adicionales en la pestaña **Configuración** de las propiedades del paquete de instalación personalizada: **Configuración** y **Proceso de instalación**.

La sección **Configuración** contiene las siguientes propiedades, que se muestran en una tabla:

- **Nombre**. Esta columna muestra el nombre asignado a un parámetro de instalación.
- **Tipo**. Esta columna muestra el tipo de parámetro de instalación.
- **Valor**. Esta columna muestra el tipo de datos definidos por un parámetro de instalación (Bool, Filepath, Numeric, Path, o String).

La sección **Proceso de instalación** contiene una tabla que describe las siguientes propiedades de la actualización incluida en el paquete de instalación personalizada:

- **Nombre**. El nombre de la clave.

- **Descripción**. La descripción de la actualización.
- **Fuente**. El origen de la actualización, es decir, si fue lanzada por Microsoft o por un otro desarrollador externo.
- **Tipo**. El tipo de actualización, es decir, si está destinada a un controlador o una aplicación.
- **Categoría**. La categoría de servicios de actualización de Windows Server (WSUS) que se muestra para las actualizaciones de Microsoft (actualizaciones críticas, actualizaciones de definiciones, controladores, paquetes de características, actualizaciones de seguridad, paquetes de servicios, herramientas, paquetes acumulativos de actualizaciones, actualizaciones o paso a nueva versión).
- **Nivel de importancia según MSRC**. El nivel de importancia de la actualización definido por Microsoft Security Response Center (MSRC).
- **Nivel de importancia** El nivel de importancia de la actualización definido por Kaspersky.
- **Nivel de importancia del parche (para parches destinados a aplicaciones de Kaspersky)**. El nivel de importancia del parche, si está destinado a una aplicación de Kaspersky.
- **Articulo**. El identificador (id.) del artículo de la Base de conocimientos que describe la actualización.
- **Boletín**. El id. del boletín de seguridad que describe la actualización.
- **No asignado para instalación**. Muestra si la actualización tiene el estado No asignado para instalación.
- **Para instalar**. Muestra si la actualización tiene el estado Para instalar.
- **Instalando**. Muestra si la actualización tiene el estado Instalando.
- **Instalada**. Muestra si la actualización tiene el estado Instalada.
- **Fallo**. Muestra si la actualización tiene el estado Fallo.
- **Se requiere reiniciar**. Muestra si la actualización tiene el estado Se requiere reiniciar.
- **Registrada**. Muestra la fecha y hora en que se registró la actualización.
- **Instalación en modo interactivo**. Muestra si la actualización requiere interactuar con el usuario durante la instalación.
- **Revocada**. Muestra la fecha y hora en que se revocó la actualización.
- **Estado de aprobación de la actualización**. Muestra si la actualización está aprobada para su instalación.
- **Revisión**. Muestra el número de revisión actual de la actualización.
- **Id. de la actualización**. Muestra el id. de la actualización.
- **Versión de la aplicación**. Muestra el número de versión al que se actualizará la aplicación.
- **Reemplazos**. Muestra otras actualizaciones que pueden reemplazar a la actualización.
- **Reemplazadas**. Muestra otras actualizaciones que pueden ser reemplazadas por la actualización.
- **Debe aceptar los términos del Contrato de licencia**. Muestra si la actualización requiere la aceptación de los términos de un Contrato de licencia de usuario final (EULA).

- **Proveedor**. Muestra el nombre del proveedor de actualizaciones.
- **Familia de aplicaciones**. Muestra el nombre de la familia de aplicaciones a la que pertenece la actualización.
- **Aplicación**. Muestra el nombre de la aplicación a la que pertenece la actualización.
- **Idioma**. Muestra el idioma de la localización de la actualización.
- **No asignado para instalación (nueva versión)**. Muestra si la actualización tiene el estado No asignado para instalación (nueva versión).
- **Requiere la instalación de requisitos previos**. Muestra si la actualización tiene el estado de instalación Requiere la instalación de requisitos previos.
- **Modo de descarga**. Muestra el modo de descarga de la actualización.
- **Es un parche**. Muestra si la actualización es un parche.
- **No instalada**. Muestra si la actualización tiene el estado No instalada.

Especificación de la configuración para la instalación remota en dispositivos Unix

Cuando instala una aplicación en un dispositivo Unix mediante una tarea de instalación remota, puede especificar la configuración específica de Unix para la tarea. Esta configuración está disponible en las propiedades de la tarea después de que se crea la tarea.

Para especificar la configuración específica de Unix para una tarea de instalación remota, haga lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en el nombre de la tarea de instalación remota para la que desea especificar la configuración específica de Unix.

   Se abrirá la ventana de propiedades de la tarea.
3. Vaya a **Configuración de la aplicación** → **Configuraciones específicas de Unix**.
4. Especifique los siguientes parámetros:
   - Establecer una contraseña para la cuenta raíz (solo para el despliegue a través de SSH)

     Si el comando `sudo` no se puede usar en el dispositivo de destino sin especificar la contraseña, seleccione esta opción y luego especifique la contraseña para la cuenta raíz. Kaspersky Security Center transmite la contraseña en forma cifrada al dispositivo de destino, descifra la contraseña y luego inicia el procedimiento de instalación en nombre de la cuenta raíz con la contraseña especificada.

     Kaspersky Security Center no utiliza la cuenta ni la contraseña especificada para crear una conexión SSH.
   - Especifique la ruta a la carpeta temporal con permisos de ejecución en el dispositivo de destino (solo para el despliegue a través de SSH)

Si el directorio /tmp en el dispositivo de destino no tiene el permiso de ejecución, seleccione esta opción y luego especifique la ruta al directorio con el permiso de ejecución. Kaspersky Security Center utiliza el directorio especificado como directorio temporal para acceder a través de SSH. La aplicación coloca el paquete de instalación en el directorio y ejecuta el procedimiento de instalación.

5. Haga clic en el botón **Guardar**.

La configuración de la tarea especificada se guarda.

Administración de dispositivos móviles

La administración de la protección de dispositivos móviles a través de Kaspersky Security Center se realiza mediante la función de administración de dispositivos móviles, que requiere una licencia dedicada. Si tiene la intención de administrar dispositivos móviles que son propiedad de los empleados de su organización, active y configure la Administración de dispositivos móviles.

La administración de dispositivos móviles le permite administrar los dispositivos Android de los empleados. La protección la proporciona la aplicación móvil Kaspersky Endpoint Security for Android instalada en los dispositivos. Esta aplicación móvil garantiza la protección de los dispositivos móviles contra las amenazas web, los virus y otros programas que suponen una amenaza. Para la administración centralizada a través de Kaspersky Security Center 14 Web Console, debe instalar los siguientes complementos de administración web en el dispositivo donde está instalado Kaspersky Security Center 14 Web Console:

- Complemento de Kaspersky Security for Mobile
- Complemento de Kaspersky Endpoint Security for Android

Para obtener información sobre el despliegue de la protección y la administración de los dispositivos móviles, consulte la Ayuda de Kaspersky Security for Mobile.

Modificación de la configuración de Administración de dispositivos móviles en Kaspersky Security Center 14 Web Console

Para modificar de la configuración de la Administración de dispositivos móviles:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Puertos adicionales**.

3. Modifique la configuración relevante:

   - **Abrir puerto para dispositivos móviles**

Si se selecciona esta opción, el puerto para dispositivos móviles se abrirá en el Servidor de administración.

Puede utilizar el puerto para dispositivos móviles solo si se encuentra instalado el componente de Administración de dispositivos móviles.

Si no se selecciona opción, no se utilizará el puerto para dispositivos móviles en el Servidor de administración.

Esta opción está desactivada de forma predeterminada.

- **Puerto para la sincronización de dispositivos móviles**

  Número del puerto que se utiliza para conectar dispositivos móviles al Servidor de administración. El número de puerto predeterminado es el 13292.

  Se usa el sistema decimal para los registros.

- **Puerto para la activación de dispositivos móviles**

  Puerto para conectar Kaspersky Endpoint Security for Android a los servidores de activación de Kaspersky.

  El número de puerto predeterminado es el 17100.

4. Haga clic en el botón **Guardar**.

Los dispositivos móviles pueden conectarse ahora al Servidor de administración.

Sustitución de aplicaciones de seguridad de terceros

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center puede requerir la eliminación del software de terceros incompatible con la aplicación instalada. Kaspersky Security Center proporciona varias formas de eliminar las aplicaciones de terceros.

Eliminar aplicaciones incompatibles utilizando el instalador

Esta opción está disponible solo en la Consola de administración basada en la Consola de administración de Microsoft.

El método del programa de instalación de eliminar aplicaciones incompatibles es compatible con varios tipos de instalación. Antes de instalar la aplicación de seguridad, todas las aplicaciones incompatibles se eliminan automáticamente si la ventana de propiedades del paquete de instalación de esta aplicación de seguridad (sección **Aplicaciones incompatibles**) tiene la opción **Desinstalar automáticamente las aplicaciones incompatibles** seleccionada.

Eliminar aplicaciones incompatibles al configurar la instalación remota de una aplicación

Puede habilitar la opción **Desinstalar automáticamente las aplicaciones incompatibles** al configurar la instalación remota de una aplicación de seguridad. En la Consola de administración basada en la Consola de administración de Microsoft (MMC), esta opción está disponible en el Asistente de instalación remota. En Kaspersky Security Center 14 Web Console, puede encontrar esta opción en el Asistente de despliegue de la protección. Cuando esta opción se activa, Kaspersky Security Center elimina la aplicación incompatible antes de instalar una aplicación de seguridad en un dispositivo administrado.

Instrucciones:

- Consola de administración: Instalación de aplicaciones con el Asistente de Instalación Remota
- Kaspersky Security Center 14 Web Console: Eliminación de aplicaciones incompatibles antes de la instalación

Eliminación de aplicaciones incompatibles mediante una tarea dedicada

Para eliminar las aplicaciones incompatibles, use la tarea **Desinstalar aplicación en remoto**. Esta tarea debería ejecutarse en dispositivos antes de la tarea de instalación de la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar el tipo de la programación **Al completar otra tarea**, donde la otra tarea es **Desinstalar aplicación en remoto**.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

Instrucciones de la Consola de administración: Crear una tarea.

Detección de dispositivos en red

Esta sección describe la búsqueda y la detección de dispositivos conectados a una red.

Kaspersky Security Center permite encontrar dispositivos según los criterios especificados. Puede guardar los resultados de la búsqueda en un archivo de texto.

La función de búsqueda y la detección permite encontrar los siguientes dispositivos:

- Dispositivos administrados en grupos de administración del Servidor de administración de Kaspersky Security Center y sus Servidores de administración secundarios.
- Dispositivos no asignados administrados por el Servidor de administración de Kaspersky Security Center y sus Servidores de administración secundarios.

Escenario: Detección de dispositivos en red

Debe realizar la detección de dispositivos antes de instalar las aplicaciones de seguridad. Cuando se detecten todos los dispositivos en red, puede obtener información sobre ellos y administrarlos a través de directivas. Se necesitan sondeos de red regulares para detectar si hay dispositivos nuevos y si los dispositivos detectados todavía están en la red.

La detección de dispositivos en red se realiza en etapas:

1. **Detección inicial de dispositivos**

El Asistente de inicio rápido le guía a través de la detección inicial de dispositivos y lo ayuda a encontrar dispositivos en red, como ordenadores, tabletas y teléfonos móviles. También puede realizar la detección de dispositivos manualmente.

2. **Configuración de futuros sondeos**

   Decida qué tipo(s) de detección desea utilizar regularmente. Asegúrese de que este tipo esté habilitado y que el calendario de sondeo cumpla con las necesidades de su organización. Al configurar el horario de sondeo, utilice las recomendaciones para la red de frecuencia de sondeo.

3. **La configuración de reglas para agregar dispositivos detectados a grupos de administración (opcional)**

   Si aparecen nuevos dispositivos de la red, que se detectan durante las sondeos regulares y se incluyen automáticamente en el grupo **Dispositivos no asignados**. Si lo desea, puede configurar las reglas para automático el traslado de estos dispositivos al grupo **Dispositivos administrados**. También puede configurar reglas de retención.

   Si omite este paso que configura la regla, todos los dispositivos recién detectados van al grupo **Dispositivos no asignados** y se quedan allí. Si lo desea, puede mover estos dispositivos al grupo de **Dispositivos administrados** manualmente. Si mueve estos dispositivos manualmente al grupo **Dispositivos administrados**, puede analizar la información sobre cada dispositivo y decidir si desea moverlo a un grupo de administración y, de ser así, a qué grupo.

Resultados

Al completar el escenario se obtienen los siguientes resultados:

- El Servidor de administración de Kaspersky Security Center detecta los dispositivos que están en la red y le proporciona información sobre ellos.
- Los sondeos futuros se configuran y funcionan de acuerdo con el calendario programado.

Los dispositivos recién descubiertos se arreglan según las reglas configuradas. (O, si no se configura ninguna regla, los dispositivos se quedan en el grupo **Dispositivos no asignados**).

Detección de dispositivos

Esta sección describe los tipos de detección de dispositivos disponibles en Kaspersky Security Center y proporciona información sobre cómo usar cada tipo.

El Servidor de administración recibe la información sobre la estructura de la red y sus dispositivos mediante sondeos periódicos. La información se registra en la base de datos del Servidor de administración. El Servidor de administración puede utilizar los siguientes tipos de sondeo:

- **Sondeo de la red de Windows**. El Servidor de administración puede realizar dos tipos de sondeo de red de Windows: rápido y completo. Durante un sondeo rápido, el Servidor de administración únicamente recopilará la información de los dispositivos de la lista de nombre NetBIOS de todos los dominios y grupos de trabajo de la red. Durante un sondeo completo, se solicita más información de cada dispositivo cliente, como nombre del sistema operativo, dirección IP, nombre DNS y nombre NetBIOS. De forma predeterminada, tanto el sondeo rápido como el sondeo completo están habilitados. El sondeo de la red de Windows puede no detectar dispositivos, por ejemplo, si los puertos UDP 137, UDP 138, TCP 139 están cerrados en el enrutador o por el firewall.
- **Sondeo de Active Directory**. El Servidor de administración recopila información de la estructura de la unidad de Active Directory y de los nombres DNS de los dispositivos de los grupos de Active Directory. Este tipo de sondeo está habilitado de forma predeterminada. Le recomendamos que utilice el sondeo de Active Directory si utiliza el directorio Activo; de lo contrario, el Servidor de administración no detecta ningún dispositivo. Si usa

Active Directory pero algunos de los dispositivos en red no están listados como miembros, estos dispositivos no pueden ser detectados por el sondeo de Active Directory.

- **Sondeo de rangos IP**. El Servidor de administración sondea los rangos IP especificados utilizando paquetes ICMP o el protocolo NBNS y recopila un conjunto completo de datos en los dispositivos de esos rangos IP. Este tipo de sondeo está deshabilitado de forma predeterminada. No se recomienda usar este tipo de sondeo si usa el sondeo de red de Windows y / o el sondeo de Active Directory.

- **Sondeo de Zeroconf**. Un punto de distribución que sondea la red IPv6 mediante el uso de una red de configuración cero (también denominada *Zeroconf*). Este tipo de sondeo está deshabilitado de forma predeterminada. Puede usar el sondeo de Zeroconf si el punto de distribución ejecuta Linux.

Si configura y activa reglas de movimiento del dispositivo, los dispositivos recién descubiertos automáticamente se incluyen en el grupo de **Dispositivos administrados**. Si ninguna regla de movimiento se ha activado, los dispositivos recién descubiertos automáticamente se incluyen en el grupo de **Dispositivos no asignados**.

Puede modificar la configuración de detección de dispositivos para cada tipo. Por ejemplo, es posible que desee modificar la programación de sondeo o establecer si desea sondar todo el bosque de Active Directory o solo un dominio específico.

Sondeo de la red de Windows

Acerca del sondeo de la red de Windows

Durante un sondeo rápido, el Servidor de administración únicamente recopilará la información de los dispositivos de la lista de nombre NetBIOS de todos los dominios y grupos de trabajo de la red. Durante un sondeo completo, en cada dispositivo cliente se solicita la siguiente información:

- Nombre del sistema operativo
- Dirección IP
- Nombre DNS
- Nombre NetBIOS

Tanto el sondeo rápido como el sondeo completo requieren lo siguiente:

- Los puertos UDP 137/138, TCP 139, UDP 445 y TCP 445 deben estar disponibles en la red.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo del navegador principal debe estar activado en el Servidor de administración.
- Se debe utilizar el servicio Explorador de equipos de Microsoft y el equipo del navegador principal debe estar activado en los dispositivos cliente:
  - En al menos un dispositivo, si el número de dispositivos en red no supera 32.
  - En al menos un dispositivo por cada 32 dispositivos en red.

El sondeo completo solo puede ejecutarse si el sondeo rápido se ha ejecutado al menos una vez.

Visualización y modificación de los parámetros para el sondeo de la red de Windows

Para modificar las propiedades para el sondeo de la red de Windows, realice lo siguiente:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → DOMINIOS DE WINDOWS**.
2. Haga clic en el botón **Propiedades**.

   Se abre la ventana de propiedades del dominio de Windows.
3. Active o desactive el sondeo de la red de Windows mediante el botón de activación **Permitir el sondeo de las redes de Windows**.
4. Configurar la programación del sondeo. De forma predeterminada, el sondeo rápido se ejecuta cada 15 minutos y el sondeo completo se ejecuta cada 60 minutos.

   Opciones de planificación de sondeo:

   - **Cada N días**

     El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

     De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.

   - **Cada N minutos**

     El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.

   - **Por días de la semana**

     El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.

   - **Cada mes, en días concretos de las semanas seleccionadas**

     El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.

   - **Ejecutar tareas no realizadas**

     Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de que se encienda o esperar a la próxima vez que se programe el sondeo.

     Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de que se encienda.

     Si esta opción está desactivada, el Servidor de administración espera a la próxima vez que se programe el sondeo.

     Esta opción está desactivada de forma predeterminada.
5. Haga clic en el botón **Guardar**.

Las propiedades se guardan y se aplican a todos los dominios y grupos de trabajo de Windows descubiertos.

Ejecución manual de la encuesta

Para ejecutar la encuesta de inmediato,

Haga clic en **Iniciar sondeo rápido** o **Iniciar sondeo completo**.

Cuando se completa el sondeo, puede ver la lista de dispositivos descubiertos en la página **DOMINIOS DE WINDOWS** al seleccionar la casilla de verificación junto a un nombre de dominio y luego hacer clic en el botón **Dispositivos**.

Sondeo de Active Directory

Use el sondeo de Active Directory si usa Active Directory; de lo contrario, se recomienda utilizar otros tipos de sondeo. Si usa Active Directory pero algunos de los dispositivos en red no están listados como miembros, estos dispositivos no pueden ser detectados usando el sondeo de Active Directory.

Kaspersky Security Center envía una solicitud al controlador del dominio y recibe la estructura del dispositivo Active Directory. El sondeo de Active Directory se realiza cada hora.

Visualización y modificación de los parámetros para el sondeo de Active Directory

Para visualizar y modificar los parámetros para el sondeo de Active Directory:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → Usuario de Active Directory**.
2. Haga clic en el botón **Propiedades**.
   Se abrirá la ventana de propiedades de Active Directory.
3. En la ventana de propiedades de Active Directory, puede definir la siguiente configuración:
   a. Active o desactive el sondeo de Active Directory con el botón de activación.
   b. Cambiar programación del sondeo.
      El periodo predeterminado es de una hora. Los datos recibidos en el siguiente sondeo reemplazan completamente los datos antiguos.
   c. Configure los ajustes avanzados para seleccionar la cobertura de sondeo:
      - El dominio de Active Directory al cual Kaspersky Security Center pertenece
      - El bosque de dominio al cual Kaspersky Security Center pertenece
      - Lista especificada de dominios de Active Directory

      Para agregar un dominio al ámbito de sondeo, seleccione una opción de dominio, haga clic en el botón **Agregar** y luego especifique la dirección del controlador de dominio y el nombre y la contraseña de la cuenta para acceder a él.
4. Para aplicar la nueva configuración, haga clic en el botón **Guardar**.

La nueva configuración se aplica al sondeo de Active Directory.

Ejecución manual de la encuesta

Para ejecutar la encuesta de inmediato,

haga clic en **Iniciar sondeo**.

Visualización de los resultados del sondeo de Active Directory

Para ver los resultados del sondeo de Active Directory:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → Usuario de Active Directory**.

   Se muestra la lista de unidades organizativas descubiertas.

2. Si lo desea, seleccione una unidad organizativa y luego haga clic en el botón **Dispositivos**.

   Se muestra la lista de dispositivos en la unidad organizativa.

Puede buscar la lista y filtrar los resultados.

Sondeo de rangos IP

Inicialmente, Kaspersky Security Center obtiene rangos de IP para el sondeo desde la configuración de red del dispositivo en el que está instalado. Si la dirección del dispositivo es 192.168.0.1 y la máscara de subred es 255.255.255.0, Kaspersky Security Center incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center sondea todas las direcciones desde 192.168.0.1 hasta 192.168.0.254.

No se recomienda usar el rango de IP de sondeo si usa el sondeo de red de Windows y / o el sondeo de Active Directory.

Kaspersky Security Center puede sondear rangos de IP mediante una búsqueda de DNS inversa o mediante el uso del protocolo NBNS:

- **Búsqueda de DNS inversa**

  Kaspersky Security Center intenta realizar una resolución de nombres inversa para cada dirección desde el rango especificado a un nombre de DNS usando solicitudes de DNS estándar. Si esta operación se realiza correctamente, el servidor envía una `ICMP ECHO REQUEST` (comando similar a "ping") al nombre recibido. Si el dispositivo responde, la información se añade a la base de datos de Kaspersky Security Center. La resolución de nombres inversa es necesaria para excluir los dispositivos de red que pueden tener una dirección IP pero no son equipos, por ejemplo, impresoras o rúteres.

  Este método de sondeo se basa en un servicio DNS local configurado correctamente. Debe tener una zona de búsqueda inversa. En las redes donde se utiliza Active Directory, esta zona se mantiene automáticamente. Pero en estas redes, el sondeo de subred IP no proporciona más información que el sondeo de Active Directory. Además, los administradores de redes pequeñas a menudo no configuran la zona de búsqueda inversa porque no es necesario para el trabajo de muchos servicios de red. Por ello, el sondeo de subred IP está deshabilitado de forma predeterminada.

- **Protocolo NBNS**

Si la resolución de nombres inversa no es posible en su red por alguna razón, Kaspersky Security Center utiliza el protocolo NBNS para sondear los rangos de IP. Si una solicitud a una dirección IP devuelve un nombre NetBIOS, la información sobre este dispositivo se agrega a la base de datos de Kaspersky Security Center.

Visualización y modificación de los parámetros para el sondeo de rangos IP

Para ver y modificar las propiedades del sondeo de rango de IP:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → RANGOS IP**.
2. Haga clic en el botón **Propiedades**.

   Se abrirá la ventana de propiedades de sondeo de IP.
3. Habilite o deshabilite el sondeo de IP con el botón de activación **Permitir sondeo**.
4. Configurar la programación del sondeo. De forma predeterminada, el sondeo IP se ejecuta cada 420 minutos (siete horas).

   Al especificar el intervalo de sondeo, asegúrese de que esta configuración no exceda el valor del parámetro de duración de la dirección IP. Si una dirección IP no se verifica mediante sondeo durante el tiempo de vida de la dirección IP, esta dirección IP se eliminará automáticamente de los resultados del sondeo. De forma predeterminada, la vida útil de los resultados del sondeo es de 24 horas, porque las direcciones IP dinámicas (asignadas mediante el Protocolo de configuración dinámica de host (DHCP)) cambian cada 24 horas.

   Opciones de planificación de sondeo:

   - **Cada N días**

     El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

     De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.

   - **Cada N minutos**

     El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.

   - **Por días de la semana**

     El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.

   - **Cada mes, en días concretos de las semanas seleccionadas**

     El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.

   - **Ejecutar tareas no realizadas**

Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de que se encienda o esperar a la próxima vez que se programe el sondeo.

Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de que se encienda.

Si esta opción está desactivada, el Servidor de administración espera a la próxima vez que se programe el sondeo.

Esta opción está desactivada de forma predeterminada.

5. Haga clic en el botón **Guardar**.

Las propiedades se guardan y se aplican a todos los rangos de IP.

Ejecución manual de la encuesta

Para ejecutar la encuesta de inmediato,

haga clic en **Iniciar sondeo**.

Adición y modificación de un rango IP

Inicialmente, Kaspersky Security Center obtiene rangos de IP para el sondeo desde la configuración de red del dispositivo en el que está instalado. Si la dirección del dispositivo es 192.168.0.1 y la máscara de subred es 255.255.255.0, Kaspersky Security Center incluye automáticamente la red 192.168.0.0/24 en la lista de direcciones del sondeo. Kaspersky Security Center sondea todas las direcciones desde 192.168.0.1 hasta 192.168.0.254. Puede modificar los rangos de IP definidos automáticamente o añadir rangos de IP personalizados.

Puede crear un rango Solo para direcciones IPv4. Si activa el Sondeo de Zeroconf, Kaspersky Security Center sondeará toda la red.

Para agregar un nuevo rango de IP:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → RANGOS IP**.
2. Para añadir un nuevo rango IP, haga clic en el botón **Añadir**.
3. En la ventana que se abre, especifique la siguiente configuración:
   - **Nombre del rango IP**

     Un nombre del rango IP. Es posible que desee especificar el rango IP como su nombre, por ejemplo, "192.168.0.0/24".

   - **Intervalo IP o dirección y máscara de subred**

Establezca el rango IP especificando las direcciones IP iniciales y finales o la dirección de subred y la máscara de subred. También puede seleccionar uno de los rangos IP existentes haciendo clic en el botón **Examinar**.

- **Vigencia de la dirección IP (horas)**

  Al especificar este parámetro, asegúrese de que exceda el intervalo de sondeo establecido en el programa de sondeo. Si una dirección IP no se verifica mediante sondeo durante el tiempo de vida de la dirección IP, esta dirección IP se eliminará automáticamente de los resultados del sondeo. De forma predeterminada, la vida útil de los resultados del sondeo es de 24 horas, porque las direcciones IP dinámicas (asignadas mediante el Protocolo de configuración dinámica de host, DHCP) cambian cada 24 horas.

4. Seleccione **Activar sondeos de rangos IP** si desea sondear la subred o el intervalo que ha añadido. De lo contrario, la subred o el intervalo que ha añadido no se sondearán.
5. Haga clic en el botón **Guardar**.

El nuevo rango IP se agrega a la lista de rangos IP.

Puede ejecutar el sondeo de cada rango IP por separado usando el botón **Iniciar sondeo**. Cuando se completa el sondeo, puede ver la lista de dispositivos descubiertos utilizando el botón **Dispositivos**. De forma predeterminada, la vida útil de los resultados del sondeo es de 24 horas y es igual a la configuración de duración de la dirección IP.

Para agregar una subred a un rango IP existente:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → RANGOS IP**.
2. Haga clic en el nombre del rango de IP al que desea agregar una subred.
3. En la ventana que se abre, haga clic en el botón **Añadir**.
4. Especifique una subred usando su dirección y máscara o usando la primera y la última dirección IP en el rango IP. O, añada una subred existente haciendo clic en el botón **Examinar**.
5. Haga clic en el botón **Guardar**.

   La nueva subred se agrega al rango IP.
6. Haga clic en el botón **Guardar**.

La nueva configuración del rango IP se guarda.

Puede añadir tantas subredes como necesite. Los rangos IP con nombre no pueden superponerse pero las subredes sin nombre dentro de un rango IP no tienen tales restricciones. Puede habilitar y deshabilitar el sondeo de forma independiente para cada rango IP.

Sondeo de Zeroconf

Este tipo de sondeo solo es compatible con los puntos de distribución basados en Linux.

Un punto de distribución puede sondear las redes que tienen dispositivos con direcciones IPv6. En este caso, no se especifican los rangos de IP y el punto de distribución sondea toda la red mediante el uso de una red de configuración cero (denominada *Zeroconf*). Para empezar a usar Zeroconf, debe instalar la utilidad avahi-browse en el punto de distribución.

Para activar el sondeo de la red IPv6:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → RANGOS IP**.
2. Haga clic en el botón **Propiedades**.
3. En la ventana que se abre, desplace el botón de alternancia **Usar Zeroconf para sondear las redes IPv6**.

Después de esto, el punto de distribución empieza a sondear su red. En este caso, se ignoran los rangos de IP especificados.

Configuración de reglas de retención para dispositivos no asignados

Una vez finalizado el sondeo de la red de Windows, los dispositivos encontrados se colocan en subgrupos del grupo de administración de dispositivos no asignados. Puede encontrar este grupo de administración en **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → DOMINIOS DE WINDOWS**. El grupo primario es **DOMINIOS DE WINDOWS**. Contiene grupos secundarios nombrados después de los dominios correspondientes y grupos de trabajo que se han encontrado durante el sondeo. El grupo primario también puede contener el grupo de administración de dispositivos móviles. Puede configurar las reglas de retención de los dispositivos no asignados para el grupo primario y para cada uno de los grupos secundarios. Las reglas de retención no dependen de la configuración de detección de dispositivos y funcionan incluso si la detección de dispositivos está desactivada.

Para configurar reglas de retención para dispositivos no asignados:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → DOMINIOS DE WINDOWS**.
2. Realice una de las siguientes acciones:
   - Para configurar los ajustes del grupo primario, haga clic en el botón **Propiedades**.

     Se abre la ventana de propiedades del dominio de Windows.
   - Para configurar los ajustes de un grupo secundario, haga clic en su nombre.

     Se abrirá la ventana de propiedades del grupo secundario.
3. Defina los siguientes parámetros:
   - **Quitar el dispositivo del grupo si ha estado inactivo durante más de (días)**

     Si esta opción está activada, puede especificar el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo. De forma predeterminada, esta opción también se distribuye a los grupos secundarios. De forma predeterminada, el intervalo de tiempo es 7 día.

     Esta opción está activada de forma predeterminada.
   - **Heredar del grupo primario**

Si esta opción está activada, el periodo de retención para los dispositivos en el grupo actual se hereda del grupo primario y no se puede cambiar.

Esta opción solo está disponible para grupos secundarios.

Esta opción está activada de forma predeterminada.

- Forzar herencia en grupos secundarios

  Los valores de configuración se distribuirán a grupos secundarios, pero en las propiedades de los grupos secundarios estas configuraciones están bloqueadas.

  Esta opción está desactivada de forma predeterminada.

4. Haga clic en el botón **Aceptar**.

Sus cambios están guardados y aplicados.

Aplicaciones de Kaspersky: licencia y activación

Esta sección describe las funciones de Kaspersky Security Center relacionadas con el manejo de claves de licencia de las aplicaciones administradas de Kaspersky.

Kaspersky Security Center le permite realizar una distribución centralizada de las claves de licencia para las aplicaciones Kaspersky en dispositivos cliente, supervisar su uso y renovar las licencias.

Al agregar una clave de licencia mediante Kaspersky Security Center, los parámetros de la clave de licencia se almacenan en el Servidor de administración. En función de esta información, la aplicación genera un informe de uso de claves de licencia y envía notificaciones al administrador cuando caducan las licencias y cuando se infringen las restricciones de las licencias especificadas en las propiedades de las claves de licencia. Puede configurar notificaciones del uso de claves de licencia en los parámetros del Servidor de administración.

Obtención de licencias de aplicaciones administradas

Las aplicaciones de Kaspersky instaladas en los dispositivos administrados se deben licenciar aplicando un archivo clave o código de activación a cada una de las aplicaciones. Los archivos clave o códigos de activación se pueden desplegar de las siguientes formas:

- Despliegue automático
- El paquete de instalación de una aplicación administrada
- La tarea *Agregar clave de licencia* para una aplicación administrada
- Activación manual de una aplicación administrada

Puede añadir una nueva clave de licencia activa o de reserva mediante cualquiera de los métodos enumerados anteriormente. Una aplicación de Kaspersky utiliza una clave activa en el momento actual y almacena una clave de reserva para aplicar después de que caduque la clave activa. La aplicación para la que añade una clave de licencia define si la clave está activa o si es de reserva. La definición de la clave no depende del método que utilice para añadir una nueva clave de licencia.

Despliegue automático

Si usa diferentes aplicaciones administradas y tiene que desplegar un archivo clave o un código de activación específicos en los dispositivos, opte por otras formas de desplegar ese código de activación o archivo clave.

Kaspersky Security Center le permite desplegar automáticamente las claves de licencia disponibles en los dispositivos. Por ejemplo, en el repositorio del Servidor de administración se almacenan tres claves de licencia. Ha seleccionado la casilla de verificación **Distribuir automáticamente la clave de licencia a los dispositivos administrados** para las tres claves de licencia. En los dispositivos de la organización se ha instalado una aplicación de seguridad de Kaspersky, por ejemplo, Kaspersky Endpoint Security para Windows. Se detecta un nuevo dispositivo en el que se debe desplegar una clave de licencia. La aplicación determina, por ejemplo, que dos de las claves de licencia del repositorio se pueden instalar en el dispositivo: una clave de licencia llamada *Clave_1* y una clave de licencia llamada *Clave_2*. Una de estas claves de licencia se despliega en el dispositivo. En este caso, no se puede predecir cuál de las dos claves de licencia se instalará en el dispositivo porque el despliegue automático de claves de licencia no prevé ninguna actividad de administrador.

Cuando se despliega una clave de licencia, los dispositivos se vuelven a contar para esa clave de licencia. Debe asegurarse de que la cantidad de dispositivos en los que se desplegó la clave de licencia no exceda el límite de la licencia. Si la cantidad de dispositivos excede el límite de la licencia, se asignará a todos los dispositivos que no estaban cubiertos por la licencia el estado *Crítico*.

Antes del despliegue, se deben añadir el archivo clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Consola de administración:
  - Adición de una clave de licencia al repositorio del Servidor de administración
  - Distribución automática de una clave de licencia

  o bien
- Kaspersky Security Center 14 Web Console:
  - Adición de una clave de licencia al repositorio del Servidor de administración
  - Distribución automática de una clave de licencia

Adición de un archivo clave o un código de activación al paquete de instalación de una aplicación administrada

Por motivos de seguridad, esta opción no se recomienda. El archivo clave o el código de activación añadidos a un paquete de instalación pueden verse comprometidos.

Si instala una aplicación administrada con un paquete de instalación, puede especificar un código de activación o un archivo clave en este paquete de instalación o en la directiva de la aplicación. La clave de licencia se desplegará en los dispositivos administrados en la próxima sincronización del dispositivo con el Servidor de administración.

Instrucciones:

- Consola de administración:
  - Creación de un paquete de instalación
  - Instalación de aplicaciones en dispositivos cliente

  o bien
- Kaspersky Security Center 14 Web Console: Agregar una clave a un paquete de instalación

Despliegue al ejecutar la tarea de añadir clave de licencia a una aplicación administrada

Si opta por usar la tarea *Agregar clave de licencia* a una aplicación administrada, puede elegir la clave de licencia que debe instalarse en los dispositivos y elegir los dispositivos con comodidad, por ejemplo, seleccionando un grupo de administración o una selección de dispositivos.

Antes del despliegue, se deben añadir el archivo clave o el código de activación al repositorio del Servidor de administración.

Instrucciones:

- Consola de administración:
  - Adición de una clave de licencia al repositorio del Servidor de administración
  - Despliegue de una clave de licencia en dispositivos cliente

  o bien
- Kaspersky Security Center 14 Web Console:
  - Adición de una clave de licencia al repositorio del Servidor de administración
  - Despliegue de una clave de licencia en dispositivos cliente

Adición de un código de activación o un archivo clave manualmente a los dispositivos

Puede activar la aplicación Kaspersky instalada localmente, usando las herramientas provistas en la interfaz de la aplicación. Por favor, consulte la documentación de la aplicación instalada.

Adición de una clave de licencia al repositorio del Servidor de administración

Para añadir una clave de licencia al repositorio del Servidor de administración, realice lo siguiente:

1. En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.

2. Haga clic en el botón **Añadir**.

3. Elija lo que quiera agregar:

   - **Añadir archivo clave**

     Haga clic en el botón **Seleccionar archivo clave** del archivo y vaya al archivo .key que desea añadir.

   - **Introducir el código de activación**

     Especifique el código de activación en el campo de texto y haga clic en el botón **Enviar**.

4. Haga clic en el botón **Cerrar**.

La clave o varias claves de licencia se añaden al repositorio del Servidor de administración.

Despliegue de una clave de licencia en dispositivos cliente

Kaspersky Security Center 14 Web Console permite distribuir una clave de licencia a los dispositivos cliente mediante la tarea de *Distribución de clave de licencia*.

Para distribuir una clave de licencia en los dispositivos cliente, realice lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.

2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas.

3. Seleccione la aplicación para la que desea añadir una clave de licencia.

4. De la lista **Tipo de tarea**, seleccione **Añadir clave de licencia**.

5. Siga las instrucciones del Asistente.

6. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

7. Haga clic en el botón **Crear**.

   La tarea se crea y se muestra en la lista de tareas.

8. Para ejecutar la tarea, selecciónela en la lista de tareas y haga clic en el botón **Iniciar**.

Cuando se realiza la tarea, la clave de licencia se despliega en los dispositivos seleccionados.

Distribución automática de una clave de licencia

Kaspersky Security Center permite la distribución automática de claves de licencias en dispositivos administrados si estas se encuentran en el repositorio de claves del Servidor de administración.

Para distribuir una clave de licencia automáticamente en dispositivos administrados:

1. En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.
2. Haga clic en el nombre de la clave que desee para distribuir automáticamente a dispositivos.
3. En la ventana de propiedades de la clave de licencia que se abre, seleccione la casilla **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.
4. Haga clic en el botón **Guardar**.

   La clave de licencia se distribuirá automáticamente a todos los dispositivos compatibles.

La distribución de claves de licencia se realiza por medio del Agente de red. No se crean tareas de distribución de clave de licencia para la aplicación.

Durante la distribución automática de una clave de licencia, se tiene en cuenta el límite del número de licencias que se pueden asignar a los dispositivos. El límite de licencias está configurado en las propiedades de la clave de licencia. Si se alcanza el límite de licencias, esta clave de licencia se deja de distribuir automáticamente en dispositivos.

Si elige la casilla de verificación **Distribuir automáticamente la clave de licencia a los dispositivos administrados**, en la ventana de propiedades de la clave de licencia, se distribuye una clave de licencia en su red inmediatamente. Si no selecciona esta opción, puede distribuir manualmente una clave de licencia más tarde.

Visualización de información sobre claves de licencias en uso

Para ver la lista de las claves de licencia agregadas al repositorio del Servidor de administración:

En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.

La lista que se muestra contiene los archivos clave y códigos de activación que se añadieron al repositorio del Servidor de administración.

Para ver información detallada sobre una clave de licencia:

1. En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.
2. Haga clic en el nombre de la clave de licencia requerida.

   En la ventana de propiedades de claves de licencia que se abre, puede:

- En la pestaña **Control de aplicaciones**: información principal sobre la clave de la licencia
- En la pestaña **Dispositivos**: La lista de dispositivos cliente donde se usó la clave de licencia para la activación de la aplicación Kaspersky instalada

Para ver qué claves de licencia se despliegan en un dispositivo cliente específico:

1. En el menú principal, vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el nombre del dispositivo requerido.

3. En la ventana de propiedades del dispositivo que se abre, seleccione la pestaña **Aplicaciones**.
4. Haga clic en el nombre de la aplicación para la que desea ver la información sobre la clave de licencia.
5. En la ventana de propiedades de la aplicación que se abre, seleccione la pestaña **Control de aplicaciones** y después abra la sección **Licencia**.

Se muestra la información principal sobre las claves de licencia activas y de reserva.

Para definir la configuración actualizada de las claves de licencia del Servidor de administración virtual, este envía una solicitud a los servidores de activación de Kaspersky como mínimo una vez al día.

Eliminación de una clave de licencia del repositorio

Cuando elimina la clave de licencia activa para una función adicional del Servidor de administración, por ejemplo Vulnerabilidad y administración de parches o Administración de dispositivos móviles, la función correspondiente deja de estar disponible. Si se ha añadido una clave de licencia de reserva, la clave de licencia de reserva se convierte automáticamente en la clave de licencia activa después de eliminar la clave de licencia activa anterior.

Cuando elimina la clave de licencia activa desplegada en un dispositivo administrado, la aplicación continua trabajando en el dispositivo administrado.

Para eliminar un archivo clave o un código de activación del repositorio del Servidor de administración, haga lo siguiente:

1. En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.
2. Seleccione el archivo clave o el código de activación que desea eliminar del repositorio.
3. Haga clic en el botón **Eliminar**.
4. Confirme la operación haciendo clic en el botón **Aceptar**.

El archivo clave seleccionado o el código de activación se eliminan del repositorio.

Puede volver a añadir una clave de licencia eliminada o bien otra nueva.

Revocación de consentimiento con el Contrato de licencia de usuario final

Si decide dejar de proteger algunos de sus dispositivos cliente, puede revocar el Contrato de licencia de usuario final (EULA) para cualquier aplicación Kaspersky administrada. Debe desinstalar la aplicación seleccionada antes de revocar su EULA.

Los EULA que se aceptaron en un Servidor de administración virtual se pueden revocar en el Servidor de administración virtual o en el Servidor de administración principal. Los EULA que se aceptaron en un Servidor de administración principal solo se pueden revocar en el Servidor de administración principal.

Para revocar un EULA para aplicaciones Kaspersky administradas:

1. Abra la ventana de propiedades del Servidor de administración y en la pestaña **Control de aplicaciones**, seleccione la sección **Contratos de licencia de usuario final**.

   Se muestra una lista de EULA, aceptada tras la creación de paquetes de instalación, la instalación sin problemas de actualizaciones o el despliegue de Kaspersky Security for Mobile.

2. En la lista, seleccione el EULA que quiere revocar.

   Puede ver las siguientes propiedades del EULA:

   - Fecha en la que se aceptó el EULA.
   - Nombre del usuario que aceptó el EULA.

3. Haga clic en la fecha de aceptación de cualquier EULA para abrir su ventana de propiedades, que muestra los siguientes datos:

   - Nombre del usuario que aceptó el EULA.
   - Fecha en la que se aceptó el EULA.
   - Identificador único (UID) del EULA.
   - Texto completo del EULA.
   - Lista de objetos (paquetes de instalación, actualizaciones integradas, aplicaciones móviles) vinculados al EULA y sus respectivos nombres y tipos.

4. En la parte inferior de la ventana de propiedades del EULA, haga clic en el botón **Revocar el Contrato de licencia**.

   Si existen objetos (paquetes de instalación y sus respectivas tareas) que impidan la revocación del EULA, se muestra la notificación correspondiente. No puede continuar con la revocación hasta que elimine estos objetos.

   En la ventana que se abre, se le informa que primero debe desinstalar la aplicación Kaspersky correspondiente al EULA.

5. Haga clic en el botón para confirmar la revocación.

El EULA se ha revocado. Ya no se lo muestra en la lista de Acuerdos de licencia en la sección **Contratos de licencia de usuario final**. La ventana de propiedades del EULA se cierra y la aplicación ya no está instalada.

Renovación de licencias para aplicaciones de Kaspersky

Puede renovar una licencia de una aplicación de Kaspersky que haya caducado o que esté a punto de caducar (en menos de 30 días).

Para renovar una licencia caducada o una licencia que está a punto de caducar:

1. Realice una de las siguientes acciones:

   - En el menú principal, vaya a **OPERACIONES → LICENCIAS → LICENCIAS DE KASPERSKY**.

- En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **PANEL** y, luego, haga clic en el enlace **Ver licencias que caducan** junto a una notificación.

Se abre la ventana **LICENCIAS DE KASPERSKY**, donde puede ver y renovar las licencias.

2. Haga clic en el enlace **Renovar licencia** que aparece junto a la licencia requerida.

   Al hacer clic en un enlace de renovación de licencia, acepta transferir a Kaspersky la siguiente información sobre Kaspersky Security Center: la versión, la localización que está utilizando, el ID de la licencia de software (es decir, el ID de la licencia que está renovando) y si compró la licencia a través de una empresa asociada o no.

3. En la ventana del servicio de renovación de licencia que se abre, siga las instrucciones para renovar una licencia.

   La licencia queda renovada.

En Kaspersky Security Center 14 Web Console, las notificaciones se muestran cuando una licencia está a punto de caducar, de acuerdo con el siguiente programa:

- 30 días antes del vencimiento
- 7 días antes del vencimiento
- 3 días antes del vencimiento
- 24 horas antes del vencimiento
- Cuando una licencia ha caducado

Utilizar Kaspersky Marketplace para elegir soluciones empresariales de Kaspersky

MERCADO es una sección en el menú principal que le permite ver toda la gama de soluciones empresariales de Kaspersky, seleccionar las que necesita y proceder a la compra en el sitio web de Kaspersky. Puede utilizar filtros para ver solo las soluciones que se ajustan a su organización y a los requisitos de su sistema de seguridad de la información. Cuando selecciona una solución, Kaspersky Security Center le redirige a la página web relacionada en el sitio web de Kaspersky para obtener más información sobre esa solución. Cada página web le permite continuar la compra o contiene instrucciones sobre el proceso de compra.

En la sección **MERCADO**, puede filtrar las soluciones de Kaspersky con los siguientes criterios:

- Número de dispositivos (puntos finales, servidores y otros tipos de activos) que desea proteger:
  - 50-250
  - 250-1000
  - Más de 1000
- Nivel de madurez del equipo de seguridad de la información de su organización:
  - **Bases**

Este nivel es típico de las empresas que solo tienen un equipo de TI. Se bloquea el máximo número posible de amenazas automáticamente.

- **Óptimo**

  Este nivel es típico de las empresas que tienen una función específica de seguridad informática dentro del equipo de TI. A este nivel, las empresas requieren soluciones que les permitan contrarrestar las amenazas de productos básicos y las amenazas que evitan los mecanismos de prevención existentes.

- **Experto**

  Este nivel es típico de las empresas con entornos complejos y distribuidos de TI. El equipo de seguridad de TI es maduro o la empresa tiene un equipo SOC (Centro de Operaciones de Seguridad). Las soluciones requeridas permiten a las empresas contrarrestar amenazas complejas y ataques dirigidos.

- Tipos de activos que desea proteger:
  - **Puntos finales**: estaciones de trabajo de los empleados, máquinas físicas y virtuales, sistemas integrados
  - **Servidores**: servidores físicos y virtuales
  - **Nube**: entornos de nube pública, privada o híbrida; servicios en la nube
  - **Red**: red de área local, infraestructura de TI
  - **Servicio**: servicios relacionados con la seguridad proporcionados por Kaspersky

Para encontrar y adquirir una solución empresarial de Kaspersky:

1. En la ventana principal, vaya a **MERCADO**.

   De forma predeterminada, la sección muestra todas las soluciones empresariales disponibles de Kaspersky.

2. Para ver solo las soluciones que se adaptan a su organización, seleccione los valores necesarios en los filtros.

3. Haga clic en la solución que desea adquirir o sobre la que desea obtener más información.

   Será redirigido a la página web de la solución. Puede seguir las instrucciones en pantalla para proceder a la compra.

Configuración de protección de la red

En esta sección, encontrará información sobre la configuración manual de las directivas y las tareas, sobre las funciones del usuario y sobre la creación de una estructura de grupos de administración y jerarquía de tareas.

Escenario: Configuración de protección de la red

El Asistente de inicio rápido crea directivas y tareas con la configuración predeterminada. Estas configuraciones pueden resultar subóptimas o, incluso, inadmisibles para la organización. Por lo tanto, le recomendamos que ajuste estas directivas y tareas, y cree otras en caso de ser necesarias para su red.

Requisitos previos

Antes de comenzar, asegúrese de haber hecho lo siguiente:

- Instalado el Servidor de administración de Kaspersky Security Center 14
- Instalado Kaspersky Security Center 14 Web Console (opcional)
- Completado el escenario de instalación principal de Kaspersky Security Center
- Completado el Asistente de inicio rápido o creado manualmente las siguientes directivas y tareas en el grupo de administración de **Dispositivos administrados**:
  - Directiva de Kaspersky Endpoint Security
  - Tarea de grupo para actualizar Kaspersky Endpoint Security
  - Directiva del Agente de red
  - Tarea *Encontrar vulnerabilidades y actualizaciones requeridas*

La configuración de la protección de red se realiza en etapas:

1. **Configuración y propagación de directivas de aplicación Kaspersky y perfiles de directiva**

   Para configurar y propagar la configuración de las aplicaciones Kaspersky instaladas en los dispositivos administrados, puede utilizar dos enfoques de la gestión de la seguridad diferentes: centrada en el dispositivo o centrada en el usuario. Estos dos enfoques también se pueden combinar. Para implementar la Administración de seguridad centrada en el dispositivo, puede usar las herramientas proporcionadas en la Consola de administración basada en la Consola de administración de Microsoft o en Kaspersky Security Center 14 Web Console. La administración de la seguridad centrada en el usuario solamente se puede implementar a través de Kaspersky Security Center 14 Web Console.

2. **Configuración de tareas para la administración remota de aplicaciones Kaspersky**

   Verifique las tareas creadas con el Asistente de inicio rápido y afínelas, si es necesario.

   Instrucciones:

   - Consola de administración:
     - Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
     - Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center 14 Web Console:
     - Configuración de la tarea de grupo para actualizar Kaspersky Endpoint Security
     - Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

   Si es necesario, cree tareas adicionales para administrar las aplicaciones Kaspersky instaladas en los dispositivos cliente.

3. **La evaluación y la limitación del evento se cargan en la base de datos**

   Se transfiere la información sobre eventos durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se registra en la base de datos del Servidor de administración. Para reducir la carga en el Servidor de administración, evalúe y limite el número máximo de eventos que se pueden almacenar en la base de datos.

   Instrucciones:

- Consola de administración: Establecer el número máximo de eventos
- Kaspersky Security Center 14 Web Console: Configuración del número máximo de eventos

Resultados

Cuando complete este escenario, su red estará protegida gracias a la configuración de las aplicaciones de Kaspersky, tareas y eventos recibidos por el Servidor de administración:

- Las aplicaciones de Kaspersky se configuran de acuerdo con las directivas y los perfiles de directiva
- Las aplicaciones se administran a través de un conjunto de tareas
- Se establece el número máximo de eventos que se pueden almacenar en la base de datos

Cuando se completa la configuración de protección de la red, puede proceder a configurar actualizaciones periódicas de las bases de datos y aplicaciones de Kaspersky.

Para obtener detalles sobre cómo configurar las respuestas automáticas a las amenazas detectadas por Kaspersky Sandbox, consulte la Ayuda en línea de Kaspersky Sandbox 2.0.

Acerca de los enfoques de administración de seguridad centrados en el dispositivo y centrados en el usuario

Puede administrar la configuración de seguridad desde el punto de vista de las funciones del dispositivo y desde el punto de vista de los roles de usuario. El primer enfoque se denomina *administración de seguridad centrada en el dispositivo* y el segundo se denomina *administración de seguridad centrada en el usuario*. Para aplicar diferentes configuraciones de aplicaciones a diferentes dispositivos, puede usar uno o ambos tipos de administración en combinación. Para implementar la Administración de seguridad centrada en el dispositivo, puede usar las herramientas proporcionadas en la Consola de administración basada en la Consola de administración de Microsoft o en Kaspersky Security Center 14 Web Console. La administración de la seguridad centrada en el usuario solamente se puede implementar a través de Kaspersky Security Center 14 Web Console.

La administración de seguridad centrada en el dispositivo le permite aplicar distintas configuraciones de la aplicación de seguridad a los dispositivos administrados según las funciones específicas del dispositivo. Por ejemplo, puede aplicar distintas configuraciones a los dispositivos asignados en diferentes grupos de administración. También puede diferenciar los dispositivos según su uso en Active Directory o según sus especificaciones de hardware.

La administración de seguridad centrada en el usuario le permite aplicar distintas configuraciones de la aplicación de seguridad a diferentes funciones de usuario. Puede crear varias funciones de usuario, asignar una función de usuario adecuada para cada usuario y definir diferentes configuraciones de la aplicación para los dispositivos de usuarios con diferentes funciones. Por ejemplo, es posible que desee aplicar diferentes configuraciones de aplicaciones a los dispositivos de contadores y especialistas del departamento de recursos humanos (HR). Como resultado, cuando se implementa la administración de seguridad centrada en el usuario, cada departamento (el departamento de contabilidad y el departamento de recursos humanos) tiene su propia configuración de opciones para las aplicaciones de Kaspersky. Una configuración define qué opciones de la aplicación pueden cambiar los usuarios y cuáles impone y bloquea el administrador.

Al utilizar la administración de seguridad centrada en el usuario, puede aplicar configuraciones de aplicaciones específicas incluso para usuarios individuales. Esto puede ser necesario cuando un empleado tiene un rol único en la empresa o cuando desea monitorear incidentes de seguridad relacionados con dispositivos de una persona específica. Dependiendo de la función de este empleado en la empresa, puede ampliar o limitar los derechos de esta persona para cambiar la configuración de la aplicación. Por ejemplo, es posible que desee ampliar los derechos de un administrador del sistema que administra los dispositivos cliente en una oficina local.

También puede combinar los enfoques de administración de seguridad centrados en el dispositivo y centrados en el usuario. Por ejemplo, puede configurar una directiva de aplicación específica para cada grupo de administración y luego crear perfiles de directivas para una o varias funciones de usuario de su empresa. En este caso, las directivas y los perfiles de directiva se aplican en el siguiente orden:

1. Se aplican las directivas creadas para la administración de seguridad centrada en el dispositivo.
2. Son modificados por los perfiles de directiva de acuerdo con las prioridades del perfil de directiva.
3. Las directivas son modificadas por los perfiles de directiva asociados con roles de usuario.

Configuración y propagación de directivas: enfoque centrado en el dispositivo

Cuando complete este escenario, las aplicaciones se configurarán en todos los dispositivos administrados de acuerdo con las directivas de aplicación y los perfiles de directiva que defina.

Requisitos previos

Antes de comenzar, asegúrese de haber instalado con éxito el Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console (opcional) Si instaló Kaspersky Security Center 14 Web Console, es posible que también desee considerar la administración de seguridad centrada en el usuario como una opción alternativa o adicional al enfoque centrado en el dispositivo.

Etapas

El escenario de administración centrada en el dispositivo de las aplicaciones de Kaspersky consiste en los siguientes pasos:

1. **Configuración de directivas de aplicación**

   Configure los ajustes para las aplicaciones de Kaspersky instaladas en los dispositivos administrados mediante la creación de una directiva para cada aplicación. El conjunto de directivas se propagará a los dispositivos cliente.

   Cuando configura la protección de su red en el Asistente de inicio rápido, Kaspersky Security Center crea la directiva predeterminada para Kaspersky Endpoint Security para Windows. Si completó el proceso de configuración utilizando este Asistente, no tiene que crear una nueva directiva para esta aplicación. Vaya a la Configuración manual de la directiva de Kaspersky Endpoint Security.

   Si tiene una estructura jerárquica de varios Servidores de administración y/o grupos de administración, los Servidores de administración secundarios y los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios y los Servidores de administración secundarios para prohibir cualquier modificación de los parámetros configurados en la directiva ascendente. Si desea que solo una parte de la configuración se herede a la fuerza, puede bloquearla en la directiva ascendente. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas creada le permitirá administrar efectivamente los dispositivos en los grupos de administración.

Instrucciones:

- Consola de administración: Creación de una directiva
- Kaspersky Security Center 14 Web Console: Crear una directiva

2. **Creación de perfiles de directivas (opcional)**

   Si desea que los dispositivos dentro de un solo grupo de administración se ejecuten bajo diferentes configuraciones de directivas, cree perfiles de directivas para esos dispositivos. Un perfil de directiva es un subconjunto de parámetros de la directiva denominado. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa en una condición específica denominada la *Condición de activación de perfil*. Los perfiles solo contienen parámetros que se diferencian de la directiva "básica", que está activa en el dispositivo administrado.

   Al utilizar las condiciones de activación del perfil, puede aplicar diferentes perfiles de directivas, por ejemplo, a los dispositivos ubicados en una unidad específica o grupo de seguridad de Active Directory, con configuración de hardware específica o marcados con etiquetas específicas. Utilice etiquetas para filtrar dispositivos que cumplan criterios específicos. Por ejemplo, puede crear una etiqueta llamada *Windows*, marcar todos los dispositivos que ejecutan el sistema operativo Windows con esta etiqueta y luego especificar esta etiqueta como condición de activación para un perfil de directiva. Como resultado, las aplicaciones de Kaspersky instaladas en todos los dispositivos que ejecutan Windows serán administradas por su propio perfil de directiva.

   Instrucciones:

   - Consola de administración:
     - Crear perfil de directiva
     - Creación de una regla de activación de perfil de directiva
   - Kaspersky Security Center 14 Web Console:
     - Crear perfil de directiva
     - Creación de una regla de activación de perfil de directiva

3. **Propagación de directivas y perfiles de directiva a los dispositivos administrados**

   De forma predeterminada, el Servidor de administración se sincroniza automáticamente con los dispositivos administrados cada 15 minutos. Durante la sincronización, las directivas nuevas o modificadas y los perfiles de directivas se propagan a los dispositivos administrados. Puede evitar la sincronización automática y ejecutar la sincronización manualmente utilizando el comando Forzar sincronización. Una vez que se complete la sincronización, las directivas y los perfiles de las directivas se entregan y aplican a las aplicaciones instaladas de Kaspersky.

   Si usa Kaspersky Security Center 14 Web Console, puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center especifica la fecha y la hora de entrega en las propiedades del dispositivo.

   Instrucciones:

   - Consola de administración: sincronización forzada
   - Kaspersky Security Center 14 Web Console: Forzar sincronización

Resultados

Cuando se completa el escenario centrado en el dispositivo, las aplicaciones de Kaspersky se configuran de acuerdo con la configuración especificada y propagada a través de la jerarquía de directivas.

Las directivas de aplicación configuradas y los perfiles de directivas se aplicarán automáticamente a los nuevos dispositivos añadidos a los grupos de administración.

Configuración y propagación de directivas: enfoque centrado en el usuario

Esta sección describe el escenario de enfoque centrado en el usuario para la configuración centralizada de las aplicaciones de Kaspersky instaladas en los dispositivos administrados. Cuando complete este escenario, las aplicaciones se configurarán en todos los dispositivos administrados de acuerdo con las directivas de aplicación y los perfiles de directiva que defina.

Este escenario se puede implementar a través de Kaspersky Security Center Web Console versión 13 o posterior.

Requisitos previos

Antes de comenzar, asegúrese de haber instalado correctamente el Servidor de administración de Kaspersky Security Center y Kaspersky Security Center 14 Web Console y de haber completado el escenario de instalación principal. También es posible que desee considerar la administración de seguridad centrada en el dispositivo como una opción alternativa o adicional al enfoque centrado en el usuario. Más información sobre dos enfoques de administración.

Proceso

El escenario de administración centrada en el usuario de las aplicaciones de Kaspersky consta de los siguientes pasos:

1. **Configuración de directivas de aplicación**

   Configure los ajustes para las aplicaciones de Kaspersky instaladas en los dispositivos administrados mediante la creación de una directiva para cada aplicación. El conjunto de directivas se propagará a los dispositivos cliente.

   Cuando configura la protección de su red en el Asistente de inicio rápido, Kaspersky Security Center crea la directiva predeterminada para Kaspersky Endpoint Security. Si completó el proceso de configuración utilizando este Asistente, no tiene que crear una nueva directiva para esta aplicación. Vaya a la Configuración manual de la directiva de Kaspersky Endpoint Security.

   Si tiene una estructura jerárquica de varios Servidores de administración y/o grupos de administración, los Servidores de administración secundarios y los grupos de administración secundarios heredan las directivas del Servidor de administración principal de forma predeterminada. Puede forzar la herencia de los grupos secundarios y los Servidores de administración secundarios para prohibir cualquier modificación de los parámetros configurados en la directiva ascendente. Si desea que solo una parte de la configuración se herede a la fuerza, puede bloquearla en la directiva ascendente. El resto de configuraciones desbloqueadas estarán disponibles para modificación en las directivas posteriores. La jerarquía de directivas creada le permitirá administrar efectivamente los dispositivos en los grupos de administración.

   Instrucciones: Creación de una directiva

2. **Especificación de propietarios de los dispositivos**

   Asigne los dispositivos administrados a los usuarios correspondientes.

   Instrucciones: Designación del usuario como propietario del dispositivo

3. **Definición de funciones de usuario típicas de su empresa**

Piense en los diferentes tipos de trabajo que normalmente realizan los empleados de su empresa. Debe dividir a todos los empleados de acuerdo con sus funciones. Por ejemplo, puede dividirlos por departamentos, profesiones o cargos. Después de eso, deberá crear una función de usuario para cada grupo. Tenga en cuenta que cada función de usuario tendrá su propio perfil de directiva que contiene la configuración de la aplicación específica para esta función.

4. **Creación de funciones de usuario**

   Cree y configure una función de usuario para cada grupo de empleados que definió en el paso anterior o use las funciones de usuario predefinidos. Las funciones de usuario contendrán un conjunto de derechos de acceso a las características de la aplicación.

   Instrucciones: Creación de una función de usuario

5. **Definición de la cobertura de cada función de usuario**

   Para cada uno de las funciones de usuario creadas, defina usuarios y/o grupos de seguridad y grupos de administración. La configuración asociada con una función de usuario se aplica solo a los dispositivos que pertenecen a usuarios que tienen esta función y solo si estos dispositivos pertenecen a grupos asociados con esta función, incluidos los grupos secundarios.

   Instrucciones: Edición de la cobertura de una función de usuario

6. **Crear perfiles de directiva**

   Crear un perfil de directiva para cada función de usuario en su empresa. Los perfiles de directivas definen qué configuración se aplicará a las aplicaciones instaladas en los dispositivos de los usuarios en función de la función de cada usuario.

   Instrucciones: Creación de un perfil de directiva

7. **Asociación de perfiles de directivas de funciones de usuario**

   Asocie los perfiles de directiva creados con las funciones de usuario. Después de eso: el perfil de la directiva se activa para un usuario que tiene la función especificada. Los parámetros configurados en el perfil de la directiva se aplicarán a las aplicaciones de Kaspersky instaladas en los dispositivos del usuario.

   Instrucciones: Asociación de perfiles de directivas con funciones

8. **Propagación de directivas y perfiles de directiva a los dispositivos administrados**

   De forma predeterminada, el Servidor de administración se sincroniza automáticamente con los dispositivos administrados cada 15 minutos. Durante la sincronización, las directivas nuevas o modificadas y los perfiles de directivas se propagan a los dispositivos administrados. Puede evitar la sincronización automática y ejecutar la sincronización manualmente utilizando el comando Forzar sincronización. Una vez que se complete la sincronización, las directivas y los perfiles de las directivas se entregan y aplican a las aplicaciones instaladas de Kaspersky.

   Puede verificar si las directivas y los perfiles de directivas se entregaron a un dispositivo. Kaspersky Security Center especifica la fecha y la hora de entrega en las propiedades del dispositivo.

   Instrucciones: Sincronización forzada

Resultados

Cuando se completa el escenario centrado en el dispositivo, las aplicaciones de Kaspersky se configuran de acuerdo con la configuración especificada y propagada a través de la jerarquía de directivas y perfiles de directivas.

Para un nuevo usuario, tendrá que crear una nueva cuenta, asignar al usuario una de las funciones de usuario creados y asignar los dispositivos al usuario. Las directivas de aplicación configuradas y los perfiles de la directiva se aplicarán automáticamente a los dispositivos de este usuario.

Configuración de la directiva del Agente de red

Para configurar la directiva del Agente de red:

1. En el menú principal, vaya a **DISPOSITIVOS** → **DIRECTIVAS Y PERFILES**.
2. Haga clic en el nombre de la directiva del Agente de red.

Se abre la ventana de propiedades de la directiva del Agente de red.

Control de aplicaciones

En esta pestaña puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- En **Estado de la directiva**, puede seleccionar uno de los modos de la directiva:
  - Activa

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.
  - Inactiva

    Si se selecciona esta opción, se inactiva la directiva, pero sigue almacenada en la carpeta **Directivas**. Si fuera necesario, se puede activar la directiva.
- En la sección de grupo **Herencia de configuración**, se puede configurar la herencia de directivas:
  - Heredar configuración de la directiva primaria

    Si se activa esta opción, los valores de la configuración de la directiva se heredan de la directiva de grupos de nivel superior y, por lo tanto, quedan bloqueados.

    Esta opción está activada de forma predeterminada.
  - Forzar la herencia de la configuración en las directivas secundarias

    Si se activa esta opción, después de aplicar modificaciones a las directivas, se realizarán las siguientes acciones:
    - Los valores de los parámetros de las directivas se distribuirán a las directivas de los grupos de administración anidados, es decir, a las directivas secundarias.
    - En el bloque **Herencia de configuración** de la sección **General** de la ventana de propiedades de cada directiva secundaria, se activará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Si se activa esta opción, la configuración de las directivas secundarias queda bloqueada.

    Esta opción está desactivada de forma predeterminada.

Configuración de eventos

En esta pestaña, puede configurar el registro de eventos y la notificación de eventos. Los eventos se distribuyen según el nivel de importancia en las siguientes secciones en la pestaña **Configuración de eventos**:

- **Fallo operativo**
- **Advertencia**
- **Información**

En cada sección, la lista de tipos de evento muestra los tipos de eventos y el plazo de almacenamiento de eventos predeterminado en el Servidor de administración (en días). Después de hacer clic en un tipo de evento, puede especificar la configuración del registro de eventos y las notificaciones relativas a los eventos elegidos en la lista. De forma predeterminada, la configuración de la notificación común especificada para el Servidor de administración completo se utiliza para todos los tipos de evento. Sin embargo, puede cambiar la configuración específica para los tipos de evento requeridos.

Por ejemplo, en la sección **Advertencia**, puede configurar el tipo de evento **Se ha producido un incidente**. Este tipo de eventos pueden ocurrir, por ejemplo, cuando el espacio libre en disco de un punto de distribución es inferior a 2 GB (se requieren al menos 4 GB para instalar aplicaciones y descargar actualizaciones de forma remota). Para configurar el evento **Se ha producido un incidente**, haga clic en este y especifique dónde almacenar los eventos ocurridos y cómo notificarlos.

Si el Agente de red detectó un incidente, usted puede administrar este incidente utilizando la configuración de un dispositivo administrado.

Configuración de la aplicación

Configuración

En la sección **Configuración**, se puede configurar la directiva del Agente de red:

- **Distribuir archivos solo mediante puntos de distribución**

  Si esta opción está activada, los Agentes de red en los dispositivos administrados recuperan las actualizaciones solo de los puntos de distribución.

  Si esta opción está desactivada, los Agentes de red en los dispositivos administrados recuperan las actualizaciones de los puntos de distribución o del Servidor de administración.

  Tenga en cuenta que las aplicaciones de seguridad en los dispositivos administrados recuperan actualizaciones del origen establecido en la tarea de actualización para cada aplicación de seguridad. Si activa la opción **Distribuir archivos solo mediante puntos de distribución**, asegúrese de que Kaspersky Security Center esté configurado como origen de actualización en las tareas de actualización.

  Esta opción está desactivada de forma predeterminada.

- **Tamaño máximo de la cola del evento, en MB**

En este campo se puede especificar el espacio máximo en disco que puede ocupar una cola de eventos.

El valor predeterminado es de 2 Megabytes (MB).

- **La aplicación podrá obtener información adicional sobre la directiva en el dispositivo**

  El Agente de red instalado en un dispositivo administrado transfiere información sobre la directiva de aplicación de seguridad aplicada a la aplicación de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows). Puede ver la información transferida en la interfaz de la aplicación de seguridad.

  El Agente de red transfiere la siguiente información:

  - Hora de entrega de la directiva al dispositivo administrado
  - Nombre de la directiva activa o fuera de la oficina en el momento de la entrega de la directiva al dispositivo administrado
  - Nombre y ruta completa al grupo de administración que contenía el dispositivo administrado en el momento de la entrega de la directiva al dispositivo administrado
  - Lista de perfiles de directivas activas

    Puede utilizar la información para asegurarse de que se aplique la directiva correcta al dispositivo y para solucionar problemas. Esta opción está desactivada de forma predeterminada.

- **Evitar que el servicio del Agente de red se detenga o se elimine sin autorización e impedir cambios en su configuración**

  Una vez que el Agente de red se instala en un dispositivo administrado, el componente no se puede eliminar ni reconfigurar sin los privilegios necesarios. El servicio del Agente de red no se puede detener.

  Esta opción está desactivada de forma predeterminada.

- **Utilizar contraseña de desinstalación**

  Si se selecciona esta opción, al hacer clic en el botón **Modificar** se puede especificar la contraseña para la desinstalación remota del Agente de red.

  Esta opción está desactivada de forma predeterminada.

Repositorios

En la sección **Repositorios**, puede seleccionar los tipos de objetos cuya información se enviará desde el Agente de red hasta el Servidor de administración. Si la modificación de algunos parámetros de esta sección está prohibida por la directiva del Agente de red, no se los podrá modificar.

- **Detalles de las aplicaciones instaladas**
- **Incluir información sobre parches**

La información sobre parches de aplicaciones instaladas en dispositivos cliente se envía al Servidor de administración. Si se activa esta opción, se puede incrementar la carga del Servidor de administración y el DBMS, así como el volumen de la base de datos.

Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

- Detalles de las actualizaciones de Windows Update

  Si se selecciona esta opción, la información sobre las actualizaciones de Microsoft Windows Update que se deben instalar en los dispositivos cliente se envía al Servidor de administración.

  A veces, incluso si la opción está desactivada, las actualizaciones se muestran en las propiedades del dispositivo en la sección **Actualizaciones disponibles**. Esto podría suceder en el caso de que, por ejemplo, los dispositivos de la organización tengan vulnerabilidades que estas actualizaciones puedan solucionar.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

- Detalles de vulnerabilidades de software y actualizaciones correspondientes

  Si esta opción está activada, la información sobre vulnerabilidades en el software de terceros (incluido el software de Microsoft), detectada en dispositivos administrados, y sobre actualizaciones de software para corregir vulnerabilidades de terceros (sin incluir el software de Microsoft) se envía al Servidor de administración.

  Al seleccionar esta opción (**Detalles de vulnerabilidades de software y actualizaciones correspondientes**) aumenta la carga de red, la carga de disco del Servidor de administración y el consumo de recursos del Agente de red.

  Esta opción está activada de forma predeterminada. Está disponible solo para Windows.

  Para administrar las actualizaciones de software de Microsoft, use la opción **Detalles de las actualizaciones de Windows Update**.

- **Detalles de registro de hardware**

Vulnerabilidades y actualizaciones de software

En la sección **Vulnerabilidades y actualizaciones de software**, puede configurar la búsqueda y distribución de actualizaciones de Windows, así como activar el análisis de archivos ejecutables en busca de vulnerabilidades. La configuración en la sección **Vulnerabilidades y actualizaciones de software** está disponible solo en dispositivos que ejecutan Windows:

- Utilizar el Servidor de administración como servidor WSUS

  Si esta opción está activada, las actualizaciones de Windows se descargan al Servidor de administración. El Servidor de administración proporciona actualizaciones descargadas a servicios de Windows Update en dispositivos cliente en el modo centralizado por medio de Agentes de red.

  Si esta opción está desactivada, el Servidor de administración no se utiliza para descargar actualizaciones de Windows. En este caso, los dispositivos cliente reciben las actualizaciones de Windows por su propia cuenta.

  Esta opción está desactivada de forma predeterminada.

- Puede limitar las actualizaciones de Windows que los usuarios pueden instalar de forma manual en sus dispositivos mediante Windows Update.

En los dispositivos que ejecutan Windows 10, si Windows Update ya encontró actualizaciones para el dispositivo, la nueva opción que seleccione en **Permitir a los usuarios administrar la instalación de las actualizaciones de Windows Update** se aplicará solo después de que se hayan instalado las actualizaciones encontradas.

Seleccione un elemento en la lista desplegable:

- **Permitir que los usuarios instalen todas las actualizaciones de Windows Update aplicables**

  Los usuarios pueden instalar todas las actualizaciones de Microsoft Windows Update que sean aplicables a sus dispositivos.

  Seleccione esta opción si no desea interferir en la instalación de actualizaciones.

  Cuando el usuario instala actualizaciones de Microsoft Windows Update manualmente, las actualizaciones pueden descargarse de los servidores de Microsoft en lugar de hacerlo desde el Servidor de administración. Esto es posible si el Servidor de administración aún no ha descargado estas actualizaciones. La descarga de actualizaciones de los servidores de Microsoft genera un tráfico adicional.

- **Permitir que los usuarios instalen solo actualizaciones aprobadas de Windows Update**

  Los usuarios pueden instalar todas las actualizaciones de Microsoft Windows Update que sean aplicables a sus dispositivos y que sean aprobadas por usted.

  Por ejemplo, es posible que desee verificar primero la instalación de actualizaciones en un entorno de prueba y asegurarse de que no interfieran con el funcionamiento de los dispositivos y solo entonces permitir la instalación de estas actualizaciones aprobadas en los dispositivos cliente.

  Cuando el usuario instala actualizaciones de Microsoft Windows Update manualmente, las actualizaciones pueden descargarse de los servidores de Microsoft en lugar de hacerlo desde el Servidor de administración. Esto es posible si el Servidor de administración aún no ha descargado estas actualizaciones. La descarga de actualizaciones de los servidores de Microsoft genera un tráfico adicional.

- **No permitir que los usuarios instalen actualizaciones de Windows Update**

  Los usuarios no pueden instalar actualizaciones de Microsoft Windows Update en sus dispositivos de manera manual. Todas las actualizaciones aplicables se instalan según lo configurado por usted.

  Seleccione esta opción si desea administrar la instalación de actualizaciones de forma centralizada.

  Por ejemplo, es posible que desee optimizar el programa de actualización para que la red no se sobrecargue. Puede programar actualizaciones fuera de horario, para que no interfieran con la productividad del usuario.

- En el grupo de configuración del **Modo de búsqueda de Windows Update**, puede seleccionar el modo de búsqueda de actualización:

  - **Activo**

Si se selecciona esta opción, el Servidor de administración, secundado por el Agente de red, iniciará una solicitud de un agente de Windows Update en el dispositivo cliente al origen de actualizaciones: Servidores de Windows Update o WSUS. A continuación, el Agente de red transmite la información que recibe del Agente de Windows Update al Servidor de administración.

La opción solo se activa si se selecciona la opción **Conectar al servidor de actualizaciones para actualizar los datos** de la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Esta opción está seleccionada de forma predeterminada.

- Pasivo

  Si se selecciona esta opción, el Agente de red transmite periódicamente al Servidor de administración información sobre las actualizaciones recuperadas en la última sincronización del Agente de Windows Update con el origen de actualizaciones. Si no se realiza ninguna sincronización del Agente de Windows Update con un origen de actualizaciones, la información sobre actualizaciones del Servidor de administración se volverá anticuada.

  Seleccione esta opción si desea obtener actualizaciones de la memoria caché del origen de actualizaciones.

- Desactivado

  Si selecciona esta opción, el Servidor de administración no solicita información alguna acerca de las actualizaciones.

  Seleccione esta opción si, por ejemplo, desea probar primero las actualizaciones en su dispositivo local.

- Analizar los archivos ejecutables para buscar vulnerabilidades al iniciarlos

  Si esta opción está seleccionada, los archivos ejecutables se analizan en busca de vulnerabilidades cuando se ejecutan.

  Esta opción está activada de forma predeterminada.

Administración de reinicios

En la sección **Administración de reinicios**, puede especificar la acción que debe realizarse si el sistema operativo de un dispositivo administrado se tiene que reiniciar para garantizar el uso correcto de una aplicación, su instalación o desinstalación. La configuración en la sección **Administración de reinicios** está disponible solo en dispositivos que ejecutan Windows:

- No reiniciar el sistema operativo

  Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- Reiniciar el sistema operativo automáticamente de ser necesario

Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

  En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

  Esta opción está seleccionada de forma predeterminada.

  - **Repetir solicitud cada (min)**

    Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

    Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

    Si esta opción está desactivada, la solicitud se muestra solo una vez.

  - **Forzar reinicio después de (min)**

    Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

    Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  - **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

    La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

    Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

    Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

    Esta opción está desactivada de forma predeterminada.

Uso compartido del escritorio de Windows

En la sección **Uso compartido del escritorio de Windows**, puede activar y configurar la auditoría de las acciones del administrador realizadas en un dispositivo remoto cuando se utiliza el acceso a escritorio compartido. La configuración en la sección **Uso compartido del escritorio de Windows** está disponible solo en dispositivos que ejecutan Windows:

- **Activar auditoría**

Si esta opción está activada, en el dispositivo remoto se habilita la auditoría de las acciones del administrador. Las acciones del administrador en el dispositivo remoto se registran:

- En el registro de eventos del dispositivo remoto
- En un archivo con extensión syslog ubicado en la carpeta de instalación del Agente de red en el dispositivo remoto
- En la base de datos de eventos de Kaspersky Security Center

La auditoría de las acciones del administrador puede realizarse cuando se cumplen estas condiciones:

- La licencia de Administración de vulnerabilidades y parches está en uso
- El administrador dispone del derecho para iniciar el acceso compartido al escritorio del dispositivo remoto

Si esta casilla está desactivada, se deshabilita la auditoría de las acciones del administrador en el dispositivo remoto.

Esta opción está desactivada de forma predeterminada.

- **Máscaras de archivos cuya lectura se debe supervisar**

  La lista muestra máscaras de archivos. Cuando se habilita la auditoría, la aplicación supervisa los archivos de lectura del administrador que coinciden con las máscaras y guarda información sobre la lectura de los archivos. Esta lista está disponible si se selecciona la casilla **Habilitar auditorías**. Puede modificar las máscaras de archivos y añadir otras nuevas a la lista. Cada máscara de archivos nueva se debe especificar en líneas distintas de la lista.

  De forma predeterminada, se especifican las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Máscaras de archivos cuya modificación se debe supervisar**

  La lista contiene máscaras de archivos en el dispositivo remoto. Cuando se habilita la auditoría, la aplicación supervisa los cambios realizados por el administrador en los archivos que coinciden con máscaras y guarda información sobre esas modificaciones. Esta lista está disponible si se selecciona la casilla **Habilitar auditorías**. Puede modificar las máscaras de archivos y añadir otras nuevas a la lista. Cada máscara de archivos nueva se debe especificar en líneas distintas de la lista.

  De forma predeterminada, se especifican las siguientes máscaras de archivos:*.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Administrar parches y actualizaciones

En la sección **Administrar parches y actualizaciones**, puede configurar la descarga y distribución de actualizaciones, como también la instalación de parches en los dispositivos administrados:

- **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir**

Si esta opción está activada, los parches de Kaspersky que tienen la *Sin definir* se instalarán automáticamente en los dispositivos administrados tras descargarse desde los servidores de actualización. La instalación automática de parches con el estado *indeterminado* está disponible para Kaspersky Security Center Service Pack 2 y posteriores.

Si esta opción está desactivada, los parches de Kaspersky que se hayan descargado y etiquetado con el estado *Indeterminado* solo se instalarán después de que el administrador cambie su estado a *Aprobados*.

Esta opción está activada de forma predeterminada.

- **Descargar actualizaciones y bases de datos antivirus del Servidor de administración (recomendado)**

  Si esta opción está activada, se utiliza el modelo de descarga de actualizaciones sin conexión. Cuando el Servidor de administración recibe actualizaciones, notifica al Agente de red (en los dispositivos donde está instalado) las actualizaciones que serán necesarias para las aplicaciones administradas. Cuando el Agente de red recibe la información sobre las actualizaciones, descarga por anticipado los archivos relevantes desde el Servidor de administración. En la primera conexión con el Agente de red, el Servidor de administración inicia una descarga de actualización. Una vez que el Agente de red descarga todas las actualizaciones a un dispositivo cliente, las actualizaciones estarán disponibles para las aplicaciones en ese dispositivo.

  Cuando una aplicación administrada de un dispositivo cliente intenta acceder al Agente de red para descargar actualizaciones, el Agente de red comprueba si tiene todas las actualizaciones necesarias. Si las actualizaciones se reciben desde el Servidor de administración no más de 25 horas antes de que la aplicación administrada las solicite, el Agente de red no se conecta al Servidor de administración, sino que proporciona actualizaciones desde el caché local a la aplicación administrada. Es posible que la conexión con el Servidor de administración no se establezca cuando el Agente de red proporciona actualizaciones para las aplicaciones en los dispositivos cliente, pero no se requiere conexión para la actualización.

  Si esta opción está desactivada, el modelo de descarga de actualizaciones sin conexión no se utiliza. Las actualizaciones se distribuyen de acuerdo con el calendario de la tarea de descarga de actualizaciones.

  Esta opción está activada de forma predeterminada.

Red

La sección **Red** incluye tres subsecciones:

- **Conectividad**
- **Perfiles de conexión**
- **Programación de conexiones**

En la subsección **Conectividad**, puede configurar la conexión con el Servidor de administración, activar el uso de un puerto UDP y especificar el número de puerto UDP.

- El grupo de configuración **Conectar al Servidor de administración** le permite configurar la conexión al Servidor de administración y especificar el período para la sincronización de los dispositivos cliente y el Servidor de administración:
  - **Intervalo de sincronización (min)**

El Agente de red sincroniza el dispositivo administrado con el Servidor de administración. Recomendamos que establezca el intervalo de sincronización (también conocido como heartbeat) en 15 minutos por cada 10 000 dispositivos administrados.

Si el intervalo de sincronización está configurado en menos de 15 minutos, la sincronización se realiza cada 15 minutos. Si el intervalo de sincronización está configurado en 15 minutos o más, la sincronización se realiza en el intervalo de sincronización especificado.

- **Comprimir tráfico de red**

  Si se selecciona esta opción, aumentará la velocidad de transferencia de datos del Agente de red, disminuirá la cantidad de información que se transfiere y disminuirá la carga en el Servidor de administración.

  Puede incrementarse la carga de trabajo de la CPU del dispositivo cliente.

  De forma predeterminada, esta opción está activada.

- **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**

  Si se selecciona esta opción, se añadirá un puerto UDP (necesario para el funcionamiento del Agente de red) a la lista de exclusiones del firewall de Microsoft Windows.

  Esta opción está activada de forma predeterminada.

- **Usar conexión SSL**

  Si esta opción está activada, la conexión al Servidor de administración se establece a través de un puerto seguro a través de SSL.

  Esta opción está activada de forma predeterminada.

- **Usar puerta de enlace de conexión del punto de distribución (si está disponible) en la configuración de la conexión predeterminada**

  Si se selecciona esta opción, la puerta de enlace de conexión en el punto de distribución se utilizará con la configuración especificada en las propiedades del grupo de administración.

  Esta opción está activada de forma predeterminada.

- **Usar puerto UDP**

  Si necesita que los dispositivos administrados se conecten al Servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado de conexión al Servidor proxy de KSN es 15111.

- **Número de puerto UDP**

En este campo se introduce el nombre del puerto UDP. El número de puerto predeterminado es el 15000.

Se usa el sistema decimal para los registros.

Si un dispositivo cliente ejecuta Windows XP Service Pack 2, el firewall integrado bloqueará el puerto UDP 15000. Este puerto debe abrirse manualmente.

- Usar un punto de distribución para forzar la conexión al Servidor de administración

  Seleccione esta opción si selecciona la opción **Utilice este punto de distribución como servidor push** en la ventana de configuración del punto de distribución. De lo contrario, el punto de distribución no funcionará como servidor push.

En la subsección **Perfiles de conexión** de la sección **Red**, puede especificar la configuración de ubicación de red y habilitar el modo fuera de la oficina cuando el Servidor de administración no esté disponible. Los ajustes de la sección **Perfiles de conexión** están disponibles solo en dispositivos que ejecutan Windows:

- Configuración de la ubicación de red

  La configuración de la ubicación de red define las características de la red a la que está conectado el dispositivo cliente y especifica las reglas para el cambio del Agente de red de un perfil de conexión Servidor de administración a otro cuando se alteran esas características de red.

- Perfiles de conexión al Servidor de administración

  En esta sección se pueden ver y añadir perfiles para la conexión del Agente de red al Servidor de administración. En esta sección, también puede crear reglas para cambiar el Agente de red a Servidores de administración diferentes cuando ocurren los siguientes eventos:

  - Cuando un dispositivo cliente se conecta a otra red local
  - Cuando un dispositivo pierde conexión con la red local de la organización
  - Cuando se cambia la dirección de la puerta de enlace de conexión o se modifica la dirección del servidor DNS

  Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

- Activar modo Fuera de la oficina cuando el Servidor de administración no esté disponible

  Si se selecciona esta opción y en el caso de que la conexión se realice con este perfil, las aplicaciones instaladas en el dispositivo cliente utilizan los perfiles de directivas para dispositivos en modo fuera de la oficina, además de directivas fuera de la oficina. Si no se ha definido una directiva fuera de la oficina en la aplicación, se utilizará la directiva activa.

  Si esta opción está desactivada, las aplicaciones utilizarán las directivas activas.

  Esta opción está desactivada de forma predeterminada.

En la subsección **Programación de conexiones**, se pueden especificar los intervalos de tiempo en los que el Agente de red envía los datos al Servidor de administración:

- Conectar cuando sea necesario

Si se selecciona esta opción, la conexión se establecerá cuando el Agente de red tenga que enviar datos al Servidor de administración.

Esta opción está seleccionada de forma predeterminada.

- **Conectarse en los intervalos de tiempo especificados**

  Si se selecciona esta opción, el Agente de red se conectará al Servidor de administración a una hora concreta. Se pueden añadir varios períodos de tiempo de conexión.

Sondeo de la red realizado por los puntos de distribución

En la sección **Sondeo de la red realizado por los puntos de distribución**, puede configurar el sondeo automático de la red. La configuración de sondeo está disponible solo en dispositivos que ejecutan Windows. Puede utilizar las siguientes opciones para habilitar el sondeo y establecer su frecuencia:

- **Red de Windows**

  Si esta opción está activada, el Servidor de administración sondea automáticamente la red según la planificación que ha configurado al hacer clic en los enlaces **Programar un sondeo rápido** y **Programar un sondeo completo**.

  Si esta opción está desactivada, el Servidor de administración no sondea la red.

  El intervalo de detección de dispositivos para las versiones del Agente de red anteriores a 10.2 se pueden configurar en los campos **Frecuencia de los sondeos desde los dominios de Windows (min)** y **Frecuencia de los sondeos de la red (min)**. Los campos están disponibles si la opción está activada.

  Esta opción está desactivada de forma predeterminada.

- **Zeroconf**

  Si esta opción está activada, el punto de distribución automáticamente sondea la red con dispositivos IPv6 mediante el uso de las redes de configuración cero (también denominadas *Zeroconf*). En este caso, el sondeo de rangos de IP activados se ignora, porque el punto de distribución sondea toda la red.

  Para empezar a usar Zeroconf, se deben cumplir las siguientes condiciones:

  - El punto de distribución debe ejecutar Linux.
  - Debe instalar la utilidad avahi-browse en el punto de distribución.

  Si esta opción está desactivada, el punto de distribución no sondea las redes con dispositivos IPv6.

  Esta opción está desactivada de forma predeterminada.

- **Rangos IP**

  Si esta opción está activada, el Servidor de administración sondea automáticamente los rangos de IP de acuerdo con la programación que ha configurado al hacer clic en el enlace **Programar sondeo**.

  Si esta opción está desactivada, el Servidor de administración no sondea los rangos de IP.

  La frecuencia de sondeos de rangos IP en las versiones del Agente de red anteriores a 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo está disponible si la opción está activada.

  Esta opción está desactivada de forma predeterminada.

- Usuario de Active Directory

  Si esta opción está activada, el Servidor de administración sondea automáticamente Active Directory según la planificación que ha configurado al hacer clic en el enlace **Programar sondeo**.

  Si esta opción está desactivada, el Servidor de administración no sondea Active Directory.

  La frecuencia de sondeo de Active Directory en las versiones de Agente de red anteriores a la 10.2 se puede configurar en el campo **Intervalo de sondeo (min)**. El campo está disponible si esta opción está activada.

  Esta opción está desactivada de forma predeterminada.

Configuración de red para puntos de distribución

En la sección **Configuración de red para puntos de distribución**, puede especificar la configuración de acceso a Internet:

- **Usar servidor proxy**
- **Dirección**
- **Número de puerto**
- No utilizar el servidor proxy para direcciones locales

  Si se selecciona esta opción, no se utilizará el servidor proxy para conectarse a los dispositivos de la red local.

  Esta opción está desactivada de forma predeterminada.

- Autenticación del servidor proxy

  Si se activa esta casilla, podrá especificar las credenciales para la autenticación del servidor proxy en los campos de entrada.

  De forma predeterminada, esta opción está desactivada.

- **Nombre de usuario**
- **Contraseña**

Proxy de KSN (puntos de distribución)

En la sección **Proxy de KSN (puntos de distribución)**, puede configurar la aplicación para utilizar el punto de distribución para reenviar solicitudes de KSN desde los dispositivos administrados:

- Activar el proxy de KSN en el punto de distribución

El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico en la red.

El punto de distribución envía a Kaspersky las estadísticas de KSN, que se incluyen en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se guarda en %Archivos de programa%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Esta opción está desactivada de forma predeterminada. Esta opción solo se activa si las opciones **Utilizar el Servidor de administración como servidor proxy** y **Acepto usar Kaspersky Security Network** están activadas en la ventana de propiedades del Servidor de administración.

Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y activar el proxy de KSN en ese nodo.

- **Reenviar solicitudes de KSN al Servidor de administración**

  El punto de distribución reenvía las solicitudes KSN de los dispositivos administrados al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- **Acceder a la nube de KSN/KSN privada directamente a través de Internet**

  El punto de distribución reenvía las solicitudes de KSN de los dispositivos administrados a KSN Cloud o KSN privada. Las solicitudes de KSN generadas en el punto de distribución también se envían directamente a KSN Cloud o KSN privada.

  Los puntos de distribución que tienen instalado el Agente de red versión 11 (o versiones anteriores) no pueden acceder a KSN Privada directamente. Si desea reconfigurar los puntos de distribución para enviar solicitudes KSN a KSN Privada, active la opción **Reenviar solicitudes de KSN al Servidor de administración** para cada punto de distribución.

  Los puntos de distribución que tienen instalado el Agente de red versión 12 (o versiones posteriores) pueden acceder a KSN privada directamente.

- **Puerto**

  El número del puerto de TCP que los dispositivos administrados utilizarán para conectar al Servidor proxy de KSN. El número de puerto predeterminado es el 13111.

- **Puerto UDP**

  Si necesita que los dispositivos administrados se conecten al Servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado de conexión al Servidor proxy de KSN es 15111.

Actualizaciones (puntos de distribución)

En la sección **Actualizaciones (puntos de distribución)**, puede activar la función de descarga de archivos diff, para que los puntos de distribución reciban actualizaciones en forma de archivos diff desde los servidores de actualización de Kaspersky.

Historial de revisión

En esta pestaña, puede ver la lista de revisiones de la directiva y revertir los cambios realizados en la directiva, si es necesario.

Comparación de funciones de los sistemas operativos del Agente de red

La siguiente tabla muestra qué configuración de directiva del Agente de red puede usar para configurar el Agente de red con un sistema operativo específico.

Configuración de la directiva del Agente de red: comparación por sistemas operativos

Sección Directiva	Windows	Mac	Linux
Control de aplicaciones	✓	✓	✓
Configuración de eventos	✓	✓	✓
Configuración	✓	✓	✓ Solo las opciones **Tamaño máximo de la cola del evento, en MB** y **La aplicación podrá obtener información adicional sobre la directiva en el dispositivo** están disponibles.
Repositorios	✓	–	✓ Solo las opciones **Detalles de las aplicaciones instaladas** y **Detalles de registro de hardware** están disponibles.
Vulnerabilidades y actualizaciones de software	✓	–	–
Administración de reinicios	✓	–	–
Uso compartido del escritorio de Windows	✓	–	–
Administrar parches y actualizaciones	✓	–	–
Red → Conectividad	✓	✓	✓ Excepto la opción **Abrir puertos del Agente de red en el Firewall de Microsoft Windows**.
Red → Perfiles de conexión	✓	✓	–
Red → Programación de conexiones	✓	✓	✓
Sondeo de la red realizado	✓	–	✓ Solo las opciones **Zeroconf** y **Rangos IP** están disponibles.

por los puntos de distribución	Solo las opciones **Red de Windows**, **Rangos IP**, y **Usuario de Active Directory** están disponibles.		
Configuración de red para puntos de distribución	✓	✓	✓
Proxy de KSN (puntos de distribución)	✓	–	–
Actualizaciones (puntos de distribución)	✓	–	–
Historial de revisión	✓	✓	✓

Configuración manual de la directiva de Kaspersky Endpoint Security

Esta sección proporciona recomendaciones sobre cómo configurar la directiva de Kaspersky Endpoint Security, que es creada por el Asistente de inicio rápido de Kaspersky Security Center 14 Web Console. La configuración se realiza en la ventana de propiedades de la directiva.

Al modificar un ajuste de configuración, tenga en cuenta que debe hacer clic en el icono de bloqueo sobre el ajuste relevante a fin de permitir que se use su valor en una estación de trabajo.

Configuración de la directiva en la sección Protección avanzada contra amenazas

En esta sección se describen las acciones de configuración adicionales que recomendamos realizar en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Protección contra amenazas avanzadas**.

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

Para especificar la configuración recomendada KSN:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.
3. En las propiedades de la directiva, vaya a **Configuración de la aplicación → Protección contra amenazas avanzada → Kaspersky Security Network**.

4. Asegúrese de que la opción **Usar el proxy de KSN** esté activada. Utilice esta opción para redistribuir y optimizar el tráfico en la red.

5. [opcional] Active el uso de servidores KSN si el servicio de proxy de KSN no está disponible. Los servidores de KSN pueden estar localizados en el lado de Kaspersky (cuando se usa KSN global) o en el lado de terceros (cuando se usa KSN privada).

6. Haga clic en **Aceptar**.

Se especifican las configuraciones KSN recomendadas.

Configuración de la directiva en la sección Protección frente a amenazas básicas

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

A continuación, se describen las acciones de configuración adicionales que recomendamos que realice en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Protección frente a amenazas básicas**.

Sección Protección frente a amenazas básicas, subsección Firewall

Compruebe la lista de redes en las propiedades de la directiva. La lista puede no contener todas las redes.

Para comprobar la lista de redes, siga estos pasos:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.

2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.

3. En las propiedades de la directiva, vaya a **Configuración de la aplicación → Protección de amenaza esencial → Firewall**.

4. Debajo de **Redes disponibles**, haga clic en el enlace **Configuración de red**.

Se abre la ventana **Conexiones de red**. Esta ventana muestra la lista de redes.

Sección Protección frente a amenazas básicas, subdivisión Protección frente a amenazas en archivos

La activación del análisis de las unidades de red puede aplicar una carga significativa a las unidades de red. Resulta más cómodo realizar un análisis indirecto en los servidores de archivo.

Para desactivar el análisis de unidades de red:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.

2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.

3. En las propiedades de la directiva, vaya a **Configuración de la aplicación** → **Protección de amenaza esencial** → **Protección frente a amenazas en archivos**.

4. En **Cobertura de la protección**, desactive la opción **Todas las unidades de red**.

5. Haga clic en **Aceptar**.

El análisis de unidades de red está desactivado.

Configuración de la directiva en la sección Configuración general

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

A continuación, se describen las acciones de configuración avanzadas que recomendamos realizar en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Configuración general**.

Sección Configuración general, subsección Informes y Almacenamiento

Para desactivar la información de guardado sobre los módulos de software instalados:

1. En el menú principal, vaya a **DISPOSITIVOS** → **DIRECTIVAS Y PERFILES**.

2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.

3. En las propiedades de la directiva, vaya a **Configuración de la aplicación** → **Configuración General** → **Informes y almacenamiento**.

4. En **Transferencia de datos al Servidor de administración**, desactive la casilla de verificación **Acerca de las aplicaciones iniciadas** si todavía está activada en la directiva de nivel superior.

   Cuando esta casilla está activada, la base de datos del Servidor de administración guarda la información acerca de todas las versiones de todos los módulos de software en los dispositivos en red. Esta información puede requerir una cantidad significativa de espacio en el disco en la base de datos de Kaspersky Security Center (docenas de gigabytes).

La información sobre los módulos de software instalados ya no se guarda en la base de datos del Servidor de administración.

Sección Configuración general, subsección Interfaz

Si la protección antivirus en la red de la organización debe administrarse en modo centralizado a través de la Consola de administración, especifique la configuración de la interfaz como se describe a continuación.

Para especificar la configuración de interfaz recomendada:

1. En la pestaña **DISPOSITIVOS**, seleccione **DIRECTIVAS Y PERFILES**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.
3. En las propiedades de la directiva, vaya a **Configuración de la aplicación → Configuración General → Interfaz**.
4. En **Interacción con el usuario**, seleccione la opción **Sin interfaz**. Esto deshabilita la visualización de la interfaz de usuario de Kaspersky Endpoint Security para Windows en las estaciones de trabajo.
5. En **Protección de contraseña**, habilite el interruptor de palanca. Esto reduce el riesgo de cambios no autorizados o no deseados en la configuración de Kaspersky Endpoint Security para Windows en estaciones de trabajo.

Se especifican las configuraciones recomendadas para la interfaz de Kaspersky Endpoint Security para Windows.

Configuración de la directiva en la sección Configuración de eventos

Para evitar el desbordamiento de la base de datos del Servidor de administración, recomendamos que solo guarde eventos importantes en la base de datos.

Para configurar el registro de eventos importantes en la base de datos del Servidor de administración:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en la directiva de Kaspersky Endpoint Security para Windows.

   Se abrirá la ventana de propiedades de la directiva seleccionada.
3. En las propiedades de la directiva, abra la pestaña **Configuración de eventos**.
4. En la sección **Crítico**, haga clic en **Agregar evento** y seleccione las casillas de verificación junto a los siguientes eventos solamente:
   - Contrato de licencia violado
   - La ejecución automática de la aplicación está desactivada
   - Error de activación
   - Se detectó una amenaza activa. Iniciar Desinfección avanzada
   - La desinfección no es posible
   - Se detectó un enlace peligroso abierto anteriormente
   - El proceso finalizó
   - Actividad de red bloqueada

- Se detectó un ataque de red
- Inicio de aplicación prohibido
- Acceso denegado (bases locales)
- Acceso denegado (KSN)
- Error de actualización local
- No se pueden iniciar dos tareas al mismo tiempo
- Error en la interacción con Kaspersky Security Center
- No todos los componentes fueron actualizados
- Error al aplicar las reglas de cifrado/descifrado del archivo
- Error al activar el modo portátil
- Error al desactivar el modo portátil
- No se pudo cargar el módulo de cifrado
- La directiva no se puede aplicar
- Error al cambiar los componentes de la aplicación

5. Haga clic en **Aceptar**.
6. En la sección **Fallo operativo**, haga clic en **Agregar evento** y seleccione solamente la casilla de verificación junto al evento «Configuración incorrecta de la tarea». Configuración no aplicada".
7. Haga clic en **Aceptar**.
8. En la sección **Advertencia**, haga clic en **Agregar evento** y seleccione las casillas de verificación junto a los siguientes eventos solamente:
   - La autoprotección está desactivada
   - Los componentes de protección están desactivados
   - Clave de reserva incorrecta
   - Se ha detectado software legítimo que puede utilizarse para dañar su ordenador o sus datos personales (bases locales)
   - Se ha detectado software legítimo que puede utilizarse para dañar su ordenador o sus datos personales (KSN)
   - Objeto eliminado
   - Objeto desinfectado
   - El usuario ha decidido excluirse de la directiva de cifrado

- Archivo restaurado de KATA Quarantine
- Archivo puesto en la cuarentena de KATA
- Mensaje de bloqueo de inicio de aplicación al administrador
- Mensaje de bloqueo de acceso a dispositivo al administrador
- Mensaje de bloqueo de acceso a página web al administrador

9. Haga clic en **Aceptar**.
10. En la sección **Información**, haga clic en **Agregar evento** y seleccione las casillas de verificación junto a los siguientes eventos solamente:
    - Se creó una copia de seguridad de la versión anterior
    - Inicio de la aplicación prohibido en el modo de prueba
11. Haga clic en **Aceptar**.

Se configura el registro de eventos importantes en la base de datos del Servidor de administración.

Configuración manual de la tarea de actualización de grupo para Kaspersky Endpoint Security

La opción de programación óptima y recomendada para Kaspersky Endpoint Security es **Cuando se descargan nuevas actualizaciones en el repositorio** cuando la casilla de verificación **Usar el retraso aleatorio automáticamente para el inicio de tareas** está seleccionada.

Conceder acceso sin conexión al dispositivo externo que ha bloqueado Control de dispositivos

En el componente Control de dispositivos de la directiva de Kaspersky Endpoint Security para Windows, puede administrar el acceso de los usuarios a los dispositivos externos que están instalados en el dispositivo cliente o conectados a este (por ejemplo, discos duros, cámaras o módulos de Wi-Fi). Esto le permite proteger el dispositivo cliente de infecciones cuando se conectan dispositivos externos de ese tipo, así como evitar la pérdida o fuga de datos.

Si necesita otorgar acceso temporal al dispositivo externo bloqueado por Control de dispositivos pero no puede añadir el dispositivo a la lista de dispositivos de confianza, puede otorgar un acceso temporal sin conexión. El acceso sin conexión significa que el dispositivo cliente no tiene acceso a la red.

> Puede conceder acceso sin conexión al dispositivo externo bloqueado por Control de dispositivos solo si en la configuración de la directiva de Kaspersky Endpoint Security para Windows, en la sección Control de dispositivos, la opción **Permitir solicitud de acceso temporal** está activada.

Para conceder acceso sin conexión al dispositivo externo que ha bloqueado Control de dispositivos, se siguen estas etapas:

1. En la ventana de diálogo de Kaspersky Endpoint Security para Windows, el usuario del dispositivo que desea acceder al dispositivo externo bloqueado, genera un archivo de solicitud de acceso y lo envía al administrador de Kaspersky Security Center.

2. Al recibir esta solicitud, el administrador de Kaspersky Security Center crea un archivo clave de acceso y lo envía al usuario del dispositivo.

3. En la ventana de diálogo de Kaspersky Endpoint Security para Windows, el usuario del dispositivo activa el archivo clave de acceso y puede acceder de manera temporal al dispositivo externo.

Para conceder acceso temporal al dispositivo externo que ha bloqueado Control de dispositivos, realice lo siguiente:

1. Seleccione **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, seleccione el dispositivo de usuario que solicita acceso al dispositivo externo bloqueado por Control de dispositivos.

   Solo puede seleccionar un dispositivo.

3. Encima de la lista de dispositivos administrados, haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.

   Se abre la ventana **Conceder acceso en modo Desconectado**.

4. En la ventana **Conceder acceso en modo Desconectado**, en la ficha **Control de dispositivos**, haga clic en el botón **Examinar**.

   Se abre la ventana estándar **Seleccionar archivo de solicitud de acceso** de Microsoft Windows.

5. En la ventana **Seleccionar archivo de solicitud de acceso**, seleccione el archivo de solicitud de acceso que le envió el usuario y haga clic en el botón **Abrir**.

   Se muestran los detalles del dispositivo bloqueado al que el usuario ha solicitado acceder.

6. Especifique el valor de la configuración de **Duración del acceso**.

   Esta configuración define la cantidad de tiempo que concede al usuario para que acceda al dispositivo bloqueado. El valor predeterminado es el valor que ha especificado el usuario al crear el archivo de solicitud de acceso.

7. Especifique el valor de la configuración del **Período de activación**.

   Esta configuración define el período durante el cual el usuario puede activar el acceso al dispositivo bloqueado con la clave de acceso provista.

8. Haga clic en el botón **Guardar**.

   Al hacerlo, se abre la ventana estándar **Guardar clave de acceso** de Microsoft Windows.

9. Seleccione la carpeta de destino en la que desea guardar el archivo que contiene la clave de acceso para el dispositivo bloqueado.

10. Haga clic en el botón **Guardar**.

En conclusión, cuando envía al usuario el archivo con la clave de acceso para que lo active en la ventana de diálogo de Kaspersky Endpoint Security para Windows, el usuario tiene acceso temporal al dispositivo bloqueado durante el período especificado.

Eliminar aplicaciones o actualizaciones de software de forma remota

Para eliminar aplicaciones o actualizaciones de software de forma remota desde dispositivos seleccionados:

1. En la ventana principal de la aplicación, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance por el Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Desinstalar aplicación en remoto**.
4. Especifique el nombre para la tarea que está creando.

   El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Seleccionar dispositivos a los que se asignará la tarea.
6. Seleccione qué tipo de software desea eliminar y luego seleccione las aplicaciones, las actualizaciones o los parches específicos que desee eliminar:

   - **Desinstalar aplicación administrada**

     Se muestra una lista de aplicaciones de Kaspersky. Seleccione la aplicación que desee eliminar.

   - **Desinstalar aplicación incompatible**

     Se muestra una lista de aplicaciones incompatibles con las aplicaciones de seguridad de Kaspersky o Kaspersky Security Center. Seleccione las casillas de verificación al lado de las aplicaciones que desea eliminar.

   - **Desinstalar aplicación del Registro de aplicaciones**

De forma predeterminada, los Agentes de red envían información al Servidor de administración sobre las aplicaciones instaladas en los dispositivos administrados. La lista de aplicaciones instaladas se almacena en el registro de aplicaciones.

Para seleccionar una aplicación del registro de aplicaciones:

a. Haga clic en el campo **Aplicación que se va a desinstalar** y luego seleccione la aplicación que desea eliminar.

b. Especifique las opciones de desinstalación:

- Modo de desinstalación

  Seleccione cómo desea eliminar la aplicación:

  - **Definir comando de desinstalación automáticamente**

    Si la aplicación tiene un comando de desinstalación definido por el proveedor de la aplicación, Kaspersky Security Center usa este comando. Le recomendamos que seleccione esta opción.

  - **Especificar comando de desinstalación**

    Seleccione esta opción si desea especificar su propio comando para la desinstalación de la aplicación.

    Le recomendamos que primero intente eliminar la aplicación utilizando la opción **Definir comando de desinstalación automáticamente**. Si falla la desinstalación mediante el comando definido automáticamente, utilice su propio comando.

    Escriba un comando de instalación en el campo y luego especifique la siguiente opción:

    Usar este comando para desinstalación únicamente cuando el comando predeterminado no se detecte automáticamente

    Kaspersky Security Center comprueba si la aplicación seleccionada tiene o no un comando de desinstalación definido por el proveedor de la aplicación. Si se encuentra el comando, Kaspersky Security Center lo usará en lugar del comando especificado en el campo **Comando para la desinstalación de la aplicación**.

    Le recomendamos que active esta opción.

- Reiniciar después de la desinstalación correcta de la aplicación

  Si la aplicación requiere que se reinicie el sistema operativo en el dispositivo administrado después de una desinstalación exitosa, el sistema operativo se reinicia automáticamente.

- Desinstalar la actualización especificada de la aplicación, parche o aplicación de terceros

Se muestra una lista de actualizaciones, parches y aplicaciones de terceros. Seleccione el elemento que desee eliminar.

La lista que se muestra es una lista general de aplicaciones y actualizaciones, y no corresponde a las aplicaciones y actualizaciones instaladas en los dispositivos administrados. Antes de seleccionar un elemento, recomendamos asegurarse de que la aplicación o la actualización estén instaladas en los dispositivos definidos en la cobertura de la tarea. Puede ver la lista de dispositivos en los que está instalada la aplicación o la actualización a través de la ventana de propiedades.

Para ver la lista de dispositivos:

a. Haga clic en el nombre de la aplicación o actualización.

Se abre la ventana de propiedades.

b. Abra la sección **Dispositivos**.

También puede ver la lista de aplicaciones y actualizaciones instaladas en la ventana de propiedades del dispositivo.

7. Especifique cómo los dispositivos cliente descargarán la utilidad de Desinstalación:

- **Usando el Agente de red**

  Los archivos se entregan a los dispositivos cliente mediante el Agente de red instalado en dichos dispositivos cliente.

  Si esta opción está deshabilitada, los archivos se entregan mediante las herramientas de Microsoft Windows.

  Recomendamos que esta opción si la tarea se ha asignado a dispositivos que tienen instalados Agentes de red.

- **Usando los recursos del sistema operativo mediante el Servidor de administración**

  Los archivos se transmiten a los dispositivos del cliente mediante herramientas de Microsoft Windows a través del Servidor de administración. Puede activar esta opción si no hay ningún Agente de red instalado en el dispositivo cliente, pero el dispositivo cliente está en la misma red que el Servidor de administración.

- **Usando los recursos del sistema operativo mediante puntos de distribución**

  Los archivos se transmiten a los dispositivos cliente mediante el uso de herramientas del sistema operativo a través de los puntos de distribución. Se puede activar esta opción si existe al menos un punto de distribución en la red.

  Si se activa la opción **Usando el Agente de red**, los archivos se entregan mediante herramientas del sistema operativo solo si los recursos del Agente de red no están disponibles.

- **Número máximo de descargas concurrentes**

  El número máximo permitido de dispositivos cliente a los que el Servidor de administración puede transmitir simultáneamente los archivos. Cuanto mayor sea este número, más rápido se desinstalará la aplicación, pero la carga en el Servidor de administración es mayor.

- **Número máximo de intentos de desinstalación**

Si, al ejecutar la tarea *Desinstalar aplicación en remoto*, Kaspersky Security Center no logra desinstalar una aplicación en un dispositivo administrado dentro del número de intentos de instalación especificado por el parámetro, Kaspersky Security Center deja de enviar la utilidad de Desinstalación a este dispositivo administrado y ya no inicia el instalador en el dispositivo.

El parámetro **Número máximo de intentos de desinstalación** le permite guardar los recursos del dispositivo administrado y reducir el tráfico (desinstalación, ejecución de archivos MSI y mensajes de error).

Los intentos de inicio de tarea reiterados pueden indicar un problema en el dispositivo que impide la desinstalación. El administrador debe resolver el problema dentro del número especificado de intentos de desinstalación y luego reiniciar la tarea (manualmente o mediante una programación).

Si finalmente no se logra realizar la desinstalación, el problema se considera irresoluble y cualquier otro inicio de tarea se percibe como costoso en cuanto a consumo innecesario de recursos y tráfico.

Cuando se crea la tarea, el contador de intentos se fija en `0`. Cada intento del instalador que devuelve un error en el dispositivo aumenta la lectura del contador.

Si se ha superado el número de intentos especificados en el parámetro y el dispositivo está listo para la desinstalación de la aplicación, puede aumentar el valor del parámetro **Número máximo de intentos de desinstalación** e iniciar la tarea de desinstalación de la aplicación. O bien, puede crear una nueva tarea *Desinstalar aplicación en remoto*.

- **Verificar el tipo de sistema operativo antes de descargar**

  Antes de transmitir los archivos a los dispositivos cliente, Kaspersky Security Center verifica si la configuración de la utilidad de Desinstalación puede aplicarse al sistema operativo del dispositivo cliente. Si la configuración no puede aplicarse, Kaspersky Security Center no transmite los archivos y no intenta desinstalar la aplicación. Por ejemplo, para desinstalar una aplicación de Windows de los dispositivos de un grupo de administración que incluye dispositivos que ejecutan varios sistemas operativos, puede asignar la tarea de desinstalación al grupo de administración y luego activar esta opción para omitir los dispositivos que ejecutan un sistema operativo que no sea Windows.

8. Especifique la configuración de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- **Reiniciar el dispositivo**

  Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  Si esta opción está desactivada, la solicitud se muestra solo una vez.

- **Reiniciar después de (min)**

  Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

9. Si es necesario, añada las cuentas que se utilizarán para iniciar la tarea de desinstalación remota:

- **No es necesaria una cuenta (Agente de red instalado)**

  Si se selecciona esta opción, no tiene que especificar la cuenta bajo la que se ejecutará el instalador de aplicación. La tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

  Si el Agente de red no se ha instalado en dispositivos cliente, esta opción no está disponible.

- **Se necesita una cuenta (para la instalación sin Agente de red)**

Si se selecciona esta opción, puede especificar la cuenta bajo la que se ejecutará el instalador de aplicación. Puede especificar la cuenta de usuario si el Agente de red no se ha instalado en los dispositivos para los cuales está asignada la tarea.

Puede especificar varias cuentas de usuario si, por ejemplo, ninguna de ellas tiene todos los derechos requeridos en todos los dispositivos a los que se asignó esta tarea. En este caso, todas las cuentas que se han agregado se utilizan para ejecutar la tarea, en orden consecutivo de arriba abajo.

Si no se agrega ninguna cuenta, la tarea se ejecutará en la cuenta en la que se está ejecutando el servicio del Servidor de administración.

10. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

11. Haga clic en el botón **Finalizar**.

    La tarea se crea y se muestra en la lista de tareas.

12. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea.

14. Haga clic en el botón **Guardar**.

15. Ejecute la tarea manualmente o espere a que se inicie de acuerdo con la programación que especificó en la configuración de la tarea.

Al finalizar la tarea de desinstalación remota, se eliminará la aplicación seleccionada de los dispositivos seleccionados.

Devolver un objeto a una revisión anterior

Puede revertir los cambios realizados en un objeto, si es necesario. Por ejemplo, es posible que tenga que revertir la configuración de una directiva a su estado en una fecha específica.

Para revertir los cambios realizados en un objeto:

1. En la ventana de propiedades del objeto, abra la pestaña **Historial de revisión**.

2. En la lista de revisiones de objetos, seleccione la revisión en la que quiere revertir los cambios.

3. Haga clic en el botón **Revertir**.

4. Haga clic en **Aceptar** para confirmar la operación.

El objeto se revierte ahora a la revisión seleccionada. La lista de revisiones de objetos muestra un registro de la acción que se tomó. La descripción de la revisión muestra la información sobre el número de la revisión a la cual revertió el objeto.

La operación de revertir los cambios solo está disponible para objetos de directiva y tareas.

Cambio de prioridad de las reglas de movimiento de dispositivos

Todas las reglas de movimiento de dispositivos tienen prioridades.

Para aumentar o disminuir la prioridad de una regla de movimiento:

use el ratón para desplazar la regla hacia arriba o hacia abajo en la lista, respectivamente.

Tareas

Esta sección describe tareas utilizadas por Kaspersky Security Center.

Acerca de las tareas

Kaspersky Security Center administra las aplicaciones de seguridad de Kaspersky instaladas en dispositivos mediante la creación y ejecución de *tareas*. Las tareas son necesarias para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software, y realizar otras acciones en las aplicaciones.

Las tareas para una aplicación específica se pueden crear utilizando Kaspersky Security Center 14 Web Console solo si el complemento de administración para esa aplicación está instalado en el Servidor de Kaspersky Security Center 14 Web Console.

Las tareas se pueden realizar en el Servidor de administración y en los dispositivos.

Las tareas que se realizan en el Servidor de administración incluyen lo siguiente:

- Distribución automática de informes
- Descargar actualizaciones en el repositorio
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de bases de datos

Los siguientes tipos de tareas se realizan en dispositivos:

- *Tareas locales*: tareas que se realizan en un dispositivo específico

  Las tareas locales pueden ser modificadas por el administrador usando herramientas de la Consola de administración, o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de la aplicación de seguridad). Si una tarea local ha sido modificada simultáneamente por el administrador y el usuario de un dispositivo administrado, los cambios hechos por el administrador entrarán en vigor, ya que tienen una prioridad más alta.

- *Tareas de grupo*: tareas que se realizan en todos los dispositivos de un grupo específico

A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Las tareas de grupo también afectan (opcionalmente) los dispositivos que se han conectado a Servidores de administración virtuales y secundarios desplegados en ese grupo o cualquiera de sus subgrupos.

- *Tareas globales*: tareas que se realizan en un conjunto de dispositivos, independientemente de si se incluyen en algún grupo.

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede realizar cambios en la configuración de tareas, ver el progreso de las tareas y copiar, exportar, importar y eliminar tareas.

Una tarea se inicia en un dispositivo solo si la aplicación para la que se creó la tarea se está en ejecución.

Los resultados de la ejecución de tareas se guardan en el registro de eventos del sistema operativo de cada dispositivo, el registro de eventos del sistema operativo del Servidor de administración, y en la base de datos del Servidor de administración.

No incluya datos confidenciales en la configuración de la tarea. Por ejemplo, no especifique la contraseña del administrador de dominio.

Acerca de la cobertura de la tarea

La *cobertura de una tarea* es el conjunto de dispositivos en los que se realiza la tarea. Los tipos de cobertura son los siguientes:

- Para una *tarea local*, la cobertura es el propio dispositivo.
- Para una *tarea del Servidor de administración*, la cobertura es el Servidor de administración.
- Para una *tarea de grupo*, la cobertura es la lista de dispositivos incluidos en el grupo.

Al crear una *tarea global*, puede usar los siguientes métodos para especificar su cobertura:

- Especificar determinados dispositivos manualmente.

  Puede utilizar una dirección IP (o un rango IP), un nombre NetBIOS o un nombre DNS como la dirección del dispositivo.

- Importación de una lista de dispositivos desde un archivo .TXT con las direcciones del dispositivo que se añadirán (cada dirección debe ubicarse en una línea individual).

  Si importa una lista de dispositivos desde un archivo o la crea manualmente, y si los dispositivos se identifican por sus nombres, la lista solo podrá contener dispositivos para los cuales ya se haya introducido información en la base de datos del Servidor de administración. Además, la información debe haberse introducido cuando se conectaron esos dispositivos o durante la detección de dispositivos.

- Especificar selección de dispositivos.

Con el tiempo, la cobertura de la tarea cambia a medida que el conjunto de dispositivos incluidos en la selección cambia. Puede realizarse una selección de dispositivos sobre la base de atributos del dispositivo, incluido el software instalado en un dispositivo y sobre la base de etiquetas asignadas a dispositivos. La selección de dispositivos es la forma más flexible de especificar la cobertura de una tarea.

Las tareas para selecciones de dispositivos siempre se ejecutan de forma programada por el Servidor de administración. Estas tareas no se pueden ejecutar en dispositivos que carecen de conexión con el Servidor de administración. Las tareas cuya cobertura se especifica mediante otros métodos se ejecutan directamente en los dispositivos y, por lo tanto, no dependen de la conexión del dispositivo al Servidor de administración.

Las tareas para selecciones de dispositivos no se ejecutan en la hora local de un dispositivo; en su lugar, se ejecutan en la hora local del Servidor de administración. Las tareas cuya cobertura se especifica mediante otros métodos se ejecutan en la hora local de un dispositivo.

Creación de una tarea

Para crear una tarea:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Siga sus instrucciones.
3. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.
4. Haga clic en el botón **Finalizar**.

La tarea se crea y se muestra en la lista de tareas.

Inicio de una tarea de forma manual

La aplicación inicia las tareas según la configuración de programación especificada en las propiedades de cada tarea. Puede iniciar una tarea de forma manual en cualquier momento.

Para iniciar una tarea manualmente, haga lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. En la lista de tareas, seleccione la casilla de verificación junto a la tarea que desea iniciar.
3. Haga clic en el botón **Iniciar**.

Se iniciará la tarea. Puede verificar el estado de la tarea en la columna **Estado** o haciendo clic en el botón **Resultado**.

Visualización de la lista de tareas

Puede ver la lista de tareas que se crean en Kaspersky Security Center.

Para ver la lista de tareas:

En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.

Se muestra la lista de tareas. Las tareas se agrupan según los nombres de las aplicaciones con las que están relacionadas. Por ejemplo, la tarea Desinstalar aplicación en remoto está relacionada con el Servidor de administración, mientras que la tarea Buscar vulnerabilidades y actualizaciones requeridas se refiere al Agente de red.

Para ver las propiedades de una tarea:

Haga clic en el nombre de la tarea.

Aparece la ventana de propiedades de la tarea se con varias pestañas con nombre. Por ejemplo, **Tipo de tarea** se muestra en la pestaña **Control de aplicaciones** y la programación de tareas, en la pestaña **Programación**.

Configuración general de la tareas

Esta sección indica los ajustes que puede ver y especificar para las tareas.

Configuraciones especificadas durante la creación de tareas

Puede especificar los siguientes ajustes al crear una tarea. Algunos de estos ajustes también se pueden modificar en las propiedades de la tarea creada.

- Configuración de reinicio del sistema operativo:
  - **No reiniciar el dispositivo**

    Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

  - **Reiniciar el dispositivo**

    Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

  - **Solicitar al usuario una acción**

En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  Si esta opción está desactivada, la solicitud se muestra solo una vez.

- **Reiniciar después de (min)**

  Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

- Configuración de programación de la tarea:

  - **Inicio programado**

    Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

    - **Cada N horas**

      La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

      De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

- **Cada N días**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

  De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Cada N minutos**

  La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- **Manualmente**

La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

Esta opción está activada de forma predeterminada.

- **Cada mes, en días concretos de las semanas seleccionadas**

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- **Cuando se descargan nuevas actualizaciones en el repositorio**

  La tarea se ejecuta después de descargar las actualizaciones en el repositorio. Por ejemplo, es posible que desee utilizar este programa para la tarea de encontrar vulnerabilidades y actualizaciones necesarias.

- **Al detectar un foco de virus**

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

Esta opción está activada de forma predeterminada.

- Usar el retraso aleatorio automáticamente para el inicio de tareas

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

- Dispositivos a los que se asignará la tarea:

  - Seleccionar dispositivos de red detectados por el Servidor de administración

    La tarea se asigna a dispositivos específicos. Los dispositivos específicos pueden incluir dispositivos en grupos de administración así como dispositivos no asignados.

    Por ejemplo, es posible que desee usar esta opción en una tarea de instalación del Agente de red en dispositivos no asignados.

  - Especificar direcciones de dispositivo manualmente o importar direcciones desde una lista

Puede especificar nombres NetBIOS, nombres DNS, direcciones IP y subredes IP de dispositivos a los cuales debe asignar la tarea.

Es posible que desee utilizar esta opción para ejecutar una tarea para una subred específica. Por ejemplo, es posible que desee instalar una aplicación determinada en dispositivos de contadores o analizar dispositivos en una subred que probablemente esté infectada.

- **Asignar tarea a una selección de dispositivos**

  La tarea se asigna a los dispositivos incluidos en una selección de dispositivos. Puede especificar una de las selecciones existentes.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea en dispositivos con una versión específica del sistema operativo.

- **Asignar tarea a un grupo de administración**

  La tarea se asigna a los dispositivos incluidos en un grupo de administración. Puede especificar uno de los grupos existentes o crear uno nuevo.

  Por ejemplo, es posible que desee utilizar esta opción para ejecutar una tarea de envío de un mensaje a los usuarios si el mensaje es específico para dispositivos incluidos en un grupo de administración específico.

- Configuraciones de la cuenta:

  - **Cuenta preconfigurada**

    La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

    Esta opción está seleccionada de forma predeterminada.

  - **Especificar una cuenta**

    Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

  - **Cuenta**

    Cuenta bajo la que se ejecuta la tarea.

  - **Contraseña**

    La contraseña de la cuenta bajo la cual la tarea se ejecutará.

Configuraciones especificadas después de la creación de tareas

Puede especificar la siguiente configuración solo después de crear una tarea.

- Ajustes de la tarea de grupo:

- **Distribuir a subgrupos**

  Esta opción solo está disponible en la configuración de las tareas de grupo.

  Cuando esta opción está activada, la cobertura de la tarea incluye:

  - El grupo de administración que seleccionó al crear la tarea.
  - Los grupos de administración subordinados al grupo de administración seleccionado en cualquier nivel inferior al de la jerarquía del grupo.

  Cuando esta opción está desactivada, el alcance de la tarea incluye solo el grupo de administración que seleccionó al crear la tarea.

  Esta opción está activada de forma predeterminada.

- **Distribuir a Servidores de administración secundarios y virtuales**

  Cuando esta opción está activada, la tarea que es efectiva en el Servidor de administración principal también se aplica en los Servidores de administración secundarios (incluidos los virtuales). Si ya existe una tarea del mismo tipo en el Servidor de administración secundario, ambas tareas se aplican en el Servidor de administración secundario: el existente y el heredado del Servidor de administración principal.

  Esta opción solo está disponible cuando está activada la opción **Distribuir a subgrupos**.

  Esta opción está desactivada de forma predeterminada.

- Configuración de programación avanzada:

  - **Activar el dispositivo con la función Wake-on-LAN antes de que se inicie la tarea (min)**

    El sistema operativo en el dispositivo se inicia a la hora especificada antes de que se inicie la tarea. El intervalo de tiempo predeterminado es de cinco minutos.

    Active esta opción si desea que la tarea se ejecute en todos los dispositivos cliente desde el ámbito de la tarea, incluidos aquellos dispositivos que están apagados cuando la tarea está a punto de comenzar.

    Si desea que el dispositivo se apague automáticamente una vez completada la tarea, habilite la opción **Apagar los dispositivos después de completar la tarea**. Esta opción se puede encontrar en la misma ventana.

    Esta opción está desactivada de forma predeterminada.

  - **Apagar el dispositivo después de completar la tarea**

    Por ejemplo, es posible que desee activar esta opción para una tarea de actualización de instalación que instale actualizaciones en los dispositivos cliente todos los viernes después del horario comercial y después apagar estos dispositivos para el fin de semana.

    Esta opción está desactivada de forma predeterminada.

  - **Detener la tarea si se ha estado ejecutando durante más de (min)**

Una vez que el periodo de tiempo especificado expira, la tarea se detiene automáticamente, ya esté completa o no.

Active esta opción si desea interrumpir (o detener) las tareas que tardan mucho en ejecutarse.

Esta opción está desactivada de forma predeterminada. El tiempo de ejecución de la tarea predeterminado es de 120 minutos.

- Configuración de la notificación:
  - Bloque **Historial de la tarea de la tienda**
    - Almacenar en la base de datos del Servidor de administración durante (días)

      Los eventos de la aplicación relacionados con la ejecución de la tarea en todos los dispositivos cliente del ámbito de la tarea se almacenan en el Servidor de administración durante el número de días especificado. Cuando transcurre este periodo, la información se elimina del Servidor de administración.

      Esta opción está activada de forma predeterminada.

    - Almacenar en el registro de eventos del SO del dispositivo

      Los eventos de la aplicación relacionados con la ejecución de la tarea se almacenan localmente en el Registro de eventos de Windows de cada dispositivo cliente.

      Esta opción está desactivada de forma predeterminada.

    - Almacenar en el registro de eventos del SO del Servidor de administración

      Los eventos de la aplicación relacionados con la ejecución de la tarea en todos los dispositivos cliente del ámbito de la tarea se almacenan de forma centralizada en el Registro de eventos de Windows del sistema operativo (SO) del Servidor de administración.

      Esta opción está desactivada de forma predeterminada.

    - Guardar todos los eventos

      Si se selecciona esta opción, todos los eventos relacionados con la tarea se guardan en los registros del evento.

    - Guardar eventos sobre el progreso de la tarea

      Si se selecciona esta opción, solo los eventos relacionados con la ejecución de la tarea se guardan en los registros del evento.

    - Guardar solo los resultados de ejecución de la tarea

      Si se selecciona esta opción, solo los eventos relacionados con los resultados de la tarea se guardan en los registros del evento.

  - Notificar al administrador los resultados de la ejecución de tareas

Puede seleccionar los métodos por los cuales los administradores reciben notificaciones sobre los resultados de la ejecución de la tarea: por correo electrónico, por SMS y ejecutando un archivo ejecutable. Para configurar la notificación, haga clic en el enlace **Configuración**.

De forma predeterminada, todos los métodos de notificación están deshabilitados.

- Notificar solo de errores

  Si esta opción está habilitada, solo se notifica a los administradores cuando una ejecución de tarea se completa con un error.

  Si esta opción está desactivada, se notifica a los administradores después de cada finalización de la ejecución de la tarea.

  Esta opción está activada de forma predeterminada.

- Configuración de seguridad
- Configuración de la cobertura de la tarea

  Dependiendo de cómo se determine la cobertura de la tarea, están presentes las siguientes configuraciones:

  - Dispositivos

    Si la cobertura de una tarea está determinada por un grupo de administración, puede ver este grupo. No hay cambios disponibles aquí. Sin embargo, puede configurar **Exclusiones de la cobertura de la tarea**.

    Si la cobertura de una tarea está determinado por una lista de dispositivos, puede modificar esta lista añadiendo y eliminando dispositivos.

  - Selección de dispositivos

    Puede cambiar la selección de dispositivos a la que se aplicará la tarea.

  - Exclusiones de la cobertura de la tarea

    Puede especificar grupos de dispositivos a los que no se aplica la tarea. Los grupos que se excluyen solo pueden ser subgrupos del grupo de administración al que se aplica la tarea.

- **Historial de revisión**

Inicio del Asistente para cambiar contraseñas de tareas

Para una tarea no local, puede especificar una cuenta en la que se debe ejecutar la tarea. Puede especificar la cuenta durante la creación de la tarea o en las propiedades de una tarea existente. Si la cuenta especificada se usa de acuerdo con las instrucciones de seguridad de la organización, estas instrucciones pueden requerir cambiar la contraseña de la cuenta de vez en cuando. Cuando la contraseña de la cuenta caduca y establece una nueva, las tareas no se iniciarán hasta que especifique la nueva contraseña válida en las propiedades de la tarea.

El Asistente para cambiar contraseñas de tareas le permite reemplazar automáticamente la contraseña anterior por la nueva en todas las tareas en las que se especifica la cuenta. Alternativamente, puede cambiar la contraseña manualmente en las propiedades de cada tarea.

Para iniciar el Asistente para cambiar contraseñas de tareas:

1. En la pestaña **DISPOSITIVOS**, seleccione **TAREAS**.
2. Haga clic en **Administrar credenciales de cuentas para tareas de inicio**.

Siga las instrucciones del Asistente.

Paso 1. Especificar credenciales

Especifique credenciales nuevas que sean válidas actualmente en su sistema (por ejemplo, en Active Directory). Cuando cambia al siguiente paso del Asistente, Kaspersky Security Center verifica si el nombre de cuenta especificado coincide con el nombre de cuenta en las propiedades de cada tarea no local. Si los nombres de las cuentas coinciden, la contraseña en las propiedades de la tarea se reemplazará automáticamente por la nueva.

Para especificar la nueva cuenta, seleccione una opción:

- **Utilizar cuenta actual**

  El Asistente utiliza el nombre de la cuenta con la que ha iniciado sesión actualmente en Kaspersky Security Center 14 Web Console. Luego, especifique manualmente la contraseña de la cuenta en el campo **Contraseña actual para utilizar en tareas**.

- **Especificar una cuenta distinta**

  Especifique el nombre de la cuenta con la que se deben iniciar las tareas. Luego especifique la contraseña de la cuenta en el campo **Contraseña actual para utilizar en tareas**.

Si completa el campo **Contraseña anterior (opcional; si desea sustituirla por la actual)**, Kaspersky Security Center reemplaza la contraseña solo para aquellas tareas en las que se encuentran tanto el nombre de la cuenta como la contraseña anterior. El reemplazo se realiza automáticamente. En todos los demás casos, debe elegir una acción para realizar el siguiente paso del Asistente.

Paso 2. Seleccionar una acción para realizar

Si no especificó la contraseña anterior en el primer paso del Asistente o si la contraseña anterior especificada no coincide con las contraseñas en las propiedades de las tareas, debe elegir una acción para las tareas encontradas.

Para elegir una acción para una tarea:

1. Seleccione la casilla junto a la tarea para la que desee elegir una acción.
2. Realice una de las siguientes acciones:

   - Para eliminar la contraseña en las propiedades de la tarea, haga clic en **Eliminar credenciales**.

     La tarea cambia para ejecutarse con la cuenta predeterminada.

- Para reemplazar la contraseña con la nueva, haga clic en **Aplicar el cambio de contraseña incluso si la contraseña anterior no se proporcionó o es incorrecta**.
- Para cancelar el cambio de contraseña, haga clic en **No se seleccionó ninguna acción**.

Las acciones elegidas se aplican después de pasar al siguiente paso del Asistente.

Paso 3. Ver los resultados

En el último paso del Asistente, vea los resultados de cada una de las tareas encontradas. Para completar el Asistente, haga clic en el botón **Finalizar**.

Administración de dispositivos cliente

Esta sección describe cómo administrar dispositivos en los grupos de administración.

Configuración de un dispositivo administrado

Para ver la configuración de un dispositivo administrado, siga estos pasos:

1. Seleccione **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el enlace con el nombre del dispositivo requerido.

Se muestra la ventana de propiedades del dispositivo seleccionado.

General

La sección **Control de aplicaciones** muestra información general sobre el dispositivo cliente. La información proporcionada se basa en los datos recibidos durante la última sincronización del dispositivo cliente con el Servidor de administración:

- **Nombre**

  En este campo se puede ver y modificar el nombre del dispositivo cliente en el grupo de administración.

- **Descripción**

  En este campo se puede introducir una descripción adicional para un dispositivo cliente.

- **Grupo**

  Grupo de administración que incluye el dispositivo cliente.

- **Última actualización**

  Fecha en que las bases de datos o las aplicaciones se actualizaron por última vez en el dispositivo.

- **Visible por última vez**

  Fecha y hora en que el dispositivo estuvo visible por última vez en la red.

- **Conectado al Servidor de administración**

  Fecha y hora en que el Agente de red instalado en el dispositivo cliente se conectó por última vez al Servidor de administración.

- **No desconectar del Servidor de administración**

  Si esta opción está activada, se mantiene la conectividad continua entre el dispositivo administrado y el Servidor de administración. Es posible que desee usar esta opción si no está utilizando servidores push, que proporcionan dicha conectividad.

  Si esta opción está desactivada y los servidores push no están en uso, el dispositivo administrado solo se conecta al Servidor de administración para sincronizar datos o transmitir información.

  El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

  Esta opción está desactivada de manera predeterminada en los dispositivos administrados. Esta opción está activada de manera predeterminada en el dispositivo donde está instalado el Servidor de administración y permanece así incluso si intenta desactivarla.

Red

La sección **Red** proporciona la siguiente información sobre las propiedades de la red del dispositivo cliente:

- **Dirección IP**

  Dirección IP del dispositivo.

- **Dominio de Windows**

  El dominio o grupo de trabajo de Windows que contiene el dispositivo.

- **Nombre DNS**

  Nombre del dominio DNS del dispositivo cliente.

- **Nombre NetBIOS**

  Nombre de red Windows del dispositivo cliente.

Sistema

La sección **Sistema** proporciona información sobre el sistema operativo instalado en el dispositivo cliente.

Protección

La sección **Protección** ofrece información sobre el estado actual de la protección antivirus en un dispositivo cliente:

- **Estado del dispositivo**

  Estado del dispositivo cliente, asignado según los criterios definidos por el administrador para el estado de la protección antivirus en el dispositivo y la actividad del dispositivo en la red.

- **Todos los problemas**

  Esta tabla contiene una lista completa de problemas detectados por las aplicaciones administradas instaladas en el dispositivo cliente. Cada problema va acompañado de un estado, que la aplicación sugiere que asigne al dispositivo para este problema.

- **Protección en tiempo real**

  Este campo muestra el estado actual de la protección en tiempo real en el dispositivo cliente.

  Cuando el estado cambia en el dispositivo, el nuevo estado se muestra en la ventana de propiedades del dispositivo solo después de que el dispositivo cliente se sincronice con el Servidor de administración.

- **Último análisis a petición**

  Fecha y hora del último análisis antivirus realizado en el dispositivo cliente.

- **Número total de amenazas detectadas**

  Número total de amenazas detectadas en el dispositivo cliente desde la instalación de la aplicación antivirus (primer análisis del dispositivo) o desde la última fecha en que el contador de amenazas se puso a cero.

- **Amenazas activas**

  Número de archivos no procesados en el dispositivo cliente.

  Este campo omite el número de archivos no procesados en dispositivos móviles.

- **Estado del cifrado del disco**

  Estado actual del cifrado de archivo en las unidades locales del dispositivo.

Estado del dispositivo definido por la aplicación

La sección **Estado del dispositivo definido por la aplicación** proporciona información sobre el estado del dispositivo definido por la aplicación administrada que está instalada en el dispositivo. El estado del dispositivo puede ser diferente al definido por Kaspersky Security Center Cloud Console.

Aplicaciones

La sección **Aplicaciones** enumera todas las aplicaciones Kaspersky instaladas en el dispositivo cliente. Puede hacer clic en el nombre de la aplicación para consultar la información general sobre la aplicación, una lista de eventos que se han producido en el dispositivo y la configuración de la aplicación.

Directivas activas y perfiles de directivas

La sección **Perfiles de directiva y directivas activas** enumera las directivas y los perfiles de directivas que se encuentran activos en el dispositivo administrado.

Tareas

En la sección **Tareas**, puede administrar tareas del dispositivo cliente: ver la lista de tareas existentes, crear nuevas, eliminar, iniciar y detener tareas, modificar su configuración y ver resultados de ejecución. La lista de tareas se proporciona a partir de los datos recibidos durante la última sesión de sincronización del cliente con el Servidor de administración. El Servidor de administración solicita los detalles de estado de la tarea desde el dispositivo cliente. No se mostrará el estado si no se ha establecido conexión.

Eventos

La sección **Eventos** muestra eventos registrados en el Servidor de administración para el dispositivo cliente seleccionado.

Incidentes

En la sección **Incidentes**, puede ver, editar y crear incidentes para el dispositivo cliente. Los incidentes se pueden crear automáticamente, mediante las aplicaciones administradas por Kaspersky que están instaladas en el dispositivo cliente, o el administrador las puede crear de forma manual. Por ejemplo, si algunos usuarios mueven regularmente el malware de sus unidades extraíbles a los dispositivos, el administrador puede crear un incidente. El administrador puede proporcionar una breve descripción del caso y las acciones recomendadas (como las medidas disciplinarias que se deben tomar contra un usuario) en el texto del incidente y puede añadir un enlace al usuario o usuarios.

Un incidente para el cual se han tomado todas las acciones necesarias se llama *procesado*. La presencia de incidentes sin procesar se puede elegir como condición para cambiar el estado del dispositivo a *Crítico* o *Advertencia*.

Esta sección contiene una lista de incidentes que se han creado para el dispositivo. Los incidentes se clasifican por nivel de gravedad y tipo. El tipo de un incidente lo define la aplicación de Kaspersky que crea el incidente. Puede resaltar incidentes procesados en la lista seleccionando la casilla de verificación en la columna **Procesado**.

Etiquetas

En la sección **Etiquetas** puede administrar la lista de palabras clave que se utilizan para buscar dispositivos cliente: ver la lista de etiquetas existentes, asignar etiquetas de la lista, configurar reglas de etiquetado automático, añadir etiquetas nuevas y cambiar el nombre de las antiguas y eliminar etiquetas.

Registro de aplicaciones

En la sección **Registro de aplicaciones** se puede ver el registro de aplicaciones instaladas en el dispositivo cliente y sus actualizaciones, y se puede configurar la visualización del registro de aplicaciones.

La información acerca de las aplicaciones instaladas se proporciona si el Agente de red instalado en el dispositivo cliente envía la información requerida al Servidor de administración. Puede configurar el envío de información al Servidor de administración en la ventana de propiedades del Agente de red o de su directiva, en la sección **Repositorios**. La información sobre las aplicaciones instaladas se proporciona solo para dispositivos que ejecutan Windows.

El Agente de red proporciona información sobre las aplicaciones en función de los datos recibidos desde el registro del sistema.

Al hacer clic en el nombre de una aplicación, se abre una ventana que contiene los detalles de la aplicación y una lista de los paquetes de actualización instalados para la aplicación.

Archivos ejecutables

La sección **Archivos ejecutables** muestra los archivos ejecutables encontrados en el dispositivo cliente.

Puntos de distribución

Esta sección proporciona una lista de puntos de distribución con los cuales interactúa el dispositivo.

- Exportar a archivo

  Haga clic en el botón **Exportar a archivo** para guardar a un archivo una lista de puntos de distribución con los cuales interacciona el dispositivo. De forma predeterminada, la aplicación exporta la lista de dispositivos a un archivo CSV.

- Propiedades

  Haga clic en el botón **Propiedades** para ver y configurar el punto de distribución con el cual interactúa el dispositivo.

Registro de hardware

En la sección **Registro de hardware**, puede ver información sobre el hardware instalado en el dispositivo cliente. Puede ver esta información para dispositivos de Windows y dispositivos Linux.

Actualizaciones disponibles

Esta sección muestra una lista de actualizaciones de software encontradas en este dispositivo, pero no instaladas aún.

Mostrar las actualizaciones instaladas

Si se selecciona esta opción, la lista de actualizaciones muestra tanto las actualizaciones que no se han instalado, como las que ya se han instalado en el dispositivo cliente.

Esta opción está desactivada de forma predeterminada.

Vulnerabilidades de software

La sección **Vulnerabilidades de software** proporciona información sobre las vulnerabilidades de las aplicaciones de terceros instaladas en dispositivos cliente.

Para guardar las vulnerabilidades en un archivo, seleccione las casillas de verificación junto a las vulnerabilidades que desea guardar y luego haga clic en el botón **Exportar filas a un archivo CSV** o **Exportar filas a un archivo TXT**.

La sección **Vulnerabilidades de software** contiene los siguientes ajustes:

- **Mostrar solo las vulnerabilidades que se pueden reparar**

  Si se selecciona esta opción, la sección muestra las vulnerabilidades que se pueden reparar mediante un parche.

  Si esta opción está desactivada, la sección muestra tanto las vulnerabilidades que se pueden reparar mediante un parche como aquellas para las que no existe ningún parche.

  Esta opción está activada de forma predeterminada.

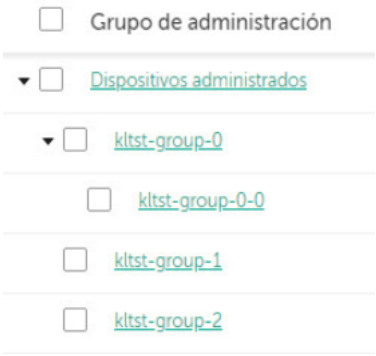
- **Propiedades de la vulnerabilidad**

  Haga clic en el nombre de una vulnerabilidad de software en la lista para ver las propiedades de la vulnerabilidad de software seleccionada en una ventana separada. En la ventana, puede hacer lo siguiente:

  - Omita la vulnerabilidad de software en este dispositivo administrado (en la Consola de administración o en Kaspersky Security Center 14 Web Console).
  - Ver la lista de soluciones recomendadas para la vulnerabilidad.
  - Especifique manualmente las actualizaciones de software para corregir la vulnerabilidad (en la Consola de administración o en Kaspersky Security Center 14 Web Console).
  - Ver instancias de vulnerabilidad.
  - Ver la lista de tareas existentes para corregir la vulnerabilidad y crear nuevas tareas para corregir la vulnerabilidad.

Creación de grupos de administración

Inmediatamente después de la instalación de Kaspersky Security Center, la jerarquía de grupos de administración contiene solo un grupo de administración, llamado **Dispositivos administrados**. Al crear una jerarquía de grupos de administración, puede añadir dispositivos, entre ellos máquinas virtuales, al grupo **Dispositivos administrados** y añadir grupos anidados (ver la figura de abajo).



Visualización de la jerarquía de los grupos de administración

Para crear un grupo de administración:

1. En el menú principal, vaya a **DISPOSITIVOS** → **JERARQUÍA DE GRUPOS**.
2. En la estructura del grupo de administración, seleccione el grupo de administración que quiere incluir en el nuevo grupo de administración.
3. Haga clic en el botón **Añadir**.
4. En la ventana **Nombre del nuevo grupo de administración** que se abre, introduzca un nombre para el grupo y haga clic en el botón **Añadir**.

   Aparece un nuevo grupo de administración con el nombre especificado en la jerarquía de los grupos de administración.

La aplicación permite crear una jerarquía de grupos de administración basada en la estructura de Active Directory o la estructura de la red de dominios. También es posible crear una estructura de grupos a partir de un archivo de texto.

Para crear una estructura de grupos de administración:

1. En el menú principal, vaya a **DISPOSITIVOS** → **JERARQUÍA DE GRUPOS**.
2. Haga clic en el botón **Importar**.

   Asistente de nueva estructura de grupos de administración. Siga las instrucciones del Asistente.

Adición de dispositivos al grupo de administración manualmente

Puede mover automáticamente dispositivos a grupos de administración creando reglas de movimiento de dispositivos o manualmente, moviendo dispositivos de un grupo de administración a otro o añadiendo dispositivos al grupo de administración seleccionado. Esta sección describe cómo añadir manualmente dispositivos a un grupo de administración.

Para añadir uno o más dispositivos a un grupo de administración seleccionado:

1. En el menú principal, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el enlace **Ruta actual:** `<ruta actual>` encima de la lista.
3. En la ventana que se abre, seleccione el grupo de administración al que desea añadir los dispositivos.

4. Haga clic en el botón **Añadir dispositivos**.

   Se inicia el Asistente para mover dispositivos.

5. Haga una lista de los dispositivos que desea añadir al grupo de administración.

   > Solo se pueden añadir dispositivos cuya información se haya añadido a la base de datos del Servidor de administración o bien al conectarse el dispositivo o bien después de la detección de dispositivos.

   Seleccione cómo desea añadir dispositivos a la lista:

   - Haga clic en el botón **Añadir dispositivos** y luego especifique los dispositivos de una de las siguientes maneras:
     - Seleccione los dispositivos de la lista de dispositivos detectados por el Servidor de administración.
     - Especifique la dirección IP del dispositivo o un rango de IP.
     - Especifique el nombre NetBIOS o el nombre DNS del dispositivo.

       > El campo del nombre del dispositivo no debe contener caracteres de espacio, ni los siguientes caracteres prohibidos: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

   - Haga clic en el botón **Importar dispositivos desde un archivo** para importar una lista de dispositivos desde un archivo .txt. Cada dirección o nombre del dispositivo debe especificarse en una línea separada.

     > El archivo no debe contener caracteres de espacio, ni los siguientes caracteres prohibidos: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. Ver la lista de dispositivos que se añadirán al grupo de administración. Puede editar la lista añadiendo o quitando dispositivos.

7. Habiéndose asegurado de que la lista es correcta, haga clic en el botón **Siguiente**.

   El Asistente procesa la lista de dispositivos y muestra el resultado. Los dispositivos correctamente procesados se incluyen en el grupo de administración y se muestran en la lista de dispositivos con nombres generados por el Servidor de administración.

Traslado manual de dispositivos al grupo de administración

Puede mover dispositivos de un grupo de administración a otro, o del grupo de dispositivos no asignados a un grupo de administración.

Para mover uno o varios dispositivos a un grupo de administración seleccionado:

1. Abra el grupo de administración donde se encuentran los dispositivos que desea mover. Puede hacerlo de una de las siguientes maneras:

   - Para abrir un grupo de administración, vaya a **DISPOSITIVOS** → **Grupos** → **<nombre del grupo>** → **DISPOSITIVOS ADMINISTRADOS**.

- Para abrir el grupo **DISPOSITIVOS NO ASIGNADOS**, vaya a **DETECCIÓN Y DESPLIEGUE** → **DISPOSITIVOS NO ASIGNADOS**.

2. Seleccione las casillas de verificación junto a los dispositivos que desea mover a un grupo diferente.
3. Haga clic en el botón **Mover a un grupo**.
4. En la jerarquía de grupos de administración, seleccione la casilla de verificación junto al grupo de administración al que desea mover los dispositivos seleccionados.
5. Haga clic en el botón **Mover**.

Los dispositivos seleccionados se mueven al grupo de administración seleccionado.

Crear reglas de movimiento de dispositivos

Puede configurar reglas de movimiento de dispositivos; es decir, reglas que asignan automáticamente dispositivos a grupos de administración.

Para crear una regla móvil:

1. En el menú principal, vaya a la pestaña **DISPOSITIVOS** → **REGLAS DE MOVIMIENTO**.
2. Haga clic en **Añadir**.
3. En la ventana que se abre, especifique la siguiente información en la pestaña **Control de aplicaciones**:

- Nombre de la regla

  Introduzca un nombre para la nueva regla.

  Si está copiando una regla, la nueva regla recibe el mismo nombre que la regla de origen, pero se añade un índice en formato () al nombre, por ejemplo: (1).

- Grupo de administración

  Seleccione el grupo de administración al que se moverán automáticamente los dispositivos.

- Aplicar regla

  Puede seleccionar una de las siguientes opciones:

  - Ejecutar una vez en cada dispositivo.

    La regla se aplica una vez para cada dispositivo que coincida con sus criterios.

  - Ejecutar una vez en cada dispositivo y luego cada vez que vuelva a instalar el Agente de red.

    La regla se aplica una vez para cada dispositivo que coincida con sus criterios, luego solo cuando el Agente de red se reinstala en estos dispositivos.

  - Regla aplicada continuamente.

    La regla se aplica de acuerdo con el programa que el Servidor de administración configura automáticamente (generalmente cada varias horas).

- Mover solo dispositivos que no pertenezcan a ningún grupo de administración

  Si esta opción está activada, solo los dispositivos no asignados se moverán al grupo seleccionado.

  Si esta opción está desactivada, los dispositivos que ya pertenecen a otros grupos de administración, así como a los dispositivos no asignados, se moverán al grupo seleccionado.

- Activar regla

  Si esta opción está activada, la regla se activa y empieza a funcionar después de que se guarde.

  Si esta opción está desactivada, la regla se crea pero no se activa. No funcionará hasta que habilites esta opción.

4. Si lo desea, en la pestaña **Condiciones de reglas**, especifique los criterios para los dispositivos que desea mover automáticamente.

5. Haga clic en **Guardar**.

Se crea la regla móvil. Se muestra en la lista de reglas móviles. Mientras más alta sea la posición en la lista, más alta es la prioridad de la regla: si los atributos del dispositivo cumplen las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, el que tiene el rango más alto en la lista de reglas).

Copiar reglas de movimiento de dispositivos

Puede copiar reglas en movimiento, por ejemplo, si desea tener varias reglas idénticas para diferentes grupos de administración de destino.

Para copiar una regla móvil existente:

1. En el menú principal, vaya a la pestaña **DISPOSITIVOS → REGLAS DE MOVIMIENTO**.

   También puede seleccionar **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN** y, en el menú, seleccionar **REGLAS DE MOVIMIENTO**.

   Se muestra la lista de reglas de movimiento.

2. Seleccione las casillas de verificación al lado de la regla que quiere copiar.

3. Haga clic en **Copiar**.

4. En la ventana que se abre, cambie la siguiente información en la pestaña **Control de aplicaciones** o no realice cambios si solo desea copiar la regla sin cambiar su configuración:

   - Nombre de la regla

     Introduzca un nombre para la nueva regla.

     Si está copiando una regla, la nueva regla recibe el mismo nombre que la regla de origen, pero se añade un índice en formato () al nombre, por ejemplo: (1).

   - Grupo de administración

Seleccione el grupo de administración al que se moverán automáticamente los dispositivos.

- Aplicar regla

  Puede seleccionar una de las siguientes opciones:

  - Ejecutar una vez en cada dispositivo.

    La regla se aplica una vez para cada dispositivo que coincida con sus criterios.

  - Ejecutar una vez en cada dispositivo y luego cada vez que vuelva a instalar el Agente de red.

    La regla se aplica una vez para cada dispositivo que coincida con sus criterios, luego solo cuando el Agente de red se reinstala en estos dispositivos.

  - Regla aplicada continuamente.

    La regla se aplica de acuerdo con el programa que el Servidor de administración configura automáticamente (generalmente cada varias horas).

- Mover solo dispositivos que no pertenezcan a ningún grupo de administración

  Si esta opción está activada, solo los dispositivos no asignados se moverán al grupo seleccionado.

  Si esta opción está desactivada, los dispositivos que ya pertenecen a otros grupos de administración, así como a los dispositivos no asignados, se moverán al grupo seleccionado.

- Activar regla

  Si esta opción está activada, la regla se activa y empieza a funcionar después de que se guarde.

  Si esta opción está desactivada, la regla se crea pero no se activa. No funcionará hasta que habilites esta opción.

5. Si lo desea, en la pestaña **Condiciones de reglas**, especifique los criterios para los dispositivos que desea mover automáticamente.

6. Haga clic en **Guardar**.

Se crea la nueva regla de movimiento. Se muestra en la lista de reglas móviles.

Ver y configurar las acciones cuando los dispositivos muestran inactividad

Si los dispositivos cliente dentro de un grupo están inactivos, puede recibir notificaciones al respecto. También puede eliminar automáticamente dichos dispositivos.

Para ver o configurar las acciones cuando los dispositivos del grupo muestran inactividad:

1. En el menú principal, vaya a **DISPOSITIVOS** → **JERARQUÍA DE GRUPOS**.

2. Haga clic en el nombre del grupo de administración requerido.

   Se abrirá la ventana de propiedades del grupo de administración.

3. En la ventana de propiedades, vaya a la pestaña **Configuración**.

4. En la sección **Herencia**, active o desactive las siguientes opciones:

   - **Heredar del grupo primario**

     La configuración en esta sección se heredará del grupo primario en el que se incluye el dispositivo cliente. Si esta opción está activada, la configuración de **Actividad de los dispositivos en la red** se bloquea de cualquier cambio.

     Esta opción está disponible solo si el grupo de administración tiene un grupo primario.

     Esta opción está activada de forma predeterminada.

   - **Forzar la herencia de la configuración en los grupos secundarios**

     Los valores de configuración se distribuirán a grupos secundarios, pero en las propiedades de los grupos secundarios estas configuraciones están bloqueadas.

     Esta opción está desactivada de forma predeterminada.

5. En la sección **Actividad de los dispositivos**, active o desactive las siguientes opciones:

   - **Notificar al administrador si el dispositivo ha estado inactivo durante más de (días)**

     Si esta opción está activada, el administrador recibe notificaciones sobre dispositivos inactivos. Puede especificar el intervalo de tiempo después del cual se crea el **dispositivo inactivo en la red en un evento de larga duración**. De forma predeterminada, el intervalo de tiempo es 7 día.

     Esta opción está activada de forma predeterminada.

   - **Quitar el dispositivo del grupo si ha estado inactivo durante más de (días)**

     Si esta opción está activada, puede especificar el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo. De forma predeterminada, el intervalo de tiempo es 60 día.

     Esta opción está activada de forma predeterminada.

6. Haga clic en **Guardar**.

Sus cambios están guardados y aplicados.

Acerca de los estados de los dispositivos

Kaspersky Security Center asigna un estado a cada dispositivo administrado. El estado particular depende de si se cumplen las condiciones definidas por el usuario. En algunos casos, al asignar un estado a un dispositivo, Kaspersky Security Center tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Si Kaspersky Security Center no encuentra un dispositivo en la red en un plazo de dos horas, el indicador de visibilidad del dispositivo se establece en *No visible*.

Los estados son los siguientes:

- *Crítico* o *Crítico/Visible*

- *Advertencia* o *Advertencia/Visible*
- *Correcto* o *Correcto/Visible*

La tabla a continuación enumera las condiciones predeterminadas que se deben cumplir para asignar el estado *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para asignar un estado a un dispositivo

Condición	Descripción de la condición	Valores disponibles
La aplicación de seguridad no está instalada	El Agente de red está instalado en el dispositivo, pero una aplicación de seguridad no está instalada.	• El botón está activado. • El botón está desactivado.
Demasiados virus detectados	Una tarea de detección de virus (por ejemplo, la tarea *Análisis antivirus*) ha detectado algunos virus en el dispositivo y el número de virus encontrados supera el valor especificado.	Más de 0.
El nivel de protección en tiempo real es distinto del establecido por el administrador	El dispositivo es visible en la red, pero el nivel de la protección en tiempo real se diferencia del nivel configurado (en la condición) por el administrador para el estado del dispositivo.	• Detenido. • En pausa. • En ejecución.
No se ha realizado ningún análisis antivirus desde hace mucho tiempo	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero la tarea *Análisis antivirus* no se ha ejecutado durante el intervalo de tiempo especificado. La condición se aplica solo a los dispositivos que se agregaron a la base de datos del Servidor de administración hace siete días o antes.	Más de 1 día.
Las bases de datos están desactualizadas	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero las bases de datos antivirus no se han actualizado en este dispositivo durante el intervalo de tiempo especificado. La condición se aplica solo a los dispositivos que se agregaron a la base de datos del Servidor de administración hace un día o antes.	Más de 1 día.
No conectado durante mucho tiempo	El Agente de red está instalado en el dispositivo, pero el dispositivo no se ha conectado a un Servidor de administración durante el intervalo de tiempo especificado porque el dispositivo se desactivó.	Más de 1 día.
Se han detectado amenazas activas	El número de objetos no procesados en la carpeta **AMENAZAS ACTIVAS** supera el valor especificado.	Más de 0 elementos.
Se requiere reiniciar	El dispositivo es visible en la red, pero una aplicación requiere que el dispositivo se reinicie por más tiempo que el intervalo de tiempo especificado y por una de las razones seleccionadas.	Más de 0 minutos.
Hay aplicaciones incompatibles instaladas	El dispositivo es visible en la red, pero el inventario del software realizado a través del Agente de red ha detectado aplicaciones incompatibles instaladas en el dispositivo.	• El botón está desactivado. • El botón está activado.

Se han detectado vulnerabilidades de software	El dispositivo es visible en la red y el Agente de red está instalado en el dispositivo, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha detectado vulnerabilidades con el nivel de gravedad especificado en aplicaciones instaladas en el dispositivo.	• Crítico. • Alta. • Media. • Ignorar si no se puede reparar la vulnerabilidad. • Ignorar si se asigna una actualización para su instalación.
La licencia comercial ha caducado	El dispositivo es visible en la red, pero la licencia ha caducado.	• El botón está desactivado. • El botón está activado.
la licencia caduca pronto	El dispositivo es visible en la red, pero la licencia caduca en el dispositivo en menos días que el número especificado de días.	Más de 0 días.
Hace mucho tiempo que no se comprueba si hay actualizaciones de Windows Update	El dispositivo es visible en la red, pero la tarea *Sincronizar Windows Update* no se ha ejecutado durante el intervalo de tiempo especificado.	Más de 1 día.
Estado de cifrado no válido	El Agente de red está instalado en el dispositivo, pero el resultado del cifrado del dispositivo es igual al valor especificado.	• No cumple con la directiva debido a la respuesta del usuario (para dispositivos externos solamente). • No cumple con la directiva debido a un error. • Se requiere reiniciar al aplicar la directiva.

		• No se indica ninguna directiva de cifrado. • No admitido. • Al aplicar la directiva.
La configuración del dispositivo móvil no cumple la directiva	La configuración del dispositivo móvil es diferente de la configuración que se especificó en la directiva de Kaspersky Endpoint Security for Android para dispositivos móviles durante la comprobación de las reglas de cumplimiento.	• El botón está desactivado. • El botón está activado.
Incidentes sin procesar detectados	Se han detectado algunos incidentes no procesados en el dispositivo. Los incidentes se pueden crear automáticamente, mediante las aplicaciones administradas por Kaspersky que están instaladas en el dispositivo cliente, o el administrador las puede crear de forma manual.	• El botón está desactivado. • El botón está activado.
Estado del dispositivo definido por la aplicación	El estado del dispositivo se define por la aplicación administrada.	• El botón está desactivado. • El botón está activado.
El dispositivo no tiene espacio disponible en el disco	El espacio libre en disco en el dispositivo es menor que el valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. El estado *Crítico* o *Advertencia* pasa al estado *Correcto* cuando el dispositivo se sincroniza correctamente con el Servidor de administración y el espacio libre en el dispositivo es mayor o igual al valor especificado.	Más de 0 MB.
Se ha perdido la conexión con el dispositivo	Durante la detección de dispositivos, el dispositivo se reconoció como visible en la red, pero más de tres intentos de sincronizar con el Servidor de administración fallaron.	• El botón está desactivado. • El botón está activado.
La protección está desactivada	El dispositivo es visible en la red, pero la aplicación de seguridad en el dispositivo se ha desactivado durante más tiempo que el intervalo de tiempo especificado.	Más de 0 minutos.
La aplicación de seguridad no se está ejecutando	El dispositivo es visible en la red y hay una aplicación de seguridad instalada en el dispositivo pero no se está ejecutando.	• El botón está desactivado. • El botón está activado.

Kaspersky Security Center le permite configurar el cambio automático del estado de un dispositivo en un grupo de administración cuando las condiciones especificadas se cumplen. Cuando las condiciones especificadas se cumplen, se asigna al dispositivo cliente uno de los estados siguientes: *Crítico* o *Advertencia*. Cuando no se cumplen las condiciones especificadas, al dispositivo cliente se le asigna el estado *Correcto*.

Distintos estados pueden corresponder a distintos valores de una condición. Por ejemplo, de manera predeterminada, si la condición **Las bases de datos están desactualizadas** tiene el valor **Más de 3 días**, se asigna el estado *Advertencia* al dispositivo cliente; si el valor fuera **Más de 7 días**, se le asignaría el estado *Crítico*.

Si actualiza Kaspersky Security Center desde la versión anterior, los valores de la condición **Las bases de datos están desactualizadas** para asignar el estado a *Crítico* o *Advertencia* no cambian.

Cuando Kaspersky Security Center asigna un estado a un dispositivo, para algunas condiciones (consulte la columna Descripción de la condición) se tiene en cuenta el indicador de visibilidad. Por ejemplo, si a un dispositivo administrado se le ha asignado el estado *Crítico* porque se cumplió la condición Las bases de datos están desactualizadas, y luego se configuró el indicador de visibilidad para el dispositivo, entonces al dispositivo se le asigna el estado *Correcto*.

Configuración del cambio de estado de los dispositivos

Puede cambiar las condiciones para asignar el estado *Crítico* o *Advertencia* a un dispositivo.

Para activar el cambio del estado del dispositivo a Crítico:

1. Abra la ventana de propiedades de alguno de los siguientes modos:
   - En la carpeta **Directivas** en el menú contextual de una directiva del Servidor de administración, seleccione **Propiedades**.
   - Seleccione **Propiedades** en el menú contextual de un grupo de administración.
2. En la ventana de propiedades que se abre, en el panel **Secciones**, seleccione **Estado del dispositivo**.
3. En el panel derecho, en la sección **Asignar Crítico si se especifican**, marque la casilla junto a una de las condiciones de la lista.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.
4. Configure el valor requerido para la condición seleccionada.

   Puede establecer valores para algunas condiciones pero no para todas.
5. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Crítico*.

Para activar el cambio del estado del dispositivo a Advertencia:

1. Abra la ventana de propiedades de alguno de los siguientes modos:

- En la carpeta **Directivas** en el menú contextual de la directiva del Servidor de administración, seleccione **Propiedades**.
- Seleccione **Propiedades** en el menú contextual del grupo de administración.

2. En la ventana de propiedades que se abre, en el panel **Secciones**, seleccione **Estado del dispositivo**.
3. En el panel derecho, en la sección **Asignar Advertencia si se especifican**, marque la casilla junto a una de las condiciones de la lista.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

4. Configure el valor requerido para la condición seleccionada.

   Puede establecer valores para algunas condiciones pero no para todas.

5. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Advertencia*.

Conexión remota con el escritorio de un dispositivo cliente

El administrador puede obtener acceso remoto al escritorio de un dispositivo cliente mediante el Agente de red instalado en el dispositivo. También se puede realizar la conexión remota a un dispositivo con Agente de red, incluso si los puertos TCP y UDP del dispositivo cliente están cerrados.

Cuando se establece una conexión con el dispositivo, el administrador obtiene acceso total a la información almacenada en dicho dispositivo, de modo que podrá administrar las aplicaciones que haya instaladas en él.

Se debe permitir la conexión remota en la configuración del sistema operativo del dispositivo administrado de destino. Por ejemplo, en Windows 10, esta opción se llama **Permitir conexiones de Asistencia remota a este equipo** (puede encontrar esta opción en **Panel de control → Sistema y seguridad → Sistema → Configuración de Acceso remoto**). Si tiene una licencia para la función Administración de vulnerabilidades y parches, puede habilitar esta opción de forma forzada cuando establece una conexión con un dispositivo administrado. Si no tiene la licencia, habilite esta opción localmente en el dispositivo administrado de destino. Si esta opción está desactivada, la conexión remota no es posible.

Para establecer una conexión remota a un dispositivo, debe tener dos utilidades:

- La utilidad de Kaspersky llamada klsctunnel. Esta utilidad debe almacenarse en la estación de trabajo del administrador. Se usa esta utilidad para tunelizar la conexión entre un dispositivo cliente y el Servidor de administración.

  Kaspersky Security Center permite los túneles de conexiones de TCP desde la Consola de administración mediante el Servidor de administración y, luego, mediante el Agente de red a un puerto especificado en un dispositivo administrado. El túnel está diseñado para conectar una aplicación cliente en un dispositivo con la Consola de administración instalada en un puerto TCP en un dispositivo administrado si una conexión directa entre la Consola de administración y el dispositivo de destino no es posible.

  Se requerirá una conexión por túnel entre un dispositivo cliente remoto y el Servidor de administración si el puerto usado para la conexión con el Servidor de administración no está disponible en el dispositivo. Es posible que el puerto del dispositivo no esté disponible en los siguientes casos:

- El dispositivo remoto está conectado a una red local que utiliza un mecanismo NAT.
- El dispositivo remoto forma parte de la red local del Servidor de administración pero su puerto está cerrado en el firewall.

- Componente estándar de Microsoft Windows denominado Conexión a Escritorio remoto. La conexión a un escritorio remoto se establece con la utilidad estándar mstsc.exe de Windows de acuerdo con la configuración de esta utilidad.

  La conexión a la sesión del escritorio remoto actual del usuario se establece sin que el usuario lo sepa. Cuando el administrador se conecta a la sesión, el usuario del dispositivo se desconecta de la sesión sin previo aviso.

Para conectarse al escritorio de un dispositivo cliente:

1. En la Consola de administración basada en MMC, en el menú contextual de la directiva del Servidor de administración, seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración que se abre, vaya a **Configuración de la conexión del Servidor de administración → Puertos de conexión**.
3. Asegúrese de que la opción **Abrir puerto RDP para Kaspersky Security Center 14 Web Console** este habilitada.
4. En Kaspersky Security Center 14 Web Console, vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS → Grupos**, y, a continuación, seleccione el grupo de administración que contiene el dispositivo al que desea obtener acceso.
5. Seleccione la casilla de verificación junto al nombre del dispositivo al que desea acceder.
6. Haga clic en el botón **Conectar con el escritorio remoto**.

   Se abre la ventana Escritorio remoto (solo Windows).
7. Habilite la opción **Permitir conexión de escritorio remota en dispositivo administrado**. En este caso, la conexión se establecerá incluso si las conexiones remotas están actualmente prohibidas en la configuración del sistema operativo del dispositivo administrado.

   Esta opción solo está disponible si tiene una licencia para la función Administración de vulnerabilidades y parches.
8. Haga clic en el botón **Descargar** para descargar la utilidad klsctunnel.
9. Haga clic en el botón **Copiar al portapapeles** para copiar el texto desde el campo de texto. Este texto es un Binary Large OBject (BLOB) que contiene la configuración requerida para establecer la conexión entre el Servidor de administración y el dispositivo administrado.

   Un BLOB es válido por 3 minutos. Si ha caducado, vuelva a abrir la ventana Escritorio remoto (solo Windows) para generar un nuevo BLOB.
10. Ejecute la utilidad klsctunnel.

    Se abre la ventana de la utilidad.
11. Pegue el texto copiado en el campo de texto.

12. Si usa un servidor proxy, seleccione la casilla de verificación **Usar servidor proxy** y luego especifique la configuración de conexión del servidor proxy.

13. Haga clic en el botón **Abrir puerto**.

    Se abre la ventana de inicio de sesión Conexión a Escritorio remoto.

14. Especifique las credenciales de la cuenta con la que ha iniciado sesión actualmente en Kaspersky Security Center 14 Web Console.

15. Haga clic en el botón **Conectar**.

    Cuando se establece la conexión al dispositivo, el escritorio está disponible en la ventana Conexión a escritorio remoto de Microsoft Windows.

Conexión con los dispositivos mediante Uso compartido del escritorio de Windows

El administrador puede obtener acceso remoto al escritorio de un dispositivo cliente mediante el Agente de red instalado en el dispositivo. También se puede realizar la conexión remota a un dispositivo con Agente de red, incluso si los puertos TCP y UDP del dispositivo cliente están cerrados.

El administrador se puede conectar a una sesión existente en un dispositivo cliente sin desconectar al usuario que la está utilizando. En ese caso, tanto el administrador como el usuario de la sesión del dispositivo comparten el acceso al escritorio.

Para establecer una conexión remota a un dispositivo, debe tener dos utilidades:

- La utilidad de Kaspersky llamada klsctunnel. Esta utilidad debe almacenarse en la estación de trabajo del administrador. Se usa esta utilidad para tunelizar la conexión entre un dispositivo cliente y el Servidor de administración.

  Kaspersky Security Center permite los túneles de conexiones de TCP desde la Consola de administración mediante el Servidor de administración y, luego, mediante el Agente de red a un puerto especificado en un dispositivo administrado. El túnel está diseñado para conectar una aplicación cliente en un dispositivo con la Consola de administración instalada en un puerto TCP en un dispositivo administrado si una conexión directa entre la Consola de administración y el dispositivo de destino no es posible.

  Se requerirá una conexión por túnel entre un dispositivo cliente remoto y el Servidor de administración si el puerto usado para la conexión con el Servidor de administración no está disponible en el dispositivo. Es posible que el puerto del dispositivo no esté disponible en los siguientes casos:

  - El dispositivo remoto está conectado a una red local que utiliza un mecanismo NAT.
  - El dispositivo remoto forma parte de la red local del Servidor de administración pero su puerto está cerrado en el firewall.

- Uso compartido del escritorio de Windows. Al conectarse a una sesión existente del escritorio remoto, el usuario de la sesión del dispositivo recibe una solicitud del administrador para establecer la conexión. No se guardará ninguna información sobre la actividad en remoto del dispositivo ni de sus resultados en los informes creados por Kaspersky Security Center.

  El administrador puede configurar una auditoría de la actividad del usuario en un dispositivo cliente remoto. Durante la auditoría, la aplicación guarda información sobre los archivos del dispositivo cliente que el administrador haya abierto o modificado.

Para conectarse al escritorio de un dispositivo cliente mediante Uso compartido del escritorio de Windows, se deben cumplir estas condiciones:

- En la estación de trabajo del administrador está instalado Microsoft Windows Vista o posterior.

  Para verificar si la función Uso compartido del escritorio de Windows está incluida en su edición de Windows, asegúrese de que CLSID {32BE5ED2-5C86-480F-A914-0FF8885A1B3F} esté incluido en el registro de 32 bits.

- Microsoft Windows Vista o posterior está instalado en el dispositivo cliente.

- Kaspersky Security Center usa una licencia para la Administración de vulnerabilidades y parches.

Para conectarse al escritorio de un dispositivo cliente mediante el componente Uso compartido del escritorio de Windows:

1. En la Consola de administración basada en MMC, en el menú contextual de la directiva del Servidor de administración, seleccione **Propiedades**.

2. En la ventana de propiedades del Servidor de administración que se abre, vaya a **Configuración de la conexión del Servidor de administración → Puertos de conexión**.

3. Asegúrese de que la opción **Abrir puerto RDP para Kaspersky Security Center 14 Web Console** este habilitada.

4. En Kaspersky Security Center 14 Web Console, vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS → Grupos**, y, a continuación, seleccione el grupo de administración que contiene el dispositivo al que desea obtener acceso.

5. Seleccione la casilla de verificación junto al nombre del dispositivo al que desea acceder.

6. Haga clic en el botón **Uso compartido del escritorio de Windows**.

   El Asistente de Uso compartido del escritorio de Windows se abre.

7. Haga clic en el botón **Descargar** para descargar la utilidad klsctunnel y espere a que se complete el proceso de descarga.

   Si ya tiene la utilidad klsctunnel, omita este paso.

8. Haga clic en el botón **Siguiente**.

9. Seleccione la sesión en el dispositivo al que desea conectarse y luego haga clic en el botón **Siguiente**.

10. En el cuadro de diálogo que se abre en el dispositivo de destino, el usuario debe permitir la sesión de uso compartido de escritorio. De lo contrario, la sesión no es posible.

    Después de que el usuario del dispositivo confirma la sesión de uso compartido de escritorio, se abre la siguiente página del Asistente.

11. Haga clic en el botón **Copiar al portapapeles** para copiar el texto desde el campo de texto. Este texto es un Binary Large OBject (BLOB) que contiene la configuración requerida para establecer la conexión entre el Servidor de administración y el dispositivo administrado.

    Un BLOB es válido por 3 minutos. Si ha expirado, genere un nuevo BLOB.

12. Ejecute la utilidad klsctunnel.

    Se abre la ventana de la utilidad.

13. Pegue el texto copiado en el campo de texto.

14. Si usa un servidor proxy, seleccione la casilla de verificación **Usar servidor proxy** y luego especifique la configuración de conexión del servidor proxy.

15. Haga clic en el botón **Abrir puerto**.

    El uso compartido del escritorio comienza en una nueva ventana. Si desea interactuar con el dispositivo, haga clic en el icono **Menú** () en la esquina superior izquierda de la ventana y luego seleccione **Modo interactivo**.

Selecciones de dispositivos

Las *selecciones de dispositivos* son una herramienta para filtrar dispositivos de acuerdo con condiciones específicas. Puede usar las selecciones de dispositivos para administrar varios dispositivos: por ejemplo, para ver un informe sobre estos dispositivos únicamente o para mover todos estos dispositivos a otro grupo.

Kaspersky Security Center proporciona un amplio intervalo de *selecciones predefinidas* (por ejemplo, **Dispositivos con el estado Crítico**, **La protección está desactivada**, **Se han detectado amenazas activas**). Las selecciones predefinidas no se pueden eliminar. También puede crear y configurar selecciones adicionales *definidas por el usuario*.

En las selecciones definidas por el usuario, puede establecer la cobertura de la búsqueda y seleccionar todos los dispositivos, dispositivos administrados o dispositivos no asignados. Los parámetros de búsqueda se especifican en las condiciones. En la selección de dispositivos puede crear varias condiciones con diferentes parámetros de búsqueda. Por ejemplo, puede crear dos condiciones y especificar diferentes rangos de IP en cada una de ellas. Si se especifican varias condiciones, una selección muestra los dispositivos que cumplen alguna de las condiciones. Por el contrario, los parámetros de búsqueda dentro de una condición están superpuestos. Si tanto el rango de IP como el nombre de una aplicación instalada se especifican en una condición, solo se mostrarán aquellos dispositivos donde la aplicación esté instalada y la dirección de IP pertenezca al rango especificado.

Para ver la selección de dispositivos:

1. En el menú principal, vaya a la sección **DISPOSITIVOS → SELECCIONES DE DISPOSITIVOS** o **DETECCIÓN Y DESPLIEGUE → SELECCIONES DE DISPOSITIVOS**.

2. En la lista de selección, haga clic en el nombre de la selección relevante.

Se muestra el resultado de selección de dispositivos.

Creación de una selección de dispositivos

Para crear una selección de dispositivos:

1. En el menú principal, vaya a **DISPOSITIVOS → SELECCIONES DE DISPOSITIVOS**.

   Se muestra una página con una lista de selecciones de dispositivos.

2. Haga clic en el botón **Añadir**.

   Se abre la ventana **Configuración de Selección de dispositivos**.

3. Introduzca el nombre de la nueva selección.

4. Especifique el tipo de dispositivos que desea incluir en la selección de dispositivos.

5. Haga clic en el botón **Añadir**.

6. En la ventana emergente, especifique las condiciones que se deben cumplir para incluir dispositivos en esta selección y, luego, haga clic en el botón **Aceptar**.

7. Haga clic en el botón **Guardar**.

La selección de dispositivo se crea y se añade a la lista de selecciones de dispositivos.

Configuración de una selección de dispositivos

Para configurar una selección de dispositivos:

1. En el menú principal, vaya a **DISPOSITIVOS → SELECCIONES DE DISPOSITIVOS**.

   Se muestra una página con una lista de selecciones de dispositivos.

2. Haga clic en la selección de dispositivos pertinente que definió el usuario.

   Se abre la ventana **Configuración de Selección de dispositivos**.

3. En la pestaña **Control de aplicaciones**, especifique las condiciones que se deben cumplir para incluir dispositivos en esta selección.

4. Haga clic en el botón **Guardar**.

La configuración se aplica y se guarda.

A continuación, aparecen descripciones de las condiciones para asignar dispositivos a una selección. Las condiciones se combinan con el operador lógico OR. En la selección estarán los dispositivos que cumplan al menos una de las condiciones enumeradas.

General

En la sección **General**, puede cambiar el nombre de una condición de la selección y especificar si esa condición se debería invertir:

- **Revertir condición de la selección**

  Si esta opción está activada, la condición de selección especificada se invertirá. La selección incluirá todos los dispositivos que no cumplen la condición.

  Esta opción está desactivada de forma predeterminada.

Red

En la sección **Red**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según sus datos de la red:

- **Nombre o dirección IP del dispositivo**

  Nombre del dispositivo en la red Windows (nombre de NetBIOS).

- **Dominio de Windows**

  Muestra todos los dispositivos incluidos en el dominio de Windows especificado.

- **Grupo de administración**

  Muestra los dispositivos incluidos en el grupo de administración especificado.

- **Descripción**

Texto de la ventana de propiedades del dispositivo: en el campo **Descripción** de la sección **General**.

Para describir texto en el campo **Descripción**, se pueden utilizar los siguientes caracteres:

- Dentro de una palabra:
  - *****. Sustituye cualquier cadena con cualquier número de caracteres.

    Ejemplo:

    Para describir las palabras como **Servidor** o **Servidores** puedes escribir **Servidor***.
  - **?.** Sustituye cualquier carácter individual.

    Ejemplo:

    Para describir palabras como **Window** o **Windows**, puedes escribir **Windo?**.

    El asterisco (*****) o signo de interrogación (**?**) no se puede utilizar como el primer carácter de la pregunta.
- Para encontrar varias palabras:
  - Espacio. Muestra todos los dispositivos cuyas descripciones contienen alguna de las palabras de la lista.

    Ejemplo:

    Para buscar una frase que incluya las palabras **secundario** o **virtual**, en la consulta puede incluir la línea **secundario virtual**.
  - **+**. Cuando se introduce el signo más delante de una palabra, todos los resultados de la búsqueda incluirán esa palabra.

    Ejemplo:

    Para encontrar una frase que contenga tanto **secundario** como **virtual**, introduzca la consulta **+secundario+virtual**.
  - **-**. Cuando se introduce el signo menos delante de una palabra, ningún resultado de la búsqueda incluirá esa palabra.

    Ejemplo:

    Para encontrar una frase que tenga la palabra **secundario**, pero no la palabra **virtual**, introduzca la consulta **+secundario-virtual**.
  - **"<algún texto>"**. El texto escrito entre comillas debe formar parte del texto.

    Ejemplo:

    Para encontrar una frase que contenga la combinación de palabras **Servidor secundario**, introduzca **"Servidor secundario"** en la consulta.

- Rango IP

  Si esta opción está activada, se pueden introducir las direcciones IP inicial y final del rango IP en el que se incluirán los dispositivos pertinentes.

  Esta opción está desactivada de forma predeterminada.

Etiquetas

En la sección **Etiquetas**, puede configurar criterios para incluir dispositivos en una selección según palabras clave (etiquetas) que se añadieron anteriormente a las descripciones de dispositivos administrados:

- Aplicar si coincide al menos una etiqueta especificada

  Si esta opción está activada, los resultados de las búsquedas mostrarán dispositivos cuyas descripciones contengan al menos una de las etiquetas seleccionadas.

  Si esta opción está desactivada, los resultados de la búsqueda solo mostrarán dispositivos con descripciones que contengan todas las etiquetas seleccionadas.

  Esta opción está desactivada de forma predeterminada.

- La etiqueta debe incluirse

  Si se selecciona esta opción, los resultados de búsqueda mostrarán los dispositivos cuyas descripciones contienen la etiqueta seleccionada. Para buscar dispositivos, puede usar el asterisco, que significa cualquier cadena con cualquier número de caracteres.

  Esta opción está seleccionada de forma predeterminada.

- La etiqueta debe excluirse

  Si esta opción se selecciona, los resultados de búsqueda mostrarán los dispositivos cuyas descripciones no contienen la etiqueta seleccionada. Para buscar dispositivos, puede usar el asterisco, que significa cualquier cadena con cualquier número de caracteres.

Active Directory

En la sección **Active Directory**, puede configurar criterios para incluir dispositivos en una selección según sus datos de Active Directory:

- El dispositivo está en una unidad organizativa de Active Directory

  Si esta opción está activada, la selección incluye dispositivos de la unidad de Active Directory especificada en el campo de entrada.

  Esta opción está desactivada de forma predeterminada.

- Incluir unidades organizativas secundarias

  Si esta opción está activada, la selección incluye dispositivos de todas las unidades organizativas (OU) secundarias de la unidad organizativa de Active Directory especificada.

  Esta opción está desactivada de forma predeterminada.

- Este dispositivo pertenece al grupo de Active Directory

Si esta opción está activada, la selección incluye dispositivos del grupo de Active Directory especificado en el campo de entrada.

Esta opción está desactivada de forma predeterminada.

Actividad de red

En la sección **Actividad de red**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según su actividad de red:

- Este dispositivo es un punto de distribución

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La selección incluirá dispositivos que funcionan como puntos de distribución.
  - **No**. Los dispositivos que funcionan como puntos de distribución no se incluirán en la selección.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- No desconectar del Servidor de administración

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Activado**. La selección incluirá dispositivos en los que la casilla de verificación **No desconectar del Servidor de administración** está seleccionada.
  - **Desactivado**. La selección incluirá dispositivos en los que la casilla de verificación **No desconectar del Servidor de administración** no está seleccionada.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Perfil de conexión cambiado

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La selección incluirá dispositivos que se conectaron al Servidor de administración después del cambio del perfil de conexión.
  - **No**. La selección no incluirá dispositivos que se conectaron al Servidor de administración después del cambio del perfil de conexión.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Última conexión al Servidor de administración

Puede utilizar esta casilla para establecer un criterio de búsqueda de dispositivos en función de la hora de la última conexión al Servidor de administración.

Si se activa esta casilla de verificación, en el campo de entrada se puede especificar el intervalo de tiempo (fecha y hora) durante el que se produjo la última conexión entre el Agente de red instalado en el dispositivo cliente y el Servidor de administración. La selección incluirá los dispositivos que se encuentren dentro del intervalo especificado.

No se aplica el criterio si esta casilla está vacía.

De forma predeterminada, esta casilla está en blanco.

- El sondeo de la red ha detectado dispositivos nuevos

  Busca los nuevos dispositivos que se han detectado mediante el sondeo de la red hace pocos días.

  Si esta opción está activada, la selección incluirá solamente los nuevos dispositivos que se hayan detectado mediante la detección de dispositivos durante el número de días especificados en el campo **Periodo de detección (días)**.

  Si esta opción está desactivada, la selección incluye todos los dispositivos que han sido detectados por detección de dispositivos.

  Esta opción está desactivada de forma predeterminada.

- El dispositivo es visible

  En la lista desplegable, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas:

  - **Sí**. La aplicación incluye en la selección los dispositivos actualmente visibles en la red.
  - **No**. La aplicación incluye en la selección los dispositivos actualmente invisibles en la red.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

Aplicación

En la sección **Aplicación**, puede configurar criterios para incluir dispositivos en una selección según la aplicación administrada seleccionada:

- Nombre de la aplicación

  En la lista desplegable, puede establecer un criterio para incluir los dispositivos en una selección al realizar búsquedas por el nombre de una aplicación Kaspersky.

  La lista proporciona únicamente los nombres de las aplicaciones con los complementos de administración instalados en la estación de trabajo del administrador.

  No se aplica el criterio si no se selecciona ninguna aplicación.

- Versión de la aplicación

  En el campo de entrada, puede establecer un criterio para incluir los dispositivos en una selección al realizar búsquedas por el número de versión de una aplicación Kaspersky.

  No se aplica el criterio si no indica el número de la versión.

- Nombre de la actualización crítica

  En el campo de entrada, puede establecer un criterio para incluir dispositivos en una selección al realizar búsquedas por el nombre de una aplicación o el número de paquete de una actualización.

  No se aplica el criterio si deja el campo en blanco.

- Última actualización de los módulos

  Puede utilizar esta opción como criterio para realizar búsquedas de dispositivos según la hora de la última actualización de los módulos de las aplicaciones instaladas en esos dispositivos.

  Si se selecciona esta casilla, en los campos de entrada podrá especificar el intervalo de tiempo (fecha y hora) en el que se realizó la última actualización de los módulos de las aplicaciones instaladas en esos dispositivos.

  No se aplica el criterio si esta casilla está vacía.

  De forma predeterminada, esta casilla está en blanco.

- El dispositivo se administra a través de Kaspersky Security Center 14

  En la lista desplegable, puede incluir en la selección los dispositivos administrados mediante Kaspersky Security Center:

  - **Sí**. En la selección los dispositivos administrados mediante Kaspersky Security Center.
  - **No**. La aplicación incluye en la selección dispositivos que no estén administrados por Kaspersky Security Center.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

- Aplicación de seguridad instalada

  En la lista desplegable, puede incluir en la selección todos los dispositivos con la aplicación de seguridad instalada:

  - **Sí**. La aplicación incluye en la selección todos los dispositivos con la aplicación de seguridad instalada.
  - **No**. La aplicación incluye en la selección todos los dispositivos que no tienen aplicación de seguridad instalada.
  - **No se ha seleccionado ningún valor**. No se aplica el criterio.

Sistema operativo

En la sección **Sistema operativo**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según su tipo del sistema operativo.

- Versión del sistema operativo

  Si se selecciona esta casilla de verificación, puede seleccionar un sistema operativo de la lista. Los dispositivos que tienen el sistema operativo especificado instalado se incluyen en los resultados de la búsqueda.

- Tamaño de bits del sistema operativo

  En la lista desplegable, puede seleccionar la arquitectura de su sistema operativo, que determinará cómo aplicar la regla de migración a su dispositivo (**Desconocido**, **x86**, **AMD64**, or **IA64**). De forma predeterminada, ninguna opción está seleccionada en la lista de modo que no se define la arquitectura del sistema operativo.

- Versión del Service Pack del sistema operativo

  En este campo, puede especificar la versión del paquete de su sistema operativo (en formato *X.Y.*), que determinará cómo aplicar la regla de migración a su dispositivo. De forma predeterminada, no se especifica ningún valor de la versión.

- Compilación del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de Windows.

  El número de compilación del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un número de compilación igual, anterior o posterior. También puede configurar la búsqueda de todos los números de compilación, excepto el especificado.

- ID de versión del sistema operativo

  Esta configuración solo se aplica a los sistemas operativos de Windows.

  El identificador de la versión (Id.) del sistema operativo. Puede especificar si el sistema operativo seleccionado debe tener un Id. de versión igual, anterior o posterior. También puede configurar la búsqueda de todos los números de Id. de versión, excepto el especificado.

Estado del dispositivo

En la sección **Estado del dispositivo**, puede configurar criterios para incluir dispositivos en una selección según la descripción del estado de dispositivos desde una aplicación administrada:

- Estado del dispositivo

  Lista desplegable en la que se puede seleccionar uno de los estados del dispositivo: *Aceptar*, *Crítico* o *Advertencia*.

- Descripción del estado del dispositivo

  En este campo se pueden seleccionar las casillas de verificación que se muestran junto a las condiciones que, si se cumplen, asignarán uno de los siguientes estados al dispositivo: *Aceptar, Crítico* o *Advertencia*.

- Estado del dispositivo definido por la aplicación

Lista desplegable en la que se puede seleccionar el estado de protección en tiempo real. Se incluyen en la selección los dispositivos que tengan el estado de protección en tiempo real especificado.

Componentes de protección

En la sección **Componentes de protección**, puede configurar los criterios para incluir dispositivos en una selección según su estado de protección:

- Bases de datos lanzadas

  Si esta opción está seleccionada, se puede hacer una búsqueda de dispositivos cliente por la fecha de lanzamiento de la base de datos antivirus. En los campos de entrada se puede establecer el intervalo de tiempo con el que se realizará la búsqueda.

  Esta opción está desactivada de forma predeterminada.

- Número de registros de la base de datos

  Si esta opción está activada, puede buscar dispositivos cliente por número de registros de la base de datos. En los campos de entrada se pueden establecer los valores máximo y mínimo de los registros de la base de datos antivirus.

  Esta opción está desactivada de forma predeterminada.

- Último análisis

  Si esta casilla está activada, se puede hacer una búsqueda de dispositivos cliente por la fecha de último análisis antivirus. En los campos de entrada puede especificar el período de tiempo en el cual se realizó el último análisis antivirus.

  Esta opción está desactivada de forma predeterminada.

- Número total de amenazas detectadas

  Si esta opción está activada, puede buscar dispositivos cliente por número de virus detectados. En los campos de entrada se pueden establecer los valores máximo y mínimo del número de virus encontrados.

  Esta opción está desactivada de forma predeterminada.

Registro de aplicaciones

En la sección **Registro de aplicaciones**, puede configurar los criterios para buscar dispositivos según aplicaciones instaladas en ellos:

- Nombre de la aplicación

  Lista desplegable en la que se puede seleccionar la aplicación. En la selección se incluirán los dispositivos que tengan instalada la aplicación especificada.

- Versión de la aplicación

Campo de entrada en el que se puede especificar la versión de la aplicación seleccionada.

- **Proveedor**

  Lista desplegable en la que se puede seleccionar el fabricante de una aplicación instalada en el dispositivo.

- **Estado de la aplicación**

  Una lista desplegable en la que se puede seleccionar el estado de una aplicación (*Instalada*, *No instalada*). Los dispositivos en los cuales la aplicación especificada está instalada o no instalada, según el estado seleccionado, se incluirán en la selección.

- **Buscar por la actualización**

  Si esta opción está activada, la búsqueda se realizará utilizando los detalles de las actualizaciones para las aplicaciones instaladas en los dispositivos relevantes. Después de seleccionar la casilla de verificación, los campos **Nombre de la aplicación**, **Versión de la aplicación** y **Estado de la aplicación** cambian a **Nombre de actualización**, **Versión de actualización** y **Estado** respectivamente.

  Esta opción está desactivada de forma predeterminada.

- **Nombre de la aplicación de seguridad incompatible**

  Lista desplegable en la que se puede seleccionar aplicaciones de seguridad de terceros. Durante la búsqueda, se incluirán en la selección los dispositivos que tengan instalada la aplicación especificada.

- **Etiqueta de la aplicación**

  En la lista desplegable se puede seleccionar la etiqueta de la aplicación. Todos los dispositivos que han instalado aplicaciones con la etiqueta seleccionada en la descripción se incluyen en la selección de dispositivos.

- **Aplicar a los dispositivos que no tengan etiquetas especificadas**

  Si esta opción está activada, el perfil de la directiva incluirá los dispositivos con descripciones que no contengan ninguna de las etiquetas seleccionadas.

  Si esta opción está desactivada, el software no se actualiza.

  Esta opción está desactivada de forma predeterminada.

Registro de hardware

En la sección **Registro de hardware**, puede configurar criterios para incluir dispositivos incluidos en una selección según su hardware instalado:

- **Dispositivo**

En la lista desplegable, puede seleccionar el tipo de unidad. Todos los dispositivos con esta unidad se incluyen en los resultados de la búsqueda.

El campo admite búsqueda de texto completo.

- **Proveedor**

  En la lista desplegable se puede seleccionar el nombre del fabricante de la unidad. Todos los dispositivos con esta unidad se incluyen en los resultados de la búsqueda.

  El campo admite búsqueda de texto completo.

- **Nombre del dispositivo**

  Nombre del dispositivo cliente en la red Windows. El dispositivo con el nombre especificado se incluirá en la selección.

- **Descripción**

  Descripción del dispositivo o unidad de hardware. Los dispositivos con la descripción especificada en este campo se incluirán en la selección.

  La descripción de un dispositivo en cualquier formato se puede introducir en la ventana de propiedades de ese dispositivo. El campo admite búsqueda de texto completo.

- **Proveedor del dispositivo**

  Nombre del fabricante del dispositivo. Los dispositivos fabricados por el fabricante especificado en este campo se incluirán en la selección.

  Puede introducir el nombre del fabricante en la ventana de propiedades de un dispositivo.

- **Número de serie**

  Todas las unidades de hardware con el número de serie especificado en este campo se incluirán en la selección.

- **Número de inventario**

  El equipo con el número de inventario especificado en este campo se incluirá en la selección.

- **Usuario**

  Todas las unidades de hardware del usuario especificado en este campo se incluirán en la selección.

- **Ubicación**

Ubicación de un dispositivo o una unidad de hardware (por ejemplo, en la sede central o en una filial). Los dispositivos u otros dispositivos desplegados en la ubicación especificada en este campo se incluirán en la selección.

Puede describir la ubicación de un dispositivo en cualquier formato en la ventana de propiedades de ese dispositivo.

- Frecuencia de la CPU (MHz)

  Intervalo de frecuencia de una CPU. Los dispositivos con las CPU que coincidan con el intervalo de frecuencia especificado en estos campos (valores máximo y mínimo incluidos) se incluirán en la selección.

- Núcleos de CPU virtual

  Intervalo del número de núcleos virtuales en una CPU. Los dispositivos con las CPU que coincidan con el intervalo especificado en estos campos (valores máximo y mínimo incluidos) se incluirán en la selección.

- Volumen del disco duro, en GB

  Intervalo de los valores para el tamaño del disco duro en el dispositivo. Los dispositivos con los discos duros que coincidan con el intervalo especificado en estos campos de entrada (valores máximo y mínimo incluidos) se incluirán en la selección.

- Tamaño de RAM, en MB

  Intervalo de los valores para el tamaño de la RAM de un dispositivo. Los dispositivos con las RAM que coincidan con el intervalo especificado en estos campos de entrada (valores máximo y mínimo incluidos) se incluirán en la selección.

Máquinas virtuales

En la sección **Máquinas virtuales**, puede configurar los criterios para incluir dispositivos en la selección según si estos son máquinas virtuales o parte de la Infraestructura de escritorio virtual (VDI):

- Es una máquina virtual

  En la lista desplegable se pueden seleccionar las siguientes opciones:

  - **No es importante**.
    - **No**. Buscar dispositivos que no son máquinas virtuales.
    - **Sí**. Buscar dispositivos que son máquinas virtuales.

- Tipo de máquina virtual

  En la lista desplegable se puede seleccionar el fabricante de la máquina virtual.

  Esta lista desplegable está disponible si el valor **Sí** o **No es importante** se selecciona en la lista desplegable **Es una máquina virtual**.

- Parte de la infraestructura de escritorio virtual

  En la lista desplegable se pueden seleccionar las siguientes opciones:

  - **No es importante**.
    - **No**. Buscar dispositivos que no formen parte de la Infraestructura de escritorio virtual.
    - **Sí**. Buscar dispositivos que formen parte de una Infraestructura de escritorio virtual (VDI) de Microsoft.

Vulnerabilidades y actualizaciones

En la sección **Vulnerabilidades y actualizaciones**, puede especificar los criterios que serán usados para incluir dispositivos en la selección según su fuente de Windows Update:

- El WUA se ha cambiado al Servidor de administración

  Puede seleccionar una de las opciones de búsqueda de la lista desplegable:

  - **Sí**. Si se selecciona esta opción, en los resultados de la búsqueda se incluirán los dispositivos que reciben actualizaciones del Servidor de administración a través de Windows Update.
  - **No**. Si se selecciona esta opción, en los resultados se incluirán los dispositivos que reciben actualizaciones de otras fuentes a través de Windows Update.

Usuarios

En la sección **Usuarios**, puede configurar los criterios para incluir dispositivos en la selección según las cuentas de usuarios que han iniciado sesión en el sistema operativo.

- Último usuario que inició sesión en el sistema

  Si esta opción está activada, haga clic en el botón **Examinar** para especificar una cuenta de usuario. Los resultados de la búsqueda incluyen los dispositivos en los que un usuario específico ha iniciado sesión por última vez.

- Usuario que inició sesión en el sistema al menos una vez

  Si esta opción está activada, haga clic en el botón **Examinar** para especificar una cuenta de usuario. Los resultados de la búsqueda incluyen los dispositivos en los que el usuario especificado inició sesión en el sistema al menos una vez.

Problemas relacionados con el estado de las aplicaciones administradas

En la sección **Problemas relacionados con el estado de las aplicaciones administradas**, puede especificar los criterios que se utilizarán para incluir dispositivos en la selección de acuerdo con la lista de posibles problemas detectados por una aplicación administrada. Si al menos un problema que selecciona existe en un dispositivo, el dispositivo se incluirá en la selección. Cuando selecciona un problema listado para varias aplicaciones, tiene la opción de seleccionar este problema en todas las listas automáticamente.

- Descripción del estado del dispositivo

  En este campo puede seleccionar las casillas para las descripciones de estados desde la aplicación administrada; al recibir estos estados, los dispositivos se incluirán en la selección. Cuando selecciona un estado listado para varias aplicaciones, tiene la opción de seleccionar este estado en todas las listas automáticamente.

Estados de los componentes en aplicaciones administradas

En la sección **Estados de los componentes en aplicaciones administradas**, puede configurar criterios para incluir dispositivos en una selección según los estados de componentes en aplicaciones administradas:

- Estado de la prevención contra fugas de datos

  Buscar dispositivos por el estado de Prevención de fuga de datos (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- Estado de la protección de los servidores de colaboración

  Buscar dispositivos por el estado de la protección de colaboración del servidor (*No hay datos del dispositivo*, *Detenido*, *Iniciando, En pausa*, *En ejecución*, *Fallo*).

- Estado de la protección antivirus de servidores de correo

  Buscar dispositivos por el estado de protección del servidor de correo (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

- Estado de sensor de Endpoint

  Buscar dispositivos por el estado del componente del sensor de Endpoint (*No hay datos del dispositivo, Detenido, Iniciando, En pausa, En ejecución, Fallo*).

Cifrado

Algoritmo de cifrado

Algoritmo de cifrado de bloques simétricos Advanced Encryption Standard (AES). En la lista desplegable, puede seleccionar el tamaño de la clave de cifrado (de 56 bits, de 128 bits, de 192 bits o de 256 bits).

Valores disponibles: *AES56*, *AES128*, *AES192* y *AES256*.

Segmentos de la nube

En la sección **Segmentos de la nube**, puede configurar criterios para incluir dispositivos en una selección según sus segmentos de la nube respectivos:

- El dispositivo está en un segmento de la nube

Si esta opción está activada, puede hacer clic en el **Examinar** para especificar qué segmento buscar.

Si la opción **Incluir objetos secundarios** también está activada, la búsqueda se ejecuta en todos los objetos secundarios del segmento especificado.

Los resultados de la búsqueda solo incluyen dispositivos desde el segmento seleccionado.

- Dispositivo descubierto mediante la API

  En la lista desplegable, puede seleccionar si un dispositivo es detectado por herramientas API.

  - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de AWS.
  - **Azure**. El dispositivo se descubre mediante la Azure API, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
  - **Google Cloud.**El dispositivo se descubre mediante la API de Google, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de Google.
  - **No**. El dispositivo no se puede detectar con AWS, Azure o Google API, es decir, o bien está fuera del entorno de nube, o está en el entorno de nube pero no se puede detectar mediante API por algún motivo.
  - Ningún valor. Este criterio no se puede aplicar.

Componentes de la aplicación

Esta sección contiene la lista de componentes de aquellas aplicaciones que tienen complementos de administración correspondientes instalados en la Consola de administración.

En la sección **Componentes de la aplicación**, puede especificar los criterios para incluir dispositivos en una selección de acuerdo con los estados y números de versión de los componentes que se refieren a la aplicación que seleccione:

- Estado

Buscar dispositivos de acuerdo con el estado del componente enviado por una aplicación al Servidor de administración. Puede seleccionar uno de los siguientes estados: *No se reciben datos del dispositivo*, *Detenido*, *Iniciado*, *Pausado*, *En ejecución*, *Mal funcionamiento* o *No instalado*. Si el componente seleccionado de la aplicación instalada en un dispositivo administrado tiene el estado especificado, el dispositivo se incluye en la selección de dispositivos.

Estados enviados por solicitudes:

- *Iniciando:* El componente está actualmente en el proceso de iniciación.
- *En ejecución:* El componente se activa y funciona correctamente.
- *En pausa:* El componente se suspende, por ejemplo, después de que el usuario ha hecho una pausa la protección en la aplicación administrada.
- *Mal funcionamiento:* Un error ha ocurrido durante la operación del componente.
- *Detenido:* El componente está desactivado y no funciona en este momento.
- *No instalado:* El usuario no seleccionó el componente para la instalación al configurar la instalación personalizada de la aplicación.

A diferencia de otros estados, las aplicaciones *no envían datos del estado del dispositivo*. Esta opción muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Por ejemplo, esto puede suceder cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo o cuando el dispositivo está apagado.

- **Versión**

  Buscar dispositivos de acuerdo con el número de versión del componente que seleccione en la lista. Puede escribir un número de versión, por ejemplo `3.4.1.0`, y luego especificar si el componente seleccionado debe tener una versión igual, anterior o posterior. También puede configurar la búsqueda de todas las versiones excepto la especificada.

Etiquetas del dispositivo

Esta sección describe las etiquetas de dispositivos y proporciona instrucciones para crearlas y modificarlas, así como para etiquetar dispositivos de forma manual o automática.

Acerca de las etiquetas del dispositivo

Kaspersky Security Center permite que usted *etiquete* dispositivos. Una etiqueta es un identificador de un dispositivo que se puede utilizar para agrupar, describir o encontrar dispositivos. Las etiquetas asignadas a dispositivos se pueden utilizar para crear selecciones, para encontrar dispositivos y para distribuir dispositivos entre grupos de administración.

Puede etiquetar dispositivos manualmente o automáticamente. Puede utilizar el etiquetado manual cuando desee etiquetar un dispositivo particular. Kaspersky Security Center realiza el etiquetado automático de acuerdo con las reglas de etiquetado especificadas.

Los dispositivos se etiquetan automáticamente cuando las reglas especificadas se cumplen. Una regla particular equivale a cada etiqueta. Las reglas se aplican a las propiedades de la red del dispositivo, sistema operativo, aplicaciones instaladas en el dispositivo y otras propiedades del dispositivo. Por ejemplo, si tiene una infraestructura híbrida de máquinas físicas, las instancia de Amazon EC2 y las máquinas virtuales de Microsoft Azure, puede configurar una regla que asignará la etiqueta `[Azure]` a todas las máquinas virtuales de Microsoft Azure. A continuación, puede usar esta etiqueta al crear una selección de dispositivos; esto le ayudará a clasificar todas las máquinas virtuales de Microsoft Azure y a asignarles una tarea.

Una etiqueta se elimina automáticamente desde un dispositivo en los siguientes casos:

- Cuando el dispositivo deja de cumplir las condiciones de la regla que asigna la etiqueta.
- Cuando la regla que asigna la etiqueta se desactiva o elimina.

La lista de etiquetas y la lista de reglas de cada Servidor de administración son independientes de todos los demás Servidores de administración, incluido un Servidor de administración principal o Servidores de administración virtuales subordinados. Una regla se aplica solo a los dispositivos del mismo Servidor de administración en el que se crea la regla.

Creación de una etiqueta de dispositivo

Para crear una etiqueta de dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS** → **ETIQUETAS** → **ETIQUETAS DEL DISPOSITIVO**.
2. Haga clic en **Añadir**.
   Una nueva ventana de etiqueta se abre.
3. En el campo **Etiqueta**, escriba un nombre de etiqueta.
4. Haga clic en **Guardar** para guardar los cambios.

La nueva etiqueta aparece en la lista de etiquetas de dispositivo.

Cambiar el nombre de una etiqueta de dispositivo

Para renombrar una etiqueta del dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS** → **ETIQUETAS** → **ETIQUETAS DEL DISPOSITIVO**.
2. Haga clic en el nombre de la etiqueta que desea renombrar.
   Se abre la ventana de propiedades de la etiqueta.
3. En el campo **Etiqueta**, cambie el nombre de etiqueta.
4. Haga clic en **Guardar** para guardar los cambios.

La etiqueta actualizada aparece en la lista de etiquetas del dispositivo.

Eliminar una etiqueta de dispositivo

Eliminar una etiqueta del dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS** → **ETIQUETAS** → **ETIQUETAS DEL DISPOSITIVO**.
2. En la lista, seleccione el botón de opción junto a la etiqueta del dispositivo que desea eliminar.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Sí**.

   Se elimina la etiqueta del dispositivo. La etiqueta eliminada se elimina automáticamente de todos los dispositivos a los que fue asignada.

> La etiqueta que eliminó se elimina automáticamente de las reglas de etiquetado automático. Después de eliminar la etiqueta, se asignará a un nuevo dispositivo solo cuando el dispositivo cumpla las condiciones de una regla que asigne la etiqueta.

Visualización de dispositivos a los que se asigna una etiqueta

Para ver los dispositivos a los que se asigna una etiqueta:

1. En el menú principal, vaya a **DISPOSITIVOS** → **ETIQUETAS** → **ETIQUETAS DEL DISPOSITIVO**.
2. Haga clic en el enlace **Ver dispositivos** al lado de la etiqueta para la cual desea ver los dispositivos asignados.

   Si no ve el enlace **Ver dispositivos** al lado de una etiqueta, la etiqueta no se asigna a ningún dispositivo.

   La lista de dispositivos que aparece muestra solo los dispositivos a los que se asigna la etiqueta.

Para volver a la lista de etiquetas del dispositivo, haga clic en el botón **Atrás** de su navegador.

Visualización de etiquetas asignadas a un dispositivo

Para visualizar etiquetas asignadas a un dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el nombre de la directiva cuyos etiquetas desea ver.
3. En la ventana de propiedades del dispositivo que se abre, seleccione la pestaña **Etiquetas**.

   Se muestra la lista de etiquetas asignadas al dispositivo seleccionado.

Puede asignar otra etiqueta al dispositivo o eliminar una etiqueta ya asignada. También puede ver todas las etiquetas del dispositivo que existen en el Servidor de administración.

Etiquetar un dispositivo manualmente

Para asignar una etiqueta a un dispositivo manualmente:

1. Ver las etiquetas asignadas al dispositivo al que desea eliminar una etiqueta.
2. Haga clic en **Añadir**.
3. En la ventana que se abre, realice una de las siguientes acciones:
   - Para crear y asignar una nueva etiqueta, seleccione **Crear nueva etiqueta** y después especifique el nombre de la nueva etiqueta.
   - Para seleccionar una etiqueta existente, seleccione **Asignar etiqueta existente** y después seleccione la etiqueta necesaria en la lista desplegable.
4. Haga clic en **Correcto** para aplicar los cambios.
5. Haga clic en **Guardar** para guardar los cambios.

La etiqueta seleccionada está asignada al dispositivo.

Eliminación de una etiqueta asignada de un dispositivo

Para eliminar una etiqueta del dispositivo:

1. Vea las etiquetas asignadas al dispositivo al que desea eliminar una etiqueta.
2. Seleccione la casilla al lado de las etiquetas que desea eliminar.
3. Haga clic en el botón **Desasignar etiqueta**.
4. En la ventana que se abre, haga clic en **Sí**.

La etiqueta se elimina del dispositivo.

La etiqueta del dispositivo no asignado no se elimina. Si lo desea, puede borrarlo manualmente.

Visualización de reglas de etiquetado automático de dispositivos

Para visualizar las reglas para etiquetar dispositivos automáticamente,

Realice una de las siguientes acciones:

- En el menú principal, vaya a **DISPOSITIVOS → ETIQUETAS → REGLAS DE ETIQUETADO AUTOMÁTICO**.

- En el menú principal, vaya a **DISPOSITIVOS** → **ETIQUETAS** y, luego, haga clic en el enlace **Configurar reglas de etiquetado automático**.
- Vea las etiquetas asignadas a un dispositivo y después haga clic en el botón **Configuración**.

Aparece la lista de reglas para los dispositivos de etiquetado automático.

Modificación de una regla de etiquetado automático de dispositivos

Para editar una regla para etiquetar dispositivos automáticamente:

1. Vea las reglas de etiquetado automático en dispositivos.
2. Haga clic en el nombre de la etiqueta que desea editar.

   Se abrirá una ventana de configuración de reglas.
3. Editar las propiedades generales de la regla:

   a. En el campo **Nombre de la regla**, cambie el nombre de regla.

   El nombre no puede tener más de 256 caracteres.

   b. Realice una de las siguientes acciones:

   - Habilite la regla cambiando el botón de activación a **Regla activada**.
   - Deshabilite la regla cambiando el botón de activación a **Regla desactivada**.
4. Realice una de las siguientes acciones:

   - Si desea agregar una nueva condición, haga clic en el botón **Añadir** y especifique la configuración de la nueva condición en la ventana que se abre.
   - Si desea editar una condición existente, haga clic en el nombre de la condición que desea editar y luego edite la configuración de la condición.
   - Si desea eliminar una condición, seleccione la casilla de verificación al lado del nombre de la condición que desea eliminar, y luego haga clic en **Eliminar**.
5. Haga clic en **Aceptar** en la ventana de configuración de las condiciones.
6. Haga clic en **Guardar** para guardar los cambios.

La regla editada se muestra en la lista.

Creación de una regla de etiquetado automático de dispositivos

Para crear una regla de etiquetado automático en dispositivos:

1. Vea las reglas de etiquetado automático en dispositivos.

2. Haga clic en **Añadir**.

   Se abre una nueva ventana de configuración de regla.

3. Configure las propiedades generales de la regla:

   a. En el campo **Nombre de la regla**, introduzca un nombre de regla.

      El nombre no puede tener más de 256 caracteres.

   b. Realice una de las siguientes acciones:

      - Habilite la regla cambiando el botón de activación a **Regla activada**.
      - Deshabilite la regla cambiando el botón de activación a **Regla desactivada**.

   c. En el campo **Etiqueta**, introduzca el nuevo nombre de etiqueta del dispositivo o seleccione una de las etiquetas del dispositivo existentes en la lista.

      El nombre no puede tener más de 256 caracteres.

4. En la sección de condiciones, haga clic en el botón **Añadir** para añadir una nueva condición.

   Se abre una nueva ventana de configuración de condiciones.

5. Introduzca el nombre de la condición.

   El nombre no puede tener más de 256 caracteres. El nombre debe ser único en una regla.

6. Configure la activación de la regla de acuerdo con las condiciones siguientes. Puede seleccionar varias condiciones.

   - **Red**: Las propiedades de la red del dispositivo, por ejemplo, nombre del dispositivo en la red Windows o inclusión del dispositivo en un dominio, o una subred IP.
   - **Aplicaciones**: Presencia del Agente de red en el dispositivo, tipo del sistema operativo, versión y arquitectura.
   - **Máquinas virtuales**: El dispositivo pertenece a un tipo concreto de máquina virtual.
   - **Usuario de Active Directory**: Presencia del dispositivo en la unidad organizativa de Active Directory e ingreso del dispositivo en un grupo de Active Directory.
   - **Registro de aplicaciones**: Presencia de aplicaciones de proveedores diferentes en el dispositivo.

7. Haga clic en **Aceptar** para guardar los cambios.

   Si es necesario, puede establecer varias condiciones para una sola regla. En este caso, la etiqueta se asignará a un dispositivo si cumple al menos una condición.

8. Haga clic en **Guardar** para guardar los cambios.

Las regla recién creada se hace cumplir en dispositivos administrados por el Servidor de administración seleccionado. Si la configuración de un dispositivo cumple las condiciones de la regla, se asigna la etiqueta al dispositivo.

Más adelante, la regla se aplica en los siguientes casos:

- Automática y periódicamente, según la cantidad de trabajo del servidor.

- Después de que edite la regla.
- Cuando ejecute la regla manualmente.
- Después de que el Servidor de administración detecte un cambio en la configuración de un dispositivo que cumpla las condiciones de la regla o la configuración de un grupo que contenga dicho dispositivo.

Puede crear varias reglas de etiquetado. Pueden asignarse varias etiquetas a un solo dispositivo si ha creado varias reglas de etiquetado y si las condiciones respectivas de estas reglas se cumplen simultáneamente. Puede ver la lista de todas las etiquetas asignadas en las propiedades del dispositivo.

Ejecución de reglas de etiquetado automático de dispositivos

Cuando se ejecuta una regla, la etiqueta especificada en las propiedades de esta regla se asigna a los dispositivos que cumplen con las condiciones especificadas en las propiedades de la misma regla. Solo puede ejecutar reglas activas.

Para ejecutar reglas para dispositivos de etiquetado automático:

1. Vea las reglas de etiquetado automático en dispositivos.
2. Seleccione las casillas de verificación junto a las reglas activas que desea ejecutar.
3. Haga clic en el botón **Ejecutar regla**.

   Se ejecutan las reglas seleccionadas.

Eliminación de una regla de etiquetado automático de dispositivos

Para eliminar una regla para etiquetar dispositivos automáticamente:

1. Vea las reglas de etiquetado automático en dispositivos.
2. Seleccione la casilla de verificación al lado de las etiquetas que desea eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

   Se eliminar la regla seleccionada. La etiqueta que se especificó en las propiedades de esta regla no está asignada a todos los dispositivos a los que fue asignada.

> La etiqueta del dispositivo no asignado no se elimina. Si lo desea, puede borrarlo manualmente.

Directivas y perfiles de directivas

En Kaspersky Security Center 14 Web Console, puede crear directivas para las aplicaciones de Kaspersky. Esta sección describe las directivas y los perfiles de directivas, y proporciona instrucciones para crearlos y modificarlos.

Acerca de las directivas y perfiles de directivas

Una *directiva* es un conjunto de configuraciones de aplicaciones de Kaspersky que se aplican a un grupo de administración y sus subgrupos. Puede instalar varias aplicaciones de Kaspersky en los dispositivos de un grupo de administración. Kaspersky Security Center proporciona una directiva única para cada aplicación de Kaspersky en un grupo de administración. Una directiva tiene uno de los siguientes estados (consulte la tabla a continuación):

El estado de la directiva

Estado	Descripción
Activo	La directiva actual que se aplica al dispositivo. Solo una directiva puede estar activa para una aplicación de Kaspersky en cada grupo de administración. Los dispositivos aplican los valores de configuración de una directiva activa para una aplicación de Kaspersky.
Inactiva	Una directiva que no se aplica actualmente a un dispositivo.
Fuera de la oficina	Si se selecciona esta opción, la directiva se activa cuando un dispositivo sale de la red corporativa.

Las directivas funcionan según las siguientes reglas:

- Se pueden configurar varias directivas con diferentes valores para una única aplicación.
- Solo una directiva puede estar activa para la aplicación actual.
- Puede activar una directiva inactiva cuando ocurre un evento específico. Por ejemplo, puede aplicar una configuración de protección antivirus más estricta durante un brote de virus.
- Una directiva puede tener directivas secundarias.

Generalmente, puede utilizar las directivas como preparación para situaciones de emergencia, como el ataque de un virus. Por ejemplo, si se trata de un ataque a través de unidades flash, puede activar una directiva que bloquee el acceso a las unidades flash. En este caso, la directiva activa actual se vuelve inactiva automáticamente.

Para evitar el mantenimiento de varias directivas, por ejemplo, cuando en diferentes ocasiones se supone el cambio de varias configuraciones únicamente, puede utilizar perfiles de directivas.

Un *perfil de directiva* es un subconjunto con nombre de valores de configuración de directiva que reemplaza los valores de configuración de una directiva. Un perfil de directiva afecta la formación de configuraciones efectivas en un dispositivo administrado. Las *configuraciones efectivas* son un conjunto de configuraciones de directivas, configuraciones de perfiles de directivas y configuraciones de aplicaciones locales que están aplicadas en ese momento en el dispositivo.

Los perfiles de directivas funcionan según las siguientes reglas:

- Un perfil de directiva entra en vigor cuando se produce una condición de activación específica.
- Los perfiles de directivas contienen valores de configuración que difieren de la configuración de la directiva.
- La activación de un perfil de directiva cambia la configuración efectiva del dispositivo administrado.
- Una directiva puede incluir un máximo de 100 perfiles de directivas.

Acerca del bloqueo y los ajustes bloqueados

Cada configuración de directiva tiene un icono de botón de bloqueo ( ). La siguiente tabla muestra los estados de los botones de bloqueo:

Estados de los botones de bloqueo

Estado	Descripción
Sin definir	Si se muestra un candado abierto junto a una configuración y el botón de alternar está desactivado, la configuración no está especificada en la directiva. El usuario puede cambiar esta configuración en la interfaz de la aplicación administrada. Este tipo de configuraciones se denominan *configuraciones desbloqueadas*.
Aplicar	Si se muestra un candado cerrado junto a una configuración y el botón de alternancia está activado, la configuración se aplica a los dispositivos donde se la directiva es obligatoria. Un usuario no podrá modificar los valores de esta configuración en l interfaz de la aplicación administrada. Este tipo de configuraciones se denominan *configuraciones bloqueadas*.

Recomendamos encarecidamente que cierre los bloqueos para la configuración de la directiva que desea aplicar en los dispositivos administrados. La configuración de la directiva desbloqueada se puede reasignar mediante la configuración de la aplicación Kaspersky en un dispositivo administrado.

Puede utilizar un botón de bloqueo para realizar las siguientes acciones:

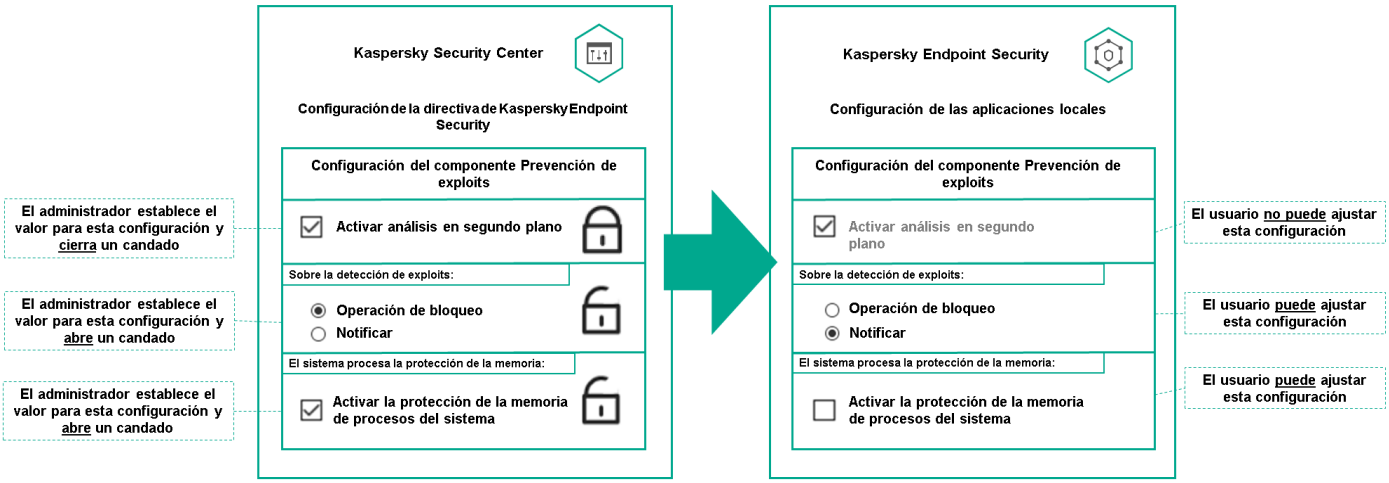
- Bloqueo de la configuración para una directiva de subgrupo de administración
- Bloqueo de la configuración de una aplicación de Kaspersky en un dispositivo administrado

Por lo tanto, una configuración bloqueada se utiliza para implementar configuraciones efectivas en un dispositivo administrado.

Un proceso de implementación efectiva de configuraciones incluye las siguientes acciones:

- El dispositivo administrado aplica los valores de configuración de la aplicación Kaspersky.
- El dispositivo administrado aplica los valores de configuración bloqueados de una directiva.

Una directiva y una aplicación de Kaspersky local contienen el mismo conjunto de configuraciones. Cuando ajusta la configuración de directiva, la configuración de la aplicación de Kaspersky cambia los valores en un dispositivo administrado. Usted no puede ajustar la configuración bloqueada en un dispositivo administrado (consulte la figura a continuación):



Configuración de bloqueos y aplicaciones de Kaspersky

Herencia de directivas y perfiles de directivas

Esta sección brinda información sobre la jerarquía y la herencia de directivas y perfiles de directivas.

Jerarquía de directivas

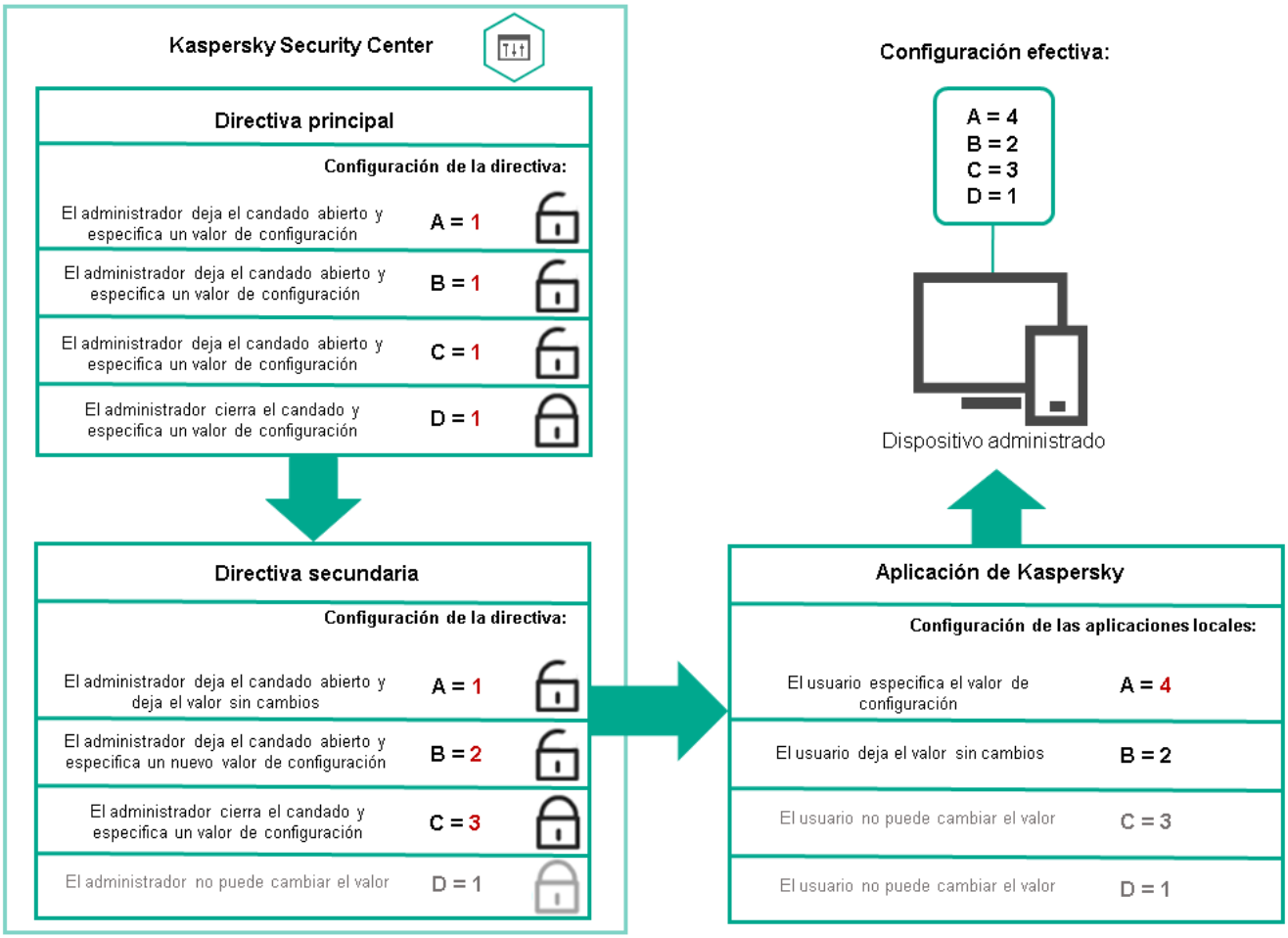
Si diferentes dispositivos necesitan diferentes configuraciones, puede organizar los dispositivos en grupos de administración.

Puede especificar una directiva para un grupo de administración único. La configuración de la directiva se puede *heredar*. Heredar una directiva significa recibir valores de configuración de directivas en subgrupos (grupos secundarios) de una directiva de un grupo de administración de nivel superior (principal).

En adelante, también se hará referencia a una directiva para un grupo primario como *directiva primaria*. Una directiva para un subgrupo (grupo secundario) también se denomina *directiva secundaria*.

De forma predeterminada, existe al menos un grupo de dispositivos administrados en el Servidor de administración. Si desea crear grupos personalizados, se crean como subgrupos (grupos secundarios) dentro del grupo de dispositivos administrados.

Las directivas de la misma aplicación actúan entre sí, de acuerdo con una jerarquía de grupos de administración. La configuración bloqueada de una directiva de un grupo de administración de nivel superior (principal) reasignará los valores de configuración de la directiva de un subgrupo (consulte la figura siguiente).

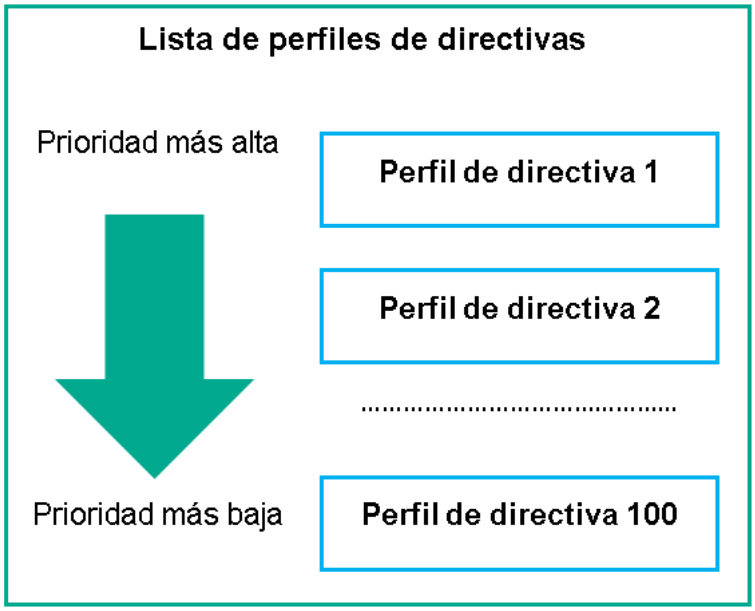


Jerarquía de directivas

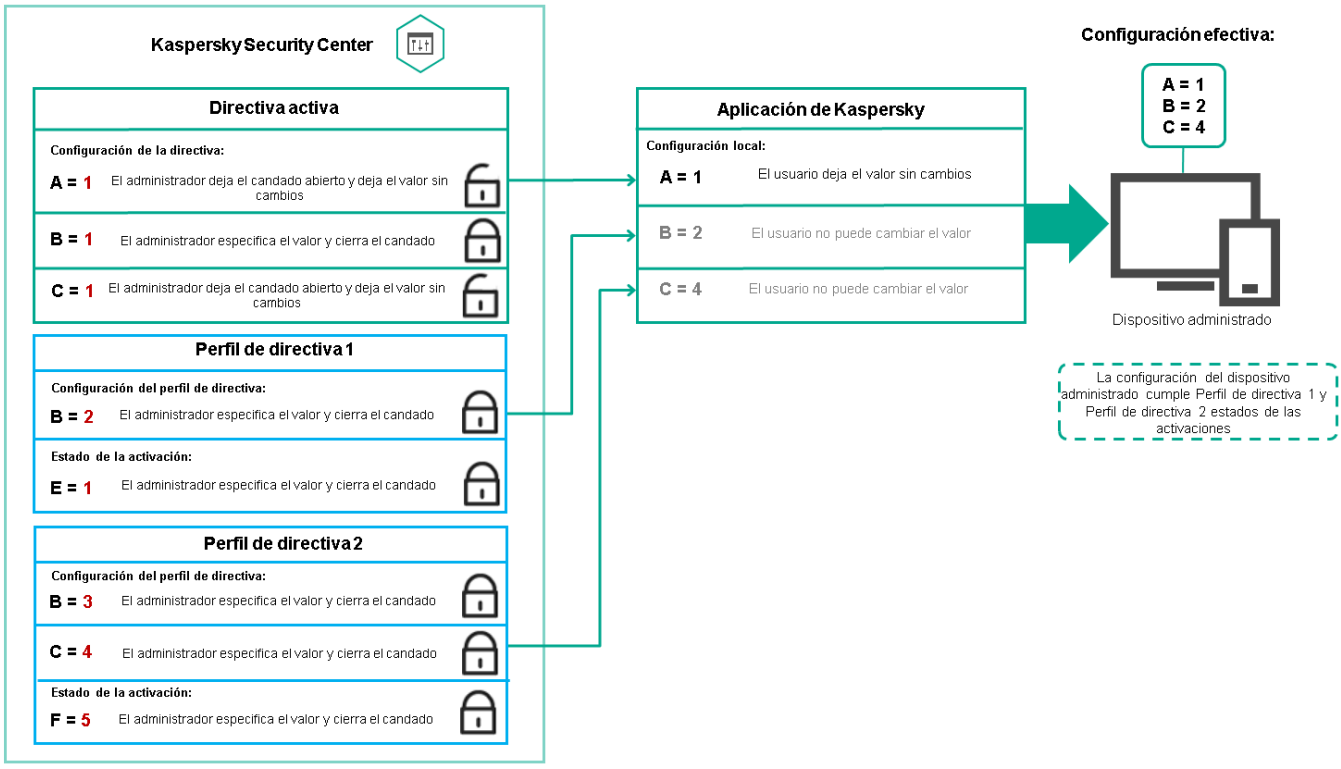
Perfiles de directivas en una jerarquía de directivas

Los perfiles de directiva tienen las siguientes condiciones de asignación de prioridad:

- La posición de un perfil en una lista de perfiles de directivas indica su prioridad. Puede cambiar una prioridad de perfil de directiva. La posición más alta en una lista indica que la máxima prioridad (consulte la siguiente figura).



- Las condiciones de activación de los perfiles de directivas no dependen unas de otras. Se pueden activar varios perfiles de directivas simultáneamente. Si varios perfiles de directiva afectan la misma configuración, el dispositivo toma el valor de configuración del perfil de directiva con la prioridad más alta (consulte la siguiente figura).



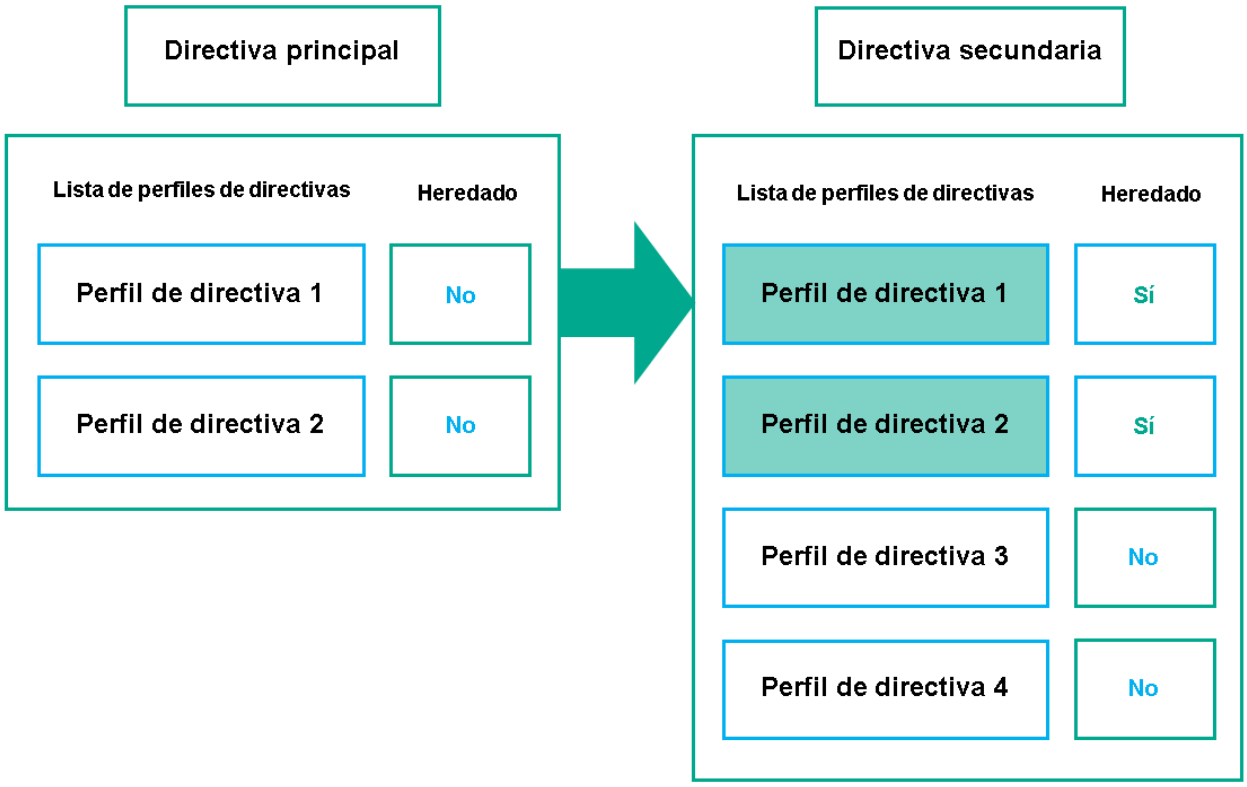
La configuración del dispositivo administrado cumple las condiciones de activación de varios perfiles de directivas

Perfiles de directivas en una jerarquía de herencia

Los perfiles de directiva de las directivas de diferentes niveles de jerarquía cumplen con las siguientes condiciones:

- Una directiva de nivel inferior hereda los perfiles de directivas de una directiva de nivel superior. Un perfil de directiva heredado de una directiva de nivel superior tiene mayor prioridad que el nivel del perfil de directiva original.

- No puede cambiar la prioridad de un perfil de directiva heredado (consulte la figura siguiente).

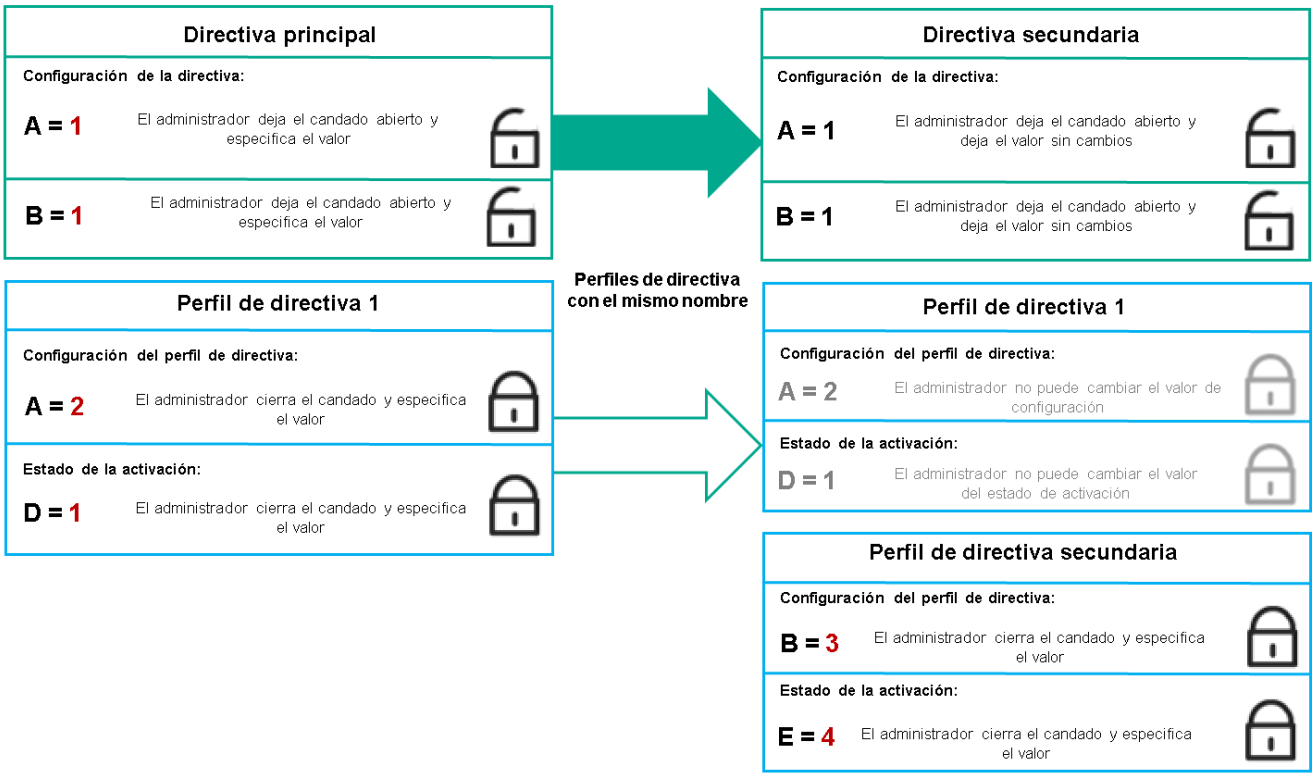


Herencia de los perfiles de directiva

Perfiles de directiva con el mismo nombre

Si hay dos directivas con el mismo nombre en diferentes niveles de jerarquía, estas directivas funcionan de acuerdo con las siguientes reglas:

- La configuración bloqueada y la condición de activación del perfil de un perfil de directiva de nivel superior cambian la configuración y la condición de activación del perfil de un perfil de directiva de nivel inferior (consulte la siguiente figura).



El perfil secundario hereda los valores de configuración de un perfil de directiva principal

- La configuración desbloqueada y la condición de activación del perfil de un perfil de directiva de nivel superior no cambian la configuración y la condición de activación del perfil de un perfil de directiva de nivel inferior.

Cómo se implementan las configuraciones en un dispositivo administrado

La implementación de configuraciones efectivas en un dispositivo administrado se puede describir de la siguiente manera:

- Los valores de todos los ajustes que no se han bloqueado se toman de la directiva.
- Luego se sobrescriben con los valores de los ajustes de la aplicación administrada.
- Y luego se aplican los valores de configuración bloqueados de la directiva efectiva. Los valores de los ajustes bloqueados cambian los valores de los ajustes efectivos desbloqueados.

Administrar directivas

Esta sección describe la gestión de directivas y proporciona información sobre cómo ver la lista de directivas, crear una directiva, modificar una directiva, copiar una directiva, mover una directiva, forzar la sincronización, ver el cuadro de estado de distribución de directivas y eliminar una directiva.

Visualización de la lista de directivas

Puede ver las listas de directivas creadas para el Servidor de administración o para cualquier grupo de administración.

Para ver una lista de directivas:

1. En el menú principal, vaya a **DISPOSITIVOS → JERARQUÍA DE GRUPOS**.
2. En la estructura del grupo de administración, seleccione el grupo de administración para el que desea ver la lista de directivas.

Aparece la lista de directivas en formato tabular. Si no hay directivas, la tabla está vacía. Puede mostrar o esconder las columnas de la tabla, cambiar su orden, ver solo las líneas que contienen un valor que especifique o utilizar la búsqueda.

Creación de una directiva

Puede crear directivas; también puede modificar y eliminar directivas existentes.

Para crear una directiva:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en **Añadir**.

   Se abre la ventana **Seleccionar aplicación**.
3. Seleccione la aplicación para la que desea crear una directiva.
4. Haga clic en **Siguiente**.

   La ventana de propiedades de nueva directiva se abre con la pestaña **Control de aplicaciones** seleccionada.
5. Si lo desea, cambie el nombre predeterminado, el estado predeterminado y la configuración de herencia predeterminada de la directiva.
6. Seleccione la pestaña **Configuración de la aplicación**.

   O, puede hacer clic en **Guardar**. La directiva aparecerá en la lista de directivas, y podrá editar su configuración más adelante.
7. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione la categoría que desea y, en el panel de resultados de la derecha, edite la configuración de la directiva. Puede editar la configuración de directivas en cada categoría (sección).

   El conjunto de configuraciones depende de la aplicación para el que crea una directiva. Para más detalles, consulte los siguientes recursos:

   - Configuración del Servidor de administración
   - Configuración de la directiva del Agente de red
   - Documentación de Kaspersky Endpoint Security para Windows

   Para obtener detalles sobre la configuración de otras aplicaciones de seguridad, consulte la documentación de la aplicación correspondiente.

   Al editar la configuración, puede hacer clic en **Cancelar** para cancelar la última operación.
8. Haga clic en **Guardar** para guardar la directiva.

La directiva aparecerá en la lista de directivas.

Modificación de una directiva

Para modificar una directiva:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en la directiva que desea modificar.

   Se abre la ventana de configuración de directivas.
3. Especifique la configuración general y la configuración de la aplicación para la que crea una directiva. Para más detalles, consulte los siguientes recursos:

   - Configuración del Servidor de administración
   - Configuración de la directiva del Agente de red
   - Documentación de Kaspersky Endpoint Security para Windows

   Para obtener detalles sobre la configuración de otras aplicaciones de seguridad, consulte la documentación de esa aplicación.
4. Haga clic en **Guardar**.

Los cambios hechos a la directiva se guardarán en las propiedades de la directiva y aparecerán en la sección **Historial de revisión**.

Configuración general de las directivas

Control de aplicaciones

En la pestaña **Control de aplicaciones**, puede modificar el estado de la directiva y especificar la herencia de la configuración de la directiva:

- En el bloque **Estado de la directiva**, puede seleccionar uno de los modos de la directiva:
  - **Activa**

    Si se selecciona esta opción, se activa la directiva.

    Esta opción está seleccionada de forma predeterminada.
  - **Fuera de la oficina**

    Si se selecciona esta opción, la directiva se activa cuando un dispositivo sale de la red corporativa.
  - **Inactiva**

Si se selecciona esta opción, se inactiva la directiva, pero sigue almacenada en la carpeta **Directivas**. Si fuera necesario, se puede activar la directiva.

- En la sección de grupo **Herencia de configuración**, se puede configurar la herencia de directivas:
  - Heredar configuración de la directiva primaria

    Si se activa esta opción, los valores de la configuración de la directiva se heredan de la directiva de grupos de nivel superior y, por lo tanto, quedan bloqueados.

    Esta opción está activada de forma predeterminada.

  - Forzar la herencia de la configuración en las directivas secundarias

    Si se activa esta opción, después de aplicar modificaciones a las directivas, se realizarán las siguientes acciones:
    - Los valores de los parámetros de las directivas se distribuirán a las directivas de los grupos de administración anidados, es decir, a las directivas secundarias.
    - En el bloque **Herencia de configuración** de la sección **General** de la ventana de propiedades de cada directiva secundaria, se activará automáticamente la opción **Heredar configuración de la directiva primaria**.

    Si se activa esta opción, la configuración de las directivas secundarias queda bloqueada.

    Esta opción está desactivada de forma predeterminada.

Configuración de eventos

La ficha **Configuración de eventos** le permite configurar el registro de eventos y la notificación de eventos. Los eventos se distribuyen en las fichas siguientes según el nivel de importancia:

- **Crítico**

  La ficha **Crítico** no se muestra en las propiedades de la directiva del Agente de red.

- **Fallo operativo**
- **Advertencia**
- **Información**

En cada sección, la lista muestra los tipos de eventos y el plazo de almacenamiento de eventos predeterminado en el Servidor de administración (en días). Al hacer clic en un tipo de evento le permite especificar la siguiente configuración:

- **Registro de eventos**

  Puede especificar cuántos días para almacenar el evento y seleccionar dónde almacenar el evento:

  - **Exportar al sistema SIEM a través de Syslog**
  - **Almacenar en el registro de eventos del SO del dispositivo**
  - **Almacenar en el registro de eventos del SO del Servidor de administración**

- **Notificaciones de eventos**

  Puede seleccionar si desea ser notificado sobre el evento en uno de estos modos:

  - **Notificar por correo electrónico**
  - **Notificar por SMS**
  - **Notificar mediante la ejecución de un script o archivo ejecutable**
  - **Notificar por SNMP**

  De forma predeterminada, se utilizan las configuraciones de notificación especificadas en la pestaña de propiedades del Servidor de administración (como la dirección del destinatario). Si lo desea, puede cambiar esta configuración en la pestaña **Correo electrónico**, **SMS** y **Archivo ejecutable para lanzar**.

Historial de revisión

La pestaña **Historial de revisión** le permite ver la lista de revisiones de la directiva y revertir los cambios realizados en la directiva, si es necesario.

Habilitar y deshabilitar una opción de herencia de directivas

Para activar o desactivar la opción de herencia en una directiva:

1. Abra la directiva requerida.
2. Abra la pestaña **Control de aplicaciones**.
3. Active o desactive la herencia de directivas:
   - Si activa **Heredar configuración de la directiva primaria** en una directiva secundaria y un administrador bloquea alguna configuración de la directiva primaria, no podrá cambiar esa configuración en la directiva secundaria.
   - Si desactiva **Heredar configuración de la directiva primaria** en una directiva secundaria, podrá cambiar toda la configuración de la directiva secundaria, incluso si hay parámetros bloqueados en la directiva primaria.
   - Si activa **Forzar la herencia de la configuración en las directivas secundarias** en el grupo primario, se activará **Heredar configuración de la directiva primaria** para cada directiva secundaria. En este caso, no puede desactivar esta opción para ninguna directiva secundaria. Todos los parámetros de configuración bloqueados en la directiva primaria se heredan obligatoriamente en los grupos secundarios y no puede cambiarlos en esos grupos.
4. Haga clic en el botón **Guardar** para guardar los cambios o haga clic en el botón **Cancelar** para rechazar los cambios.

De manera predeterminada, la opción **Heredar configuración de la directiva primaria** está activada para las directivas nuevas.

Si una directiva tiene perfiles, todas las directivas secundarias heredan estos perfiles.

Copia de una directiva

Puede copiar directivas de un grupo de administración a otro.

Para copiar una directiva a otro grupo de administración:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Seleccione la casilla de verificación junto a la directiva (o directivas) que desea copiar.
3. Haga clic en el botón **Copiar**.

   En el lado derecho de la pantalla, aparece el árbol de los grupos de administración.
4. En el árbol, seleccione el grupo objetivo, es decir, el grupo al que desea copiar la directiva (directivas).
5. Haga clic en el botón **Copiar** al final de la pantalla.
6. Haga clic en **Aceptar** para confirmar la operación.

La directiva (directivas) se copiarán al grupo objetivo con todos sus perfiles. El estado de cada directiva copiada en el grupo objetivo será **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si ya existe una directiva con el nombre idéntico al de la directiva recién movida en el grupo objetivo, el nombre de la directiva recién movida se expande con el índice (<siguiente número secuencial>); por ejemplo: (1).

Movimiento de una directiva

Puede mover directivas de un grupo de administración a otro. Por ejemplo, desea eliminar un grupo, pero desea utilizar sus directivas para otro grupo. En este caso, le recomendamos que mueva la directiva del grupo anterior al nuevo antes de eliminar el grupo anterior.

Para mover una directiva a otro grupo de administración:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Seleccione la casilla de verificación junto a la directiva (o directivas) que desea mover.
3. Haga clic en el botón **Mover**.

   En el lado derecho de la pantalla, aparece el árbol de los grupos de administración.
4. En el árbol, seleccione el grupo de destino, es decir, el grupo al que desea mover la directiva (o directivas).
5. Haga clic en el botón **Mover** al final de la pantalla.
6. Haga clic en **Aceptar** para confirmar la operación.

Si una directiva no se hereda del grupo de origen, se mueve al grupo objetivo con todos sus perfiles. El estado de la directiva en el grupo objetivo es **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si una directiva se hereda del grupo de origen, permanece en el grupo de origen. Se copia al grupo objetivo con todos sus perfiles. El estado de la directiva en el grupo objetivo es **Inactiva**. Puede cambiar el estado a **Activa** en cualquier momento.

Si ya existe una directiva con el nombre idéntico al de la directiva recién movida en el grupo objetivo, el nombre de la directiva recién movida se expande con el índice (<siguiente número secuencial>); por ejemplo: (1).

Visualización del diagrama del estado de distribución de directivas

En Kaspersky Security Center, puede ver el estado de la aplicación de directivas en cada dispositivo en un gráfico del estado de distribución de directivas.

Para ver el estado de distribución de directivas en cada dispositivo:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Seleccione la casilla de verificación junto al nombre de la directiva cuyo estado de distribución en los dispositivos desea ver.
3. En el menú que aparece, seleccione el enlace **Distribución**.

   Se abre la ventana **Resultados de la distribución de <nombre de la directiva>**.
4. En la ventana **Resultados de la distribución de <nombre de la directiva>** que se abre, se muestra la **Descripción del estado** de la directiva.

Puede cambiar el número de resultados que se muestran en la lista con la distribución de directivas. El número predeterminado de eventos es de 100.000.

Para cambiar la cantidad de dispositivos que se muestran en la lista de resultados de la distribución de directivas:

1. En el menú principal, vaya a la sección **Opciones de interfaz** en la barra de herramientas.
2. En el **Límite de dispositivos que se muestran en los resultados de distribución de directivas**, ingrese la cantidad de dispositivos (hasta 100.000).

   El número de puerto predeterminado es 5000.
3. Haga clic en **Guardar**.

   Sus cambios quedan guardados y aplicados.

Activación automática de una directiva en el evento Brote de virus

Para que una directiva realice la activación automática en el evento Brote de virus:

1. En la parte superior de la pantalla, haga clic en el icono de la **Configuración** ( ) al lado del nombre del Servidor de administración requerido.

   Se abrirá la ventana de propiedades del Servidor de administración, con la pestaña **General** seleccionada.
2. Seleccione la sección de **Brote de virus**.
3. En el panel derecho, haga clic en el enlace **Configurar directivas para activar cuando se produce un evento de brote de virus**.

Se abre la ventana **Activación de directiva**.

4. En la sección relativa al componente que detecta un Brote de virus — Antivirus para estaciones de trabajo y servidores de archivos, Antivirus para servidores de correo o Antivirus para la protección del perímetro — seleccione la opción junto a la entrada que desea y, a continuación, haga clic en **Añadir**.

   Se abrirá una ventana con el grupo de administración **Dispositivos administrados**.

5. Haga clic en el icono de flecha (>) al lado de **Dispositivos administrados**.

   Se muestra una jerarquía de grupos de administración y sus directivas.

6. En la jerarquía de los grupos de administración y sus directivas, haga clic en el nombre de una directiva o directivas que se activan cuando se detecta un Brote de virus.

   Para seleccionar todas las directivas en la lista o en un grupo, marque la casilla junto al nombre que desee.

7. Haga clic en el botón **Guardar**.

   La ventana con la jerarquía de grupos de administración y sus directivas está cerrada.

Las directivas seleccionadas se agregan a la lista de directivas que se activan cuando se detecta un Brote de virus. Las directivas seleccionadas se activan cuando se detecta un Brote de virus, independientemente de si están activas o inactivas.

Si se activa una directiva en el evento Brote de virus, la única forma de volver a la directiva anterior es mediante el modo manual.

Eliminación de una directiva

Puede eliminar una directiva si ya no la necesita. Solo puede eliminar una directiva que no se herede en el grupo de administración especificado. Si se hereda una directiva, solo puede eliminarla en el grupo de nivel superior para el que se creó.

Para eliminar una directiva:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.

2. Seleccione la casilla de verificación junto a la directiva que desea eliminar y haga clic en **Eliminar**.

   El botón **Eliminar** no estará disponible (atenuado) si selecciona una directiva heredada.

3. Haga clic en **Aceptar** para confirmar la operación.

La directiva se elimina junto con todos sus perfiles.

Administración de perfiles de directivas

Esta sección describe la gestión de perfiles de directivas y proporciona información sobre cómo ver los perfiles de una directiva, cambiar la prioridad de un perfil de directiva, crear un perfil de directiva, modificar un perfil de directiva, copiar un perfil de directiva, crear una regla de activación de perfil de directiva y eliminar un perfil de directiva.

Visualización de perfiles de directiva

Ver perfiles de una directiva:

1. En el menú principal, vaya a **DISPOSITIVOS** → **DIRECTIVAS Y PERFILES**.
2. Haga clic en el nombre de la directiva cuyos perfiles desea ver.

   La ventana de propiedades de la directiva se abre con la pestaña **Control de aplicaciones** seleccionada.
3. Abra la pestaña **Perfiles de directiva**.

Aparece la lista de perfiles de directiva en formato tabular. Si la directiva no tiene perfiles, la tabla aparecerá vacía.

Cambiar una prioridad de perfil de directiva

Para cambiar una prioridad de perfil de directiva:

1. Vaya la lista de los perfiles de una directiva que desee.

   Aparece la lista de perfiles de directiva.
2. En la pestaña **Perfiles de directiva**, seleccione la casilla de verificación al lado del perfil de la directiva para el que desea cambiar la prioridad.
3. Establezca una nueva posición del perfil de directivas en la lista haciendo clic en **Priorizar** o **Despriorizar**.

   Cuanto mayor sea el perfil de una directiva en la lista, mayor será su prioridad.
4. Haga clic en el botón **Guardar**.

La prioridad del perfil de directivas seleccionado se cambia y se aplica.

Crear perfil de directiva

Puede crear perfiles de directivas para una directiva.

Crear perfil de directiva:

1. Vaya la lista de los perfiles de la directiva que desee.

   Aparece la lista de perfiles de directiva. Si la directiva no tiene perfiles, aparecerá una tabla vacía.
2. Haga clic en **Añadir**.
3. Si lo desea, cambie el nombre predeterminado y la configuración de herencia predeterminada del perfil.
4. Seleccione la pestaña **Configuración de la aplicación**.

   O, puede hacer clic en **Guardar**. El perfil que ha creado aparecerá en la lista de perfiles de directivas y podrá editar su configuración más adelante.

5. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione la categoría que desea y, en el panel de resultados de la derecha, edite la configuración del perfil. Puede editar la configuración del perfil de directiva en cada categoría (sección).

   Al editar la configuración, puede hacer clic en **Cancelar** para cancelar la última operación.

6. Haga clic en **Guardar** para guardar el perfil.

El perfil aparecerá en la lista de perfiles de directivas.

Modificación de un perfil de directiva

La capacidad de editar un perfil de directiva solo está disponible para las directivas de Kaspersky Endpoint Security para Windows.

Para modificar un perfil de directiva, siga estos pasos:

1. Vaya la lista de los perfiles de una directiva que desee.

   Aparece la lista de perfiles de directiva.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de directiva que desea modificar.

   Se abre la ventana de propiedades de perfiles de directiva.

3. Configure el perfil en la ventana de propiedades:

   - Si es necesario, en la pestaña **Control de aplicaciones**, cambie el nombre del perfil y habilite o deshabilite el perfil.
   - Editar las reglas de activación del perfil.
   - Editar la configuración de la aplicación.

     Para obtener detalles sobre la configuración de las aplicaciones de seguridad, consulte la documentación de la aplicación correspondiente.

4. Haga clic en **Guardar**.

La configuración que ha modificado se aplicará después de que el dispositivo se sincronice con el Servidor de administración (si el perfil de directiva está activo) o cuando se active una regla de activación (si el perfil de directiva no está activo).

Copiar perfil de directiva

Puede copiar un perfil de directiva en la directiva actual o en otra, por ejemplo, si desea tener perfiles idénticos para directivas diferentes. También puede usar la copia si desea tener dos o más perfiles que se diferencien solo en un pequeño número de configuraciones.

Para copiar un perfil de directiva:

1. Vaya la lista de los perfiles de una directiva que desee.

Aparece la lista de perfiles de directiva. Si la directiva no tiene perfiles, aparecerá una tabla vacía.

2. En la pestaña **Perfiles de directiva**, seleccione el perfil de la directiva que desea copiar.
3. Haga clic en **Copiar**.
4. En la ventana que se abre, seleccione la directiva en la que desea copiar el perfil.

   Puede copiar un perfil de directiva en la misma directiva o en una directiva que especifique.
5. Haga clic en **Copiar**.

El perfil de la directiva se copia en la directiva que seleccionó. El perfil recién copiado obtiene la prioridad más baja. Si copia el perfil a la misma directiva, el nombre del perfil recién copiado se ampliará con el índice (), por ejemplo: (1), (2).

Más adelante, puede cambiar la configuración del perfil, incluyendo su nombre y su prioridad; el perfil de la directiva original no se cambiará en este caso.

Creación de una regla de activación de perfil de directiva

Para crear una regla de activación de perfil de directiva:

1. Vaya la lista de los perfiles de una directiva que desee.

   Aparece la lista de perfiles de directiva.
2. En la pestaña **Perfiles de directiva**, haga clic en el perfil de la directiva para el que tiene que crear una regla de activación.

   Si la lista de perfiles de directiva está vacía, puede crear un perfil de directiva.
3. En la pestaña **Reglas de activación**, haga clic en el botón **Añadir**.

   Se abrirá la ventana con las reglas de activación del perfil de la directiva.
4. Especifique un nombre para la regla.
5. Seleccione las casillas al lado de las condiciones que deben afectar a la activación del perfil de la directiva que está creando:

   - **Reglas generales de activación de perfiles de directivas**

     Seleccione esta casilla para configurar reglas de activación de perfiles de directiva del dispositivo según el estado del modo desconectado del dispositivo, la regla para la conexión con el Servidor de administración y las etiquetas asignadas al dispositivo.

     Para esta opción, especifique en el paso siguiente:

     - **Estado del dispositivo**

Define la condición de la presencia del dispositivo en la red:

- **En línea**: El dispositivo está en la red, lo que significa que el Servidor de administración está disponible.
- **Desconectado**: El dispositivo está en una red externa, lo que significa que el Servidor de administración no está disponible.
- **N/D**: No se aplica el criterio.

- La regla de conexión con el Servidor de administración está activa en este dispositivo

  Elija la condición de activación del perfil de directiva (si la regla se ejecuta o no) y seleccione el nombre de la regla.

  La regla define la localización de la red del dispositivo para la conexión con el Servidor de administración, cuyas condiciones se deben cumplir (o no se debe cumplir) para la activación del perfil de la directiva.

  Se puede crear o configurarse una descripción de la ubicación de la red de dispositivos para la conexión con un Servidor de administración en una regla de conmutación de Agente de red.

- **Reglas para un propietario del dispositivo específico**

  Para esta opción, especifique en el paso siguiente:

  - Propietario del dispositivo

    Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según su propietario. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

    - El dispositivo pertenece al propietario especificado (símbolo "=").
    - El dispositivo no pertenece al propietario especificado (símbolo "#").

      Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar el propietario del dispositivo cuando la opción está activada. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

  - El propietario del dispositivo está incluido en un grupo de seguridad interno

    Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según la pertenencia del propietario del dispositivo a un grupo interno de seguridad de Kaspersky Security Center. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

    - El propietario del dispositivo es un miembro del grupo de seguridad especificado (símbolo "=").
    - El propietario del dispositivo no es un miembro del grupo de seguridad especificado (símbolo "#").

      Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar un grupo de seguridad de Kaspersky Security Center. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

- **Reglas para especificaciones de hardware**

  Seleccione esta casilla para configurar reglas de activación del perfil de la directiva en el dispositivo según el volumen de memoria y el número de procesadores lógicos.

  Para esta opción, especifique en el paso siguiente:

  - **Tamaño de RAM, en MB**

    Active esta opción para configurar y activar la regla de activación de perfil en el dispositivo según el volumen de RAM disponible en ese dispositivo. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

    - El tamaño de la RAM del dispositivo es menor que el valor especificado (signo "<").
    - El tamaño de la RAM del dispositivo es mayor que el valor especificado (signo ">").

    Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar el volumen de RAM en el dispositivo. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

  - **Número de procesadores lógicos**

    Active esta opción de verificación para configurar y activar la regla de activación de perfil en el dispositivo según el número de procesadores lógicos de dicho dispositivo. En la lista desplegable de la casilla de verificación, puede seleccionar un criterio para la activación de perfil:

    - El número de procesadores lógicos en el dispositivo es menor o igual que el valor especificado (signo "<").
    - El número de procesadores lógicos en el dispositivo es mayor o igual que el valor especificado (signo ">").

    Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado. Puede especificar la cantidad de procesadores lógicos en el dispositivo. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

- **Reglas para la asignación de funciones**

  Para esta opción, especifique en el paso siguiente:

  Activar perfil de directiva según la función específica del propietario del dispositivo

  Seleccione esta opción para configurar y activar la regla de activación de perfil en el dispositivo según la función del propietario. Añada la función de manera manual desde la lista de funciones existentes.

  Si esta opción está activada, el perfil se activa en el dispositivo conforme al criterio configurado.

- **Reglas para el uso de etiquetas**

  Seleccione esta casilla para configurar reglas para la activación del perfil de la directiva en el dispositivo según las etiquetas asignadas al dispositivo. Puede activar el perfil de directiva tanto para los dispositivos que tienen las etiquetas seleccionadas, como para las que no las tienen.

  Para esta opción, especifique en el paso siguiente:

- **Etiqueta**

  En la lista de etiquetas, puede especificar la regla para incluir dispositivos en el perfil de la directiva seleccionando las casillas junto a las etiquetas correspondientes.

  Puede añadir nuevas etiquetas a la lista al introducirlas en el campo sobre la lista y hacer clic en el botón **Añadir**.

  El perfil de la directiva incluye los dispositivos con descripciones que contienen todas las etiquetas seleccionadas. El criterio no se aplica si las casillas están vacías. De forma predeterminada, estas casillas están en blanco.

- **Aplicar a los dispositivos que no tengan etiquetas especificadas**

  Active esta opción si tiene que cambiar su selección de etiquetas.

  Si se selecciona esta opción, el perfil de la directiva incluirá los dispositivos con descripciones que no contengan ninguna de las etiquetas seleccionadas. Si esta opción está desactivada, el software no se actualiza.

  Esta opción está desactivada de forma predeterminada.

- **Reglas para el uso de Active Directory**

  Seleccione esta casilla para configurar reglas de activación de un perfil de directiva en el dispositivo según la presencia del dispositivo en una unidad organizativa de Active Directory, o la pertenencia del dispositivo (o su propietario) a un grupo de seguridad de Active Directory.

  Para esta opción, especifique en el paso siguiente:

  - **Pertenencia del propietario del dispositivo en el grupo de seguridad de Active Directory**

    Si se selecciona esta opción, el perfil de directiva se activa en el dispositivo cuyo propietario pertenece al grupo de seguridad especificado. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

  - **Pertenencia del dispositivo al grupo de seguridad de Active Directory**

    Si se selecciona esta opción, el perfil de directiva se activa en el dispositivo. Si esta opción está desactivada, el criterio de activación del perfil no se aplica. Esta opción está desactivada de forma predeterminada.

  - **Asignación de dispositivos en la unidad organizativa de Active Directory**

    Si se selecciona esta opción, se activa el perfil de directiva en el dispositivo, que se incluye en la unidad organizativa de Active Directory especificada. Si esta opción está desactivada, el criterio de activación del perfil no se aplica.

    Esta opción está desactivada de forma predeterminada.

El número de páginas adicionales del Asistente depende de la configuración que seleccione en el primer paso. Puede modificar las reglas de activación de perfil de la directiva más adelante.

6. Compruebe la lista de los parámetros configurados. Si la lista es correcta, haga clic en **Crear**.

El perfil se guardará. El perfil se activará en el dispositivo cuando se activen las reglas de activación.

Las reglas de activación del perfil de directiva creadas para el perfil se muestran en las propiedades del perfil de directiva en la pestaña **Reglas de activación**. Puede modificar o eliminar cualquier regla de activación de perfil de directiva.

Se pueden activar simultáneamente varias reglas de activación.

Eliminar perfil de directiva

Para eliminar el perfil de directiva:

1. Vaya la lista de los perfiles de una directiva que desee.

   Aparece la lista de perfiles de directiva.

2. En la pestaña **Perfiles de directiva**, seleccione la casilla de verificación al lado del perfil de directiva que desee eliminar y hacer clic en **Eliminar**.

3. En la ventana que se abre, haga clic de nuevo en **Eliminar**.

   El perfil de directiva será eliminado. Si la directiva es heredada por un grupo de nivel inferior, el perfil permanece en ese grupo pero se convierte en el perfil de la directiva de ese grupo. Esto se hace para eliminar un cambio significativo en la configuración de las aplicaciones administradas instaladas en los dispositivos de grupos de nivel inferior.

Protección y cifrado de datos

El cifrado de datos reduce el riesgo de pérdida involuntaria de datos en caso de que le roben o pierda su ordenador portátil o su disco duro, o en caso de que usuarios no autorizados y aplicaciones accedan a ellos.

Las siguientes aplicaciones Kaspersky admiten el cifrado:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security para Mac

Puede mostrar u ocultar algunos de los elementos de la interfaz relacionados con la función de administración de cifrado mediante la configuración de la interfaz de usuario.

Cifrado de datos en Kaspersky Endpoint Security para Windows

Puede administrar el cifrado de BitLocker en dispositivos administrados a través de Kaspersky Endpoint Security para Windows de la siguiente manera: active o desactive el cifrado, vea la lista de dispositivos cifrados, genere y vea informes sobre cifrado.

El cifrado se configura al definir las directivas de Kaspersky Endpoint Security para Windows en Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security para Windows realiza el cifrado y descifrado de acuerdo con la directiva activa. Si desea obtener instrucciones detalladas sobre cómo configurar reglas, así como una descripción de las funciones de cifrado, consulte la *Ayuda en línea de Kaspersky Endpoint Security para Windows*.

Cifrado de datos en Kaspersky Endpoint Security para Mac

Puede utilizar el cifrado FileVault en dispositivos que ejecutan macOS. Al trabajar con Kaspersky Endpoint Security para Mac, puede habilitar o deshabilitar este cifrado.

El cifrado se configura al definir las directivas de Kaspersky Endpoint Security para Mac en Kaspersky Security Center Cloud Console. Kaspersky Endpoint Security para Mac realiza el cifrado y descifrado de acuerdo con la directiva activa. Para obtener información detallada sobre las funciones de cifrado, consulte la *Ayuda en línea de Kaspersky Endpoint Security para Mac*.

Visualización de la lista de dispositivos cifrados

Los elementos de la interfaz relacionados con la función de administración de cifrado se muestran u ocultan según la configuración de la interfaz de usuario.

Para visualizar la lista de dispositivos cifrados:

Seleccione **OPERACIONES** → **PROTECCIÓN Y CIFRADO DE DATOS** y, en la lista desplegable, seleccione **DISPOSITIVOS CIFRADOS**.

Aparece una lista de dispositivos cifrados.

La ventana de trabajo muestra información acerca de las unidades cifradas, así como acerca de dispositivos cifrados en el nivel de la unidad. Una vez que se descifre la información de una unidad, la unidad se elimina automáticamente de la lista.

Puede exportar la lista de dispositivos cifrados a un archivo CSV o TXT.

Visualización de la lista de eventos de cifrado

Al ejecutar tareas de cifrado y descifrado de datos en los dispositivos cliente, Kaspersky Endpoint Security para Windows envía a Kaspersky Security Center información sobre los siguientes tipos de eventos:

- No se puede cifrar o descifrar un archivo, o crear un archivo cifrado debido a que falta espacio en disco.
- No se puede cifrar o descifrar un archivo, o crear un archivo cifrado debido a problemas de licencia.
- No se puede cifrar o descifrar un archivo, o crear un archivo cifrado debido a que faltan derechos de acceso.
- Se ha prohibido el acceso de la aplicación a un archivo cifrado.
- Errores desconocidos.

Los elementos de la interfaz relacionados con la función de administración de cifrado se muestran u ocultan según la configuración de la interfaz de usuario.

Para ver una lista de eventos que se han producido al cifrar datos en dispositivos:

Seleccione **OPERACIONES** → **PROTECCIÓN Y CIFRADO DE DATOS** y, en la lista desplegable, seleccione **EVENTOS DE CIFRADO**.

Aparece una lista de eventos de cifrado.

La ventana muestra información acerca de los problemas que se han producido al cifrar datos en dispositivos.

Puede exportar la lista de dispositivos cifrados a un archivo CSV o TXT.

Creación y visualización de informes sobre el cifrado

Puede generar los siguientes informes:

- Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo. Este informe contiene información sobre el estado de cifrado del dispositivo para todos los grupos de dispositivos.
- Informe sobre los derechos de acceso a dispositivos cifrados. Este informe contiene información sobre el estado de las cuentas de usuario a las que se ha otorgado acceso a los dispositivos cifrados.
- Informe sobre errores en el cifrado de archivos. Este informe contiene información sobre errores que han ocurrido durante tareas de cifrado o descifrado de datos en dispositivos.
- Informe sobre el bloqueo del acceso a archivos cifrados. Este informe contiene información sobre el bloqueo del acceso de la aplicación a archivos encriptados.

Puede generar cualquier informe en la sección **INFORMES** (**SUPERVISIÓN E INFORMES** → **INFORMES**). Alternativamente, puede generar algunos de los informes de cifrado en las secciones **DISPOSITIVOS CIFRADOS** y **EVENTOS DE CIFRADO**.

Para generar informes de cifrado en la sección DISPOSITIVOS CIFRADOS:

1. Asegúrese de habilitar la opción **Mostrar protección y cifrado de datos** en las opciones de interfaz.
2. Seleccione **OPERACIONES** → **PROTECCIÓN Y CIFRADO DE DATOS** y, en la lista desplegable, seleccione **DISPOSITIVOS CIFRADOS**.
3. Para generar un informe de cifrado, haga clic en el nombre del informe que desea generar:
   - **Informe sobre el estado del cifrado de los dispositivos de almacenamiento masivo**
   - **Informe sobre los derechos de acceso a dispositivos cifrados**

   Se inicia la generación de informes.

Para generar el informe sobre errores en el cifrado en la sección EVENTOS DE CIFRADO:

1. Asegúrese de habilitar la opción **Mostrar protección y cifrado de datos** en las opciones de interfaz.
2. Seleccione **OPERACIONES → PROTECCIÓN Y CIFRADO DE DATOS** y, en la lista desplegable, seleccione **EVENTOS DE CIFRADO**.
3. Para generar el informe de cifrado, haga clic en el enlace **Informe sobre errores en el cifrado de archivos**.

Se inicia la generación de informes.

Conceder acceso a una unidad cifrada en modo desconectado

Un usuario puede solicitar acceso a un dispositivo cifrado, por ejemplo, cuando Kaspersky Endpoint Security para Windows no está instalado en el dispositivo administrado. Después de recibir la solicitud, puede crear un archivo de clave de acceso y enviárselo al usuario. Todos los casos de uso y las instrucciones detalladas se proporcionan en la documentación de Kaspersky Endpoint Security para Windows.

Para conceder acceso a una unidad cifrada en modo desconectado, haga lo siguiente:

1. Seleccione **OPERACIONES → PROTECCIÓN Y CIFRADO DE DATOS** y, en la lista desplegable, seleccione **DISPOSITIVOS CIFRADOS**.

   Aparece una lista de dispositivos cifrados.
2. Seleccione la unidad para la cual el usuario solicitó acceso.
3. Haga clic en el botón **Conceder acceso al dispositivo en modo desconectado**.
4. En la ventana que se abre, seleccione el complemento correspondiente a la aplicación de Kaspersky que se utilizó para cifrar la unidad seleccionada.

   > Si una unidad está cifrada con una aplicación de Kaspersky que no es compatible con Kaspersky Security Center 14 Web Console, utilice la Consola de administración basada en Microsoft Management Console para conceder el acceso desconectado.
5. Siga las instrucciones proporcionadas en la documentación de Kaspersky Endpoint Security para Windows.

El usuario puede usar el archivo recibido para acceder a la unidad cifrada y leer los datos almacenados en la unidad.

Usuarios y funciones de usuario

Esta sección describe los usuarios y las funciones de usuarios, y proporciona instrucciones para crearlos y modificarlos, para asignar funciones y grupos a los usuarios y para asociar los perfiles de directivas con las funciones.

Acerca de las funciones de usuario

Una *función de usuario* (también denominada *función*) es un objeto que contiene un conjunto de derechos y privilegios. Se puede asociar una función con la configuración de las aplicaciones de Kaspersky instaladas en un dispositivo de usuario. Puede asignar una función a un conjunto de usuarios o a un conjunto de grupos de seguridad en cualquier nivel en la jerarquía de grupos de administración.

Puede asociar funciones de usuario con perfiles de directiva. Si a un usuario se le asigna una función, este usuario obtiene la configuración de seguridad necesaria para realizar funciones de trabajo.

Una función de usuario se puede asociar con usuarios de dispositivos en un grupo de administración específico.

Cobertura de la función de usuario

Una *cobertura de la función de usuario* es una combinación de usuarios y grupos de administración. La configuración asociada con una función de usuario se aplica solo a los dispositivos que pertenecen a usuarios que tienen esta función y solo si estos dispositivos pertenecen a grupos asociados con esta función, incluidos los grupos secundarios.

Ventajas de utilizar funciones

Una ventaja de usar roles es que no tiene que especificar la configuración de seguridad para cada uno de los dispositivos administrados o para cada uno de los usuarios por separado. La cantidad de usuarios y dispositivos en una empresa puede ser bastante grande, pero la cantidad de funciones de trabajo diferentes que requieren configuraciones de seguridad diferentes es considerablemente menor.

Diferencias de utilizar perfiles de directivas

Los perfiles de directivas son propiedades de una directiva que se crea para cada aplicación de Kaspersky por separado. Una función está asociada con muchos perfiles de directivas creados para aplicaciones diferentes. Por lo tanto, una función es un método de unir configuraciones para un determinado tipo de usuario en un solo lugar.

Configuración de los derechos de acceso a las funciones de la aplicación. Control de acceso basado en funciones

Kaspersky Security Center proporciona recursos para el acceso basado en funciones a las funciones de Kaspersky Security Center o las aplicaciones administradas de Kaspersky.

Puede configurar los derechos de acceso a las funciones de la aplicación para los usuarios de Kaspersky Security Center de una de las siguientes formas:

- Mediante la configuración por separado de los derechos de cada usuario o grupo de usuarios.
- Mediante la creación de funciones de usuario estándar con un conjunto de derechos preestablecido y la asignación de esas funciones a los usuarios según su ámbito de responsabilidad.

La aplicación de funciones de usuario tiene como objetivo simplificar y acortar los procedimientos de rutina para configurar los derechos de acceso de los usuarios a las funciones de la aplicación. Los derechos de acceso de una función se configuran según las tareas estándares y el ámbito de las responsabilidades de los usuarios.

A las funciones de usuario se les puede asignar nombres que se correspondan con sus respectivos propósitos. Puede crear un número ilimitado de funciones en la aplicación.

Puede utilizar las funciones de usuario predefinidas con un conjunto de derechos ya configurado, o crear nuevas funciones y configurar los derechos necesarios usted mismo.

Derechos de acceso a las funciones de la aplicación

La siguiente tabla muestra las funciones de Kaspersky Security Center con los derechos de acceso para administrar las tareas, informes y configuraciones asociados y realizar las acciones de usuario asociadas.

Para realizar las acciones de usuario enumeradas en la tabla, un usuario debe tener el derecho especificado junto a la acción.

Los derechos de **lectura**, **modificación** y **ejecución** pueden aplicarse a cualquier tarea, informe o configuración. Además de estos derechos, el usuario debe tener el derecho de **Realizar operaciones en selecciones de dispositivos** para administrar tareas, informes o configuraciones en selecciones de dispositivos.

Todas las tareas, informes, configuraciones y paquetes de instalación que faltan en la tabla pertenecen al área funcional **Características generales: funcionalidad básica**.

Derechos de acceso a las funciones de la aplicación

Área funcional	Derecho	Acción del usuario: derecho necesario para realizar la acción	Tarea	Informe
Características generales: **Gestión de grupos de administración**	**Modificación**	• Añadir dispositivos a un grupo de administración: **Modificación** • Eliminar dispositivos de un grupo de administración: **Modificación** • Agregar un grupo de administración a otro grupo de administración: **Modificación** • Eliminar un grupo de administración de otro grupo de administración: **Modificación**	Ninguno	Ninguno
Características generales: **Acceder a objetos independientemente de sus ACL**	**Lectura**	Obtener acceso de lectura a todos los objetos: **Leer**	Ninguno	Ninguno
Características generales: **Funcionalidad básica**	• **Lectura** • **Modificación**	• Reglas de movimiento de dispositivos (crear,	• "Descargar actualizaciones en el repositorio	• "Informe del estado de la protección"

	• **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	modificar o eliminar) para el Servidor virtual: **Modificación**, **realizar operaciones en selecciones de dispositivos** • Obtener certificado personalizado del protocolo móvil (LWNGT): **Lectura** • Establecer certificado personalizado del protocolo móvil (LWNGT): **Escritura** • Obtener lista de redes definidas por NLA: **Lectura** • Añadir, modificar o eliminar una lista de redes definida por NLA: **Modificación** • Ver lista de control de acceso de grupos: **Lectura** • Ver el registro de eventos de Kaspersky: **Lectura**	del Servidor de administración" • "Entregar informes" • "Distribuir paquetes de instalación" • "Instalar una aplicación de forma remota en Servidores de administración secundarios"	• "Informe de amenazas" • "Informe sobr los dispositivo más infectad • "Informe sobr el estado de l bases de dat antivirus" • "Informe de errores" • "Informe sobr ataques a la r • "Informe resumido sob las aplicacion de protecció del sistema d correo instaladas" • "Informe resumido sob las aplicacion de defensa perimetral instaladas" • "Informe resumido sob los tipos de aplicaciones instalados" • "Informe sobr usuarios de dispositivos infectados" • "Informe sobr incidentes" • "Informe sobr eventos" • "Informe sobr la actividad d los puntos de distribución" • "Informe sobr Servidores d

				administración secundarios" • "Informe sobre eventos de control de dispositivos" • "Informe de vulnerabilidad • "Informe sobre aplicaciones prohibidas" • "Informe de Control web" • "Informe sobre el estado del cifrado de los dispositivos administrados • "Informe sobre el estado del cifrado de los dispositivos d almacenamien masivo" • "Informe sobre errores en el cifrado de archivos" • "Informe sobre el bloqueo del acceso a archivos cifrados" • "Informe sobre los derechos d acceso a dispositivos cifrados" • "Informe sobre permisos de usuario vigentes" • "Informe sobre derechos"
Características	• **Lectura**	• Ver objetos	Ninguno	Ninguno

generales: **Objetos eliminados**	• **Modificación**	eliminados en la Papelera de reciclaje: **Lectura** • Eliminar objetos de la Papelera de reciclaje: **Modificación**		
Características generales: **Procesamiento de eventos**	• **Eliminación de eventos** • **Edición de la configuración de notificación de eventos** • **Edición de la configuración del registro de eventos** • **Modificación**	• Cambiar la configuración del registro de eventos: **Edición de la configuración del registro de eventos** • Cambiar la configuración de notificación de eventos: **Edición de la configuración de notificación de eventos** • Eliminar eventos: **Eliminación de eventos**	Ninguno	Ninguno
Características generales: **Operaciones en el Servidor de administración**	• **Lectura** • **Modificación** • **Ejecución** • **Modificación de las LCA de objetos**	• Especificar puertos del Servidor de administración para la conexión del Agente de red: **Modificación** • Especificar los puertos del Proxy de activación que se está ejecutando en	• "Copia de seguridad de los datos del Servidor de administración" • "Mantenimiento de bases de datos"	Ninguno

	• **Realizar operaciones en selecciones de dispositivos**	el Servidor de administración: **Modificación** • Especificar los puertos del Proxy de activación de dispositivos móviles que se está ejecutando en el Servidor de administración: **Modificación** • Especificar los puertos del Servidor web para la distribución de paquetes independientes: **Modificación** • Especificar los puertos del Servidor web para la distribución de perfiles MDM: **Modificación** • Especificar los puertos SSL del Servidor de administración para la conexión a través de Kaspersky Security Center Web Console: **Modificación** • Especificar puertos del Servidor de administración para conexión de dispositivos móviles: **Modificación** • Especificar el número máximo de eventos que pueden almacenar en la base de datos del Servidor de administración: **Modificación** • Especificar el número máximo de eventos que el Servidor de		

		administración puede enviar: **Modificación** • Especificar el periodo de tiempo durante el cual el Servidor de administración puede enviar eventos: **Modificación**		
Funciones generales: **despliegue del software de Kaspersky**	• **Administración de parches de Kaspersky** • **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	Aprobar o rechazar la instalación del parche: **Administración de parches de Kaspersky**	Ninguno	• "Informe sobre el uso de clave de licencia por parte del Servidor de administración virtual" • "Informe de versiones de software de Kaspersky" • "Informe de aplicaciones incompatibles" • "Informe sobre las versiones de las actualizaciones del módulo de software de Kaspersky" • "Informe del despliegue de protección"
Características generales: Administración de claves	• **Exportar archivo clave** • **Modificación**	• Exportar archivo clave: **Exportar archivo clave** • Modificar la configuración de la clave de licencia del Servidor de administración: **Modificación**	Ninguno	Ninguno
Características generales:	• **Lectura**	• Crear informes independientemente	Ninguno	Ninguno

Administración de informes	• **Modificación**	de sus ACL: **Escritura** • Ejecutar informes independientemente de sus ACL: **Lectura**		
Funciones generales: **Jerarquía de Servidores de administración**	**Configuración de jerarquía de Servidores de administración**	Registrar, actualizar o eliminar Servidores de administración secundarios: **Configuración de la jerarquía del Servidor de administración**	Ninguno	Ninguno
Características generales: **Permisos de usuario**	**Modificación de las LCA de objetos**	• Cambiar las propiedades de "seguridad" de cualquier objeto: **Modificación de las LCA de objetos** • Administrar roles de usuario: **Modificación de las LCA de objetos** • Administrar usuarios internos: **Modificación de las LCA de objetos** • Administrar grupos de seguridad: **Modificación de las LCA de objetos** • Administrar alias: **Modificación de las LCA de objetos**	Ninguno	Ninguno
Características generales: **Servidores de administración virtuales**	• **Administración de Servidores de administración virtuales** • **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones**	• Obtener lista de Servidores de administración: **Lectura** • Obtener información sobre el Servidor de administración virtual: **Lectura** • Crear, actualizar o eliminar un Servidor de administración virtual: **Administración de Servidores de**	Ninguno	"Informe sobre lo resultados de la instalación de actualizaciones d software de terceros"

	en selecciones de dispositivos	**administración virtuales** • Mover un Servidor de administración virtual a otro grupo: **Administración de Servidores de administración virtuales** • Establecer permisos de Servidor virtual de administración: **Administración de Servidores de administración virtuales**		
Administración de dispositivos móviles: **General**	• **Conectar nuevos dispositivos** • **Enviar solo comandos de información a dispositivos móviles** • **Enviar comandos a dispositivos móviles** • **Administración de certificados** • **Lectura** • **Modificación**	• Obtener datos de restauración del Servicio de administración de claves: **Leer** • Eliminar certificados de usuario: **Administración de certificados** • Obtener la parte pública del certificado de usuario: **Lectura** • Comprobar si la infraestructura de clave pública está activada: **Lectura** • Comprobar la cuenta de infraestructura de clave pública: **Lectura** • Obtener plantillas de infraestructura de clave pública: **Lectura** • Obtener plantillas de infraestructura de clave pública mediante certificado de uso	Ninguno	Ninguno

		extendido de clave: **Lectura** • Comprobar si el certificado de infraestructura de clave pública está revocado: **Lectura** • Actualizar la configuración de emisión de certificados de usuario: **Administración de certificados** • Obtener la configuración de emisión del certificado de usuario: **Lectura** • Obtener paquetes por nombre de aplicación y versión: **Lectura** • Establecer o cancelar el certificado de usuario: **Administración de certificados** • Renovar certificado de usuario: **Administración de certificados** • Establecer etiqueta de certificado de usuario: **Administración de certificados** • Ejecutar la generación del paquete de instalación de MDM; cancelar la generación del paquete de instalación de MDM: **Conexión de nuevos dispositivos**		
Administración del	• **Iniciar**	• Crear sesión para	Ninguno	"Informe sobre

sistema: **Conectividad**	**sesiones de RDP** • **Conectarse a sesiones de RDP existentes** • **Iniciar tunelización** • **Guardar archivos de dispositivos en la estación de trabajo del administrador** • **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	compartir escritorio: **Derecho a crear una sesión para compartir escritorio** • Crear sesión RDP: **Conectarse a sesiones RDP existentes** • Crear túnel: **Iniciar tunelización** • Guardar lista de contenido de red: **Guardar archivos de dispositivos en la estación de trabajo del administrador**		usuarios de dispositivos"
Administración del sistema: **Inventario de hardware**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Obtener o exportar objeto de inventario de hardware: **Lectura** • Añadir, establecer o eliminar objeto de inventario de hardware: **Escritura**	Ninguno	• "Informe sobr el registro de hardware" • "Informe sobr cambios de configuración • "Informe sobr hardware"
Administración del sistema: **Control de acceso a la red**	• **Lectura** • **Modificación**	• Ver la configuración de CISCO: **Lectura** • Cambiar la configuración de CISCO: **Escritura**	Ninguno	Ninguno
Administración del sistema: **Despliegue del sistema operativo**	• **Desplegar servidores PXE** • **Lectura** • **Modificación**	• Desplegar servidores PXE: **Desplegar servidores PXE** • Ver una lista de servidores PXE:	"Crear paquete de instalación basado en la imagen del sistema operativo del dispositivo de referencia"	Ninguno

	• **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	**Lectura** • Iniciar o detener el proceso de instalación en clientes PXE: **Ejecución** • Administrar controladores para WinPE y las imágenes del sistema operativo: **Modificación**		
Administración del sistema: **Administración de vulnerabilidades y parches**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Ver propiedades de parches de terceros: **Lectura** • Cambiar las propiedades del parche de terceros: **Modificación**	• "Realizar la sincronización de Windows Update" • "Instalar actualizaciones de Windows Update" • "Reparar vulnerabilidades" • "Instalar las actualizaciones necesarias y corregir vulnerabilidades"	"Informe de actualizaciones d software"
Administración del sistema: **Instalación remota**	• **Lectura** • **Modificación** • **Ejecución** • **Realizar operaciones en selecciones de dispositivos**	• Consulte las propiedades del paquete de instalación basado en Administración de vulnerabilidades y parches de terceros: **Leer** • Cambiar las propiedades del paquete de instalación basado en Administración de vulnerabilidades y parches de terceros: **Modificar**	Ninguno	Ninguno
Administración del sistema: **Inventario de software**	• **Lectura** • **Modificación**	Ninguno	Ninguno	• "Informe sobr aplicaciones instaladas"

	• **Ejecución** • **Realizar operaciones en selecciones de dispositivos**			• "Historial de informes sobr el registro de aplicaciones" • "Informe sobr el estado de l grupos de aplicaciones c licencia" • "Informe sobr claves de licencia de software de terceros"

Funciones de usuario predefinidas

Las funciones de usuario asignadas a los usuarios de Kaspersky Security Center les proporcionan conjuntos de derechos de acceso a las funciones de la aplicación.

Puede utilizar las funciones de usuario predefinidas con un conjunto de derechos ya configurado, o crear nuevas funciones y configurar los derechos necesarios usted mismo. Algunas de las funciones de usuario predefinidas disponibles en Kaspersky Security Center se pueden asociar con puestos de trabajo específicos, por ejemplo, **Auditor**, **Director de seguridad**, **Supervisor** (estas funciones están presentes en Kaspersky Security Center a partir de la versión 11). Los derechos de acceso de estas funciones están preconfiguradas de acuerdo con las tareas estándar y el alcance de las responsabilidades de los puestos asociados. La siguiente tabla muestra como las funciones pueden estar asociadas con puestos de trabajo específicos.

Ejemplos de funciones para puestos de trabajo específicos

Función	Comentario
Auditor	Permisos de todas las operaciones con todos los tipos de informes, todas las operaciones de visualización, incluyendo la visualización de objetos eliminados (concede los permisos **Leer** y **Editar** en el área de **objetos eliminados**). No permite otras operaciones. Puede asignar esta función a una persona que realice la auditoría de su organización.
Supervisor	Permite todas las operaciones de visualización, no permite otras operaciones. Puede asignar esta función a un director de seguridad y otros gerentes a cargo de la seguridad de TI en su organización.
Director de seguridad.	Permite todas las operaciones de visualización, permite la administración de informes; otorga permisos limitados en la **administración del sistema**: área de **Conectividad**. Puede asignar esta función a un responsable a cargo de la seguridad de TI en su organización.

La siguiente tabla muestra los derechos de acceso asignados a cada función de usuario predefinida.

Derechos de acceso de las funciones de usuario predefinidas

Función	Descripción
Administrador del Servidor de administración	Permite todas las operaciones en las siguientes áreas funcionales: • **Funciones generales**: • **Funcionalidad básica**

	• **Procesamiento de eventos** • **Jerarquía de Servidores de administración** • **Servidores de administración virtual** • **Administración del sistema**: • **Conectividad** • **Inventario de hardware** • **Inventario de software**
Operador del Servidor de administración	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes: • **Funciones generales**: • **Funcionalidad básica** • **Servidores de administración virtual** • **Administración del sistema**: • **Conectividad** • **Inventario de hardware** • **Inventario de software**
Auditor	Permite todas las operaciones de las áreas funcionales, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL** • **Objetos eliminados** • **Gestión reforzada de informes** Puede asignar esta función a una persona que realice la auditoría de su organización.
Administrador de instalación	Permite todas las operaciones en las siguientes áreas funcionales: • **Funciones generales**: • **Funcionalidad básica** • **Despliegue del software de Kaspersky** • **Administración de claves de licencia** • **Administración del sistema**: • **Despliegue del sistema operativo** • **Administración de vulnerabilidades y parches** • **Instalación remota**

	• **Inventario de software** Otorga los derechos de **lectura** y **ejecución** en el área funcional **Características generales: Servidores de administración virtual**.

Operador de instalación	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes:
	• **Funciones generales**:
	  • **Funcionalidad básica**
	  • **Despliegue del software Kaspersky** (también otorga el derecho **Administrar parches de Kaspersky** en esta área)
	  • **Servidores de administración virtual**
	• **Administración del sistema**:
	  • **Despliegue del sistema operativo**
	  • **Administración de vulnerabilidades y parches**
	  • **Instalación remota**
	  • **Inventario de software**

Administrador de Kaspersky Endpoint Security	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: Funcionalidad básica** • Área de Kaspersky Endpoint Security, incluidas todas las funciones
Operador de Kaspersky Endpoint Security	Otorga los derechos de **lectura** y **ejecución** en todas las áreas funcionales siguientes: • **Características generales: Funcionalidad básica** • Área de Kaspersky Endpoint Security, incluidas todas las funciones
Administrador principal	Permite todas las operaciones en áreas funcionales, *excepto* en las siguientes áreas, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL** • **Gestión reforzada de informes**

Operador principal	Otorga los derechos de **lectura** y **ejecución** (cuando corresponda) en todas las áreas funcionales siguientes:
	• **Funciones generales**:
	  • **Funcionalidad básica**
	  • **Objetos eliminados**
	  • **Operaciones en el Servidor de administración**
	  • **Despliegue del software de Kaspersky**

	• **Servidores de administración virtual** • **Administración de dispositivos móviles: General** • **Administración del sistema**, incluidas todas las funciones • Área de Kaspersky Endpoint Security, incluidas todas las funciones
Administrador de Administración de dispositivos móviles	Permite todas las operaciones en las siguientes áreas funcionales: • **Características generales: Funcionalidad básica** • **Administración de dispositivos móviles: General**
Operador de Administración de dispositivos móviles	Otorga los derechos de **lectura** y **ejecución** en el área funcional **Funciones generales**: **Funcionalidad básica**. Otorga derechos de **lectura** y **Enviar solo comandos de información a dispositivos móviles** en el área funcional **Administración de dispositivos móviles**: **General**.
Director de seguridad.	Permite todas las operaciones de las siguientes áreas funcionales, en **Funciones generales**: • **Acceder a objetos independientemente de sus ACL** • **Gestión reforzada de informes** Otorga derechos de **Lectura**, **Modificación**, **Ejecución**, **Guardar archivos desde los dispositivos a la estación de trabajo del administrador** y **Realizar operaciones para las selecciones de dispositivos** en el área funcional **Administración del sistema: Conectividad**. Puede asignar esta función a un responsable a cargo de la seguridad de TI en su organización.
Usuario del Self Service Portal	Permite todas las operaciones en el área funcional **Administración de dispositivos móviles: Self Service Portal**. Esta función no es compatible con Kaspersky Security Center 11 y versiones posteriores.
Supervisor	Otorga el derecho de **lectura** en las áreas funcionales **Funciones generales**: **Acceder a objetos, independientemente de sus ACL** y **Funciones generales**: **Gestión reforzada de informes**. Puede asignar esta función a un director de seguridad y otros gerentes a cargo de la seguridad de TI en su organización.
Administrador de Administración de vulnerabilidades y parches	Permite todas las operaciones en las áreas funcionales **Funciones generales**: **Funcionalidad básica** y **Administración del sistema** (incluidas todas las funciones).
Operador de Administración de vulnerabilidades y parches	Otorga derechos de **lectura** y **ejecución** (cuando corresponda) en las áreas funcionales **Funciones generales**: **Funcionalidad básica** y **Administración del sistema** (incluidas todas las funciones).

Añadir una cuenta de un usuario interno

Para añadir una nueva cuenta de usuario interna a Kaspersky Security Center:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Haga clic en **Añadir**.
3. En la ventana **Nueva entidad** que se abre, especifique la configuración de la nueva cuenta de usuario:
   - Mantenga la opción predeterminada **Usuario**.
   - **Nombre**.
   - **Contraseña** para la conexión del usuario a Kaspersky Security Center.
     La contraseña debe cumplir con las siguientes reglas:
     - La contraseña debe tener entre 8 y 16 caracteres.
     - La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
       - Mayúsculas (A-Z)
       - Minúsculas (a-z)
       - Números (0-9)
       - Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

     Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

     El número de intentos de introducción de la contraseña es limitado. De forma predeterminada, el número máximo de intentos de introducción de la contraseña permitidos es 10. Puede cambiar el número permitido de intentos para introducir una contraseña, como se describe en "Cambiar el número de intentos de ingreso de contraseña permitidos".

     Si el usuario introduce incorrectamente la contraseña el número especificado de veces, la cuenta de usuario quedará bloqueada durante una hora. Puede desbloquear la cuenta de usuario cambiando solo la contraseña.
   - **Nombre completo**
   - **Descripción**
   - **Dirección de correo electrónico**
   - **Teléfono**
4. Haga clic en **Correcto** para guardar los cambios.

La nueva cuenta de usuario aparece en la lista usuarios y grupos de usuarios.

Crear un grupo de usuarios

Para crear un grupo de usuarios:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Haga clic en **Añadir**.
3. Cuando se abre la ventana **Nueva entidad**, seleccione **Grupo**.
4. Especifique la siguiente configuración para el nuevo grupo de usuarios:
   - **Nombre del grupo**
   - **Descripción**
5. Haga clic en **Correcto** para guardar los cambios.

El nuevo grupo de usuarios aparece en la lista de usuarios y grupos de usuarios.

Editar una cuenta de un usuario interno

Modificar una cuenta de usuario interna en Kaspersky Security Center:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Haga clic en el nombre de la cuenta de usuario que desea editar.
3. En la ventana de configuración de usuario que se abre, en la pestaña **Control de aplicaciones**, cambie la configuración de la cuenta de usuario:
   - **Descripción**
   - **Nombre completo**
   - **Dirección de correo electrónico**
   - **Teléfono principal**
   - **Contraseña** para la conexión del usuario a Kaspersky Security Center.
     La contraseña debe cumplir con las siguientes reglas:
     - La contraseña debe tener entre 8 y 16 caracteres.
     - La contraseña debe contener caracteres de al menos tres de los grupos enumerados a continuación:
       - Mayúsculas (A-Z)
       - Minúsculas (a-z)

- Números (0-9)
- Caracteres especiales (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- La contraseña no debe contener espacios en blanco, caracteres Unicode o la combinación de "." y "@", cuando "." está colocado delante de "@".

Para ver la contraseña introducida, haga clic y mantenga presionado el botón **Mostrar**.

El número de intentos de introducción de la contraseña es limitado. De forma predeterminada, el número máximo de intentos de introducción de la contraseña permitidos es 10. Puede cambiar el número permitido de intentos; sin embargo, por razones de seguridad, no recomendamos que reduzca este número. Si el usuario introduce incorrectamente la contraseña el número especificado de veces, la cuenta de usuario quedará bloqueada durante una hora. Puede desbloquear la cuenta de usuario cambiando solo la contraseña.

- Si es necesario, cambie el botón de alternar a **Desactivado** para prohibir que el usuario se conecte a la aplicación. Puede desactivar una cuenta, por ejemplo, después de que un empleado abandone la empresa.

4. En la pestaña **Seguridad de la autenticación**, puede especificar la configuración de seguridad para esta cuenta.
5. En la pestaña **Grupos**, puede añadir al usuario a grupos de seguridad.
6. En la pestaña **Dispositivos**, puede asignar dispositivos al usuario.
7. En la pestaña **Funciones**, puede asignar dispositivos al usuario.
8. Haga clic en **Guardar** para guardar los cambios.

La cuenta de usuario actualizada aparece en la lista de usuarios y en los grupos de usuarios.

Editar un grupo de usuarios

Puede editar solo los grupos internos.

Para editar un grupo de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Haga clic en el nombre del grupo de usuarios que desea editar.
3. En la ventana de configuración del grupo que se abre, cambie la configuración del grupo de usuarios:
   - **Nombre**
   - **Descripción**
4. Haga clic en **Guardar** para guardar los cambios.

El grupo de usuarios actualizado aparece en la lista de usuarios y grupos de usuarios.

Adición de cuentas de usuario a un grupo interno

Solo puede añadir cuentas de usuarios internos a un grupo interno.

Para añadir cuentas de usuario a un grupo interno:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Seleccione las casillas junto a las cuentas de usuario que desea añadir a un grupo.
3. Haga clic en el botón **Asignar grupo**.
4. En la ventana que se abre **Asignar grupo**, seleccione el grupo al que desea añadir cuentas de usuario.
5. Haga clic en el botón **Asignar**.

Las cuentas de usuario se añaden al grupo.

Designación del usuario como propietario del dispositivo

Para obtener información sobre cómo asignar un usuario como propietario de un dispositivo móvil, consulte la Ayuda de Kaspersky Security para dispositivos móviles.

Para asignar un usuario como propietario del dispositivo:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Haga clic en el nombre de la cuenta de usuario que desea asignar como propietario del dispositivo.
3. En la ventana de configuración de usuario que se abre, seleccione la pestaña **Dispositivos**.
4. Haga clic en **Añadir**.
5. En la lista de dispositivos, seleccione el dispositivo que desea asignar al usuario.
6. Haga clic en **Aceptar**.

El dispositivo seleccionado se añade a la lista de dispositivos asignados al usuario.

Puede realizar la misma operación en **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**, haciendo clic en el nombre del dispositivo que desea asignar y después haciendo clic en el enlace **Administrar propietario del dispositivo**.

Eliminar un usuario o un grupo de seguridad

Solo puede eliminar usuarios internos o grupos de seguridad internos.

Para eliminar un usuario o un grupo de seguridad:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Seleccione la casilla de verificación junto al usuario o el grupo de seguridad que desea eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Correcto**.

Se elimina el usuario o el grupo de seguridad.

Creación de funciones de usuario

Para crear una función de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.
2. Haga clic en **Añadir**.
3. En la ventana **Nombre de la nueva función** que se abre, introduzca el nombre de la nueva función.
4. Haga clic en **Correcto** para aplicar los cambios.
5. En la ventana de propiedades de la función que se abre, cambie la configuración de la función:
   - En la pestaña **Control de aplicaciones**, modifique el nombre de la función.
     No puede editar el nombre de una función predefinida.
   - En la pestaña **Configuración**, modifique la cobertura de la función y directivas y los perfiles asociados con la función.
   - En la pestaña **Derechos de acceso**, modifique los derechos para el acceso a aplicaciones de Kaspersky.
6. Haga clic en **Guardar** para guardar los cambios.

La nueva función aparece en la lista de funciones del usuario.

Editar una función de usuario

Para editar una función de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.
2. Haga clic en el nombre de la función que desea editar.
3. En la ventana de propiedades de la función que se abre, cambie la configuración de la función:
   - En la pestaña **Control de aplicaciones**, modifique el nombre de la función.
     No puede editar el nombre de una función predefinida.
   - En la pestaña **Configuración**, modifique la cobertura de la función y directivas y los perfiles asociados con la función.
   - En la pestaña **Derechos de acceso**, modifique los derechos para el acceso a aplicaciones de Kaspersky.
4. Haga clic en **Guardar** para guardar los cambios.

La nueva función aparece en la lista de funciones de usuario.

Editar la cobertura de una función de usuario

Una *cobertura de la función de usuario* es una combinación de usuarios y grupos de administración. La configuración asociada con una función de usuario se aplica solo a los dispositivos que pertenecen a usuarios que tienen esta función y solo si estos dispositivos pertenecen a grupos asociados con esta función, incluidos los grupos secundarios.

Para añadir usuarios, grupos de seguridad y grupos de administración a la cobertura de una función del usuario, puede utilizar cualquiera de los siguientes métodos:

Método 1:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **USUARIOS**.
2. Seleccione las casillas de verificación junto a los usuarios y grupos de seguridad que desee añadir a la cobertura de la función de usuario.
3. Haga clic en el botón **Asignar función**.
   Se inicia el Asistente de asignación de funciones. Avance a través del Asistente utilizando el botón **Siguiente**.
4. En la página del Asistente **Seleccionar función**, seleccione la función de usuario que quiere asignar.
5. En la página del Asistente **Definir cobertura**, seleccione el grupo de administración que desea añadir a la cobertura de la función de usuario.
6. Haga clic en el botón **Asignar función** para cerrar el Asistente.

Los usuarios o grupos de seguridad seleccionados y el grupo de administración seleccionado se añaden al ámbito de la función de usuario.

Método 2:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.

2. Haga clic en el nombre de la función para la que desea definir la cobertura.

3. En la ventana de propiedades de la función que se abre, seleccione la pestaña **Configuración**.

4. En la sección **Cobertura de la función**, haga clic en **Añadir**.

   Se inicia el Asistente de asignación de funciones. Avance a través del Asistente utilizando el botón **Siguiente**.

5. En la página del Asistente **Definir cobertura**, seleccione el grupo de administración que desea añadir a la cobertura de la función de usuario.

6. En la página del Asistente **Seleccionar usuarios**, seleccione el grupo de seguridad y usuarios que desea añadir a la cobertura de la función de usuario.

7. Haga clic en el botón **Asignar función** para cerrar el Asistente.

8. Haga clic en el botón **Cerrar** (⨯) para cerrar la ventana de propiedades de la función.

Los usuarios o grupos de seguridad seleccionados y el grupo de administración seleccionado se añaden al ámbito de la función de usuario.

Eliminar una función de usuario

Para eliminar una función de usuario:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.

2. Seleccione las casillas de verificación junto al nombre de la función que quiere eliminar.

3. Haga clic en **Eliminar**.

4. En la ventana que se abre, haga clic en **Correcto**.

Se elimina la función del usuario.

Asociación de perfiles de directivas con funciones

Puede asociar funciones de usuario con perfiles de directiva. En este caso, la regla de activación para este perfil de directiva se basa en la función: el perfil de directiva se activa para un usuario que tiene la función especificada.

Por ejemplo, la directiva obstruye cualquier software de navegación GPS en todos los dispositivos en un grupo de administración. El software de navegación GPS solo hace falta en un dispositivo del grupo de administración de usuarios: el perteneciente al mensajero. En este caso, puede asignar una función de "Mensajero" a su propietario y luego crear un perfil de directiva que permita que el software de navegación GPS se ejecute solo en los dispositivos cuyos propietarios tienen asignada la función de "Mensajero". Todas las demás configuraciones de directivas se conservan. Solo el usuario con la función "Mensajero" podrá ejecutar el software de navegación GPS. Más adelante, si a otro trabajador se le asigna la función de "Mensajero", el nuevo trabajador también puede ejecutar el software de navegación en el dispositivo de su organización. La ejecución del software de navegación GPS aún estará prohibida en otros dispositivos en el mismo grupo de administración.

Asociar una función con un perfil de directiva:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES** → **Funciones**.
2. Haga clic en el nombre de la función que desea asociar con un perfil de directiva.
   La ventana de propiedades de la función se abre con la pestaña **Control de aplicaciones** seleccionada.
3. Seleccione la pestaña **Configuración** y desplácese hacia abajo a la sección **Directivas y perfiles**.
4. Haga clic en **Editar**.
5. Asociar la función con:
   - **Un perfil de directiva existente**: Haga clic en el icono de flecha (>) al lado del nombre de la directiva requerida, y luego seleccione la casilla que está al lado del perfil con la cual desea asociar la función.
   - **Nuevo perfil de directiva**:
     a. Seleccione la casilla junto a la directiva para la que desee crear un perfil.
     b. Haga clic en **Nuevo perfil de directiva**.
     c. Seleccione la casilla de verificación junto a la directiva para la que desea crear un perfil.
     d. Haga clic en el botón **Guardar**.
     e. Seleccione la casilla de verificación junto al nuevo perfil.
6. Haga clic en **Asignar a función**.

El perfil está asociado con la función y aparece en las propiedades de la función. El perfil se aplica automáticamente a cualquier dispositivo cuyo propietario tenga asignada la función.

Gestión de objetos en Kaspersky Security Center 14 Web Console:

Esta sección contiene información sobre la administración de la revisión de objetos. Kaspersky Security Center le permite rastrear la modificación de objeto. Cada vez que guarda cambios realizados en un objeto, se crea una *revisión*. Cada revisión tiene un número.

Los objetos de aplicación que admiten administración de la revisión incluyen:

- Servidores de administración
- Directivas
- Tareas
- Grupos de administración
- Cuentas de usuario
- Paquetes de instalación

Puede realizar las acciones siguientes en revisiones de objetos:

- Compare una revisión seleccionada con la actual
- Comparar revisiones seleccionadas
- Compare un objeto con una revisión seleccionada de otro objeto del mismo tipo
- Vea una revisión seleccionada
- Deshaga cambios realizados en un objeto a una revisión seleccionada
- Guardar revisiones como un archivo .txt

En la ventana de propiedades de cualquier objeto que admita administración de la revisión, la sección **Historial de revisiones** muestra una lista de revisiones de objetos con los siguientes datos:

- Número de revisión del objeto
- Fecha y hora de modificación del objeto
- Nombre del usuario que modificó el objeto
- Acción que se ejecutó sobre el objeto
- Descripción de la revisión relacionada con el cambio realizado a la configuración de objeto

De forma predeterminada, la descripción de la revisión de objeto está en blanco. Para agregar una descripción a una revisión, seleccione la revisión relevante y haga clic en el botón **Descripción**. En la ventana **Descripción de la revisión del objeto**, añada texto para la descripción de la revisión.

Agregar una descripción a la revisión

Kaspersky Security Center le permite rastrear la modificación de objeto. Cada vez que guarda cambios realizados en un objeto, se crea una revisión. Cada revisión tiene un número.

Puede agregar una descripción a la revisión para simplificar la búsqueda de revisiones en la lista.

Para agregar una descripción para una revisión:

1. Vaya a la sección **Historial de revisión** del objeto.
2. En la lista de revisiones de objetos, seleccione la revisión a la que necesita agregar una descripción.
3. Haga clic en el botón **Editar descripción**.
   Se abre la ventana **Descripción**.
4. En la ventana **Descripción**, añada texto para la descripción de la revisión.
   De forma predeterminada, la descripción de la revisión de objeto está en blanco.
5. Haga clic en el botón **Guardar**.

La descripción se añade a la revisión del objeto.

Eliminación de un objeto

Puede eliminar objetos como políticas, tareas, paquetes de instalación, usuarios internos y grupos de usuarios internos si tiene permisos de Edición que están dentro de la categoría de derechos de Funcionalidad básica.

Para eliminar un objeto:

1. Seleccione el objeto o los objetos que desea eliminar.
2. Haga clic en el botón **Eliminar**.
3. Haga clic en el botón **Aceptar** para confirmar la eliminación de los objetos seleccionados.

El objeto (o los objetos seleccionados) se eliminará y la información sobre él se guardará en la base de datos.

Kaspersky Security Network (KSN)

Esta sección describe cómo utilizar la infraestructura de servicios en línea denominada Kaspersky Security Network (KSN). La sección proporciona información sobre KSN, así como instrucciones acerca de cómo habilitar KSN, configurar el acceso a KSN y consultar estadísticas de uso de KSN.

Acerca de KSN

Kaspersky Security Network (KSN) es una infraestructura de servicios en línea que proporciona acceso a la Base de conocimientos en línea de Kaspersky, donde hay información disponible sobre la reputación de los archivos, los recursos web y el software. El uso de datos de Kaspersky Security Network garantiza respuestas más rápidas de las aplicaciones Kaspersky a las amenazas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos. KSN permite utilizar las bases de datos de reputación de Kaspersky para obtener información sobre las aplicaciones instaladas en los dispositivos administrados.

Al participar en el programa KSN, acepta enviar automáticamente a Kaspersky información sobre el funcionamiento de las aplicaciones Kaspersky instaladas en los dispositivos cliente administrados por Kaspersky Security Center. La información se transfiere de acuerdo con la configuración de acceso de KSN actual.

La aplicación le solicita que se una a KSN durante la ejecución del Asistente de inicio rápido. Puede comenzar a utilizar KSN o dejar de hacerlo en cualquier momento que se encuentre utilizando la aplicación.

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si la Declaración de KSN se ha actualizado, se la muestra cuando actualiza o el Servidor de administración o pasa a una versión más nueva. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si la rechaza, seguirá usando KSN de acuerdo con la versión anterior de la Declaración de KSN que aceptó anteriormente.

Cuando KSN está activado, Kaspersky Security Center comprueba si se puede acceder a los servidores de KSN. Si no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza el DNS público. Esto es necesario para garantizar que se mantenga el nivel de seguridad de los dispositivos administrados.

Los dispositivos cliente administrados por el Servidor de administración interactúan con KSN mediante el proxy de KSN. El proxy KSN proporciona las funciones siguientes:

- Los dispositivos cliente pueden enviar consultas a KSN y transferir información a KSN aunque no dispongan de acceso directo a Internet.
- El Servidor proxy de KSN coloca en la memoria caché los datos procesados, de manera que se reduce la carga en el canal de salida, así como el tiempo de espera en las consultas de información realizadas por un dispositivo cliente.

Puede configurar el Servidor proxy de KSN en la sección **Proxy de KSN** de la ventana de propiedades del Servidor de administración.

Configuración del acceso a Kaspersky Security Network

Puede configurar el acceso a Kaspersky Security Network (KSN) en el Servidor de administración y en un punto de distribución.

Para configurar el acceso del Servidor de administración a Kaspersky Security Network (KSN):

1. Haga clic en el icono de **Configuración** () junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Configuración del proxy de KSN**.

3. Ponga el botón de alternancia en la posición **Activar proxy de KSN en el Servidor de administración ACTIVADA**.

   El Dato se envía desde dispositivos cliente a KSN de acuerdo con la directiva de seguridad de Kaspersky Endpoint que esté activa en esos dispositivos cliente. Si esta casilla está vacía, no se enviará ningún dato a KSN desde el Servidor de administración y los dispositivos cliente mediante Kaspersky Security Center. Sin embargo, los dispositivos cliente pueden enviar datos directamente a KSN (omitiendo Kaspersky Security Center), de conformidad con sus respectivas configuraciones. La directiva de Kaspersky Endpoint Security para Windows, que está activa en los dispositivos cliente determina qué datos enviarán directamente (omitiendo Kaspersky Security Center) dichos dispositivos a KSN.

4. Ponga el botón de alternancia en la posición **Usar Kaspersky Security Network ACTIVADA**.

   Si activa esta opción, los dispositivos cliente enviarán resultados sobre la instalación de parches a Kaspersky. Antes de activar esta opción, asegúrese de leer y aceptar las condiciones de la Declaración de KSN.

   Si está utilizando KSN privada, ponga el botón de alternancia en la posición **Usar Kaspersky Private Security Network ACTIVADA** y haga clic en el botón **Seleccionar archivo con la configuración del Proxy de KSN** para descargar la configuración de KSN privada (archivos con las extensiones pkcs7 y pem). Tras descargar la configuración, la interfaz muestra el nombre y los contactos del proveedor, así como la fecha de creación del archivo de configuración de la KSN privada.

   > Cuando habilite KSN privada, preste atención a los puntos de distribución configurados para enviar solicitudes de KSN directamente a Cloud KSN. Los puntos de distribución que tengan instalado el Agente de red versión 11 (o versiones anteriores) continuarán enviando solicitudes KSN a Cloud KSN. Para reconfigurar los puntos de distribución para enviar solicitudes KSN a KSN privada, active la opción **Reenviar solicitudes de KSN al Servidor de administración** para cada punto de distribución. Puede activar esta opción en las propiedades del punto de distribución o en la directiva del Agente de red.

   Cuando pone el botón de alternancia en la posición **Usar Kaspersky Private Security Network ACTIVADA**, aparece un mensaje con detalles sobre KSN privada.

   Las siguientes aplicaciones Kaspersky admiten KSN privada:

   - Kaspersky Security Center 10 Service Pack 1 o posterior

- Kaspersky Endpoint Security 10 Service Pack 1 para Windows o posterior
- Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
- Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

Si activa KSN privada en Kaspersky Security Center, estas aplicaciones reciben información sobre la compatibilidad con KSN privada. En la ventana de configuración de la aplicación, en la subsección **Kaspersky Security Network** de la sección **Protección contra amenazas avanzada**, se muestra **proveedor de KSN: KSN privada**. De lo contrario, se muestra **proveedor de KSN: KSN Global**.

Si utiliza versiones de aplicaciones anteriores a Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 o una anteriores a Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent cuando ejecuta KSN privada, le recomendamos que utilice Servidores de administración secundarios que no tengan habilitado el uso de KSN privada.

Kaspersky Security Center no envía ningún dato estadístico a Kaspersky Security Network si KSN privada está configurada en la sección **Configuración del proxy de KSN** de la ventana de propiedades del Servidor de administración.

Si tiene la configuración del servidor proxy configurada en las propiedades del Servidor de administración pero su arquitectura de red requiere que su KSN privada active directamente la opción **Ignorar la configuración del servidor proxy al conectarse a KSN privada**. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a la KSN privada.

5. Configure la conexión del Servidor de administración al servicio de proxy de KSN:
   - Bajo **Configuración de la conexión**, para el **Puerto TCP**, especifique el número de puerto TCP que se debe usar para conectarse al Servidor proxy de KSN. El puerto predeterminado de conexión al Servidor proxy de KSN es 13111.
   - Si desea que el Servidor de administración se conecte al Servidor proxy de KSN mediante un puerto UDP, active la opción **Usar puerto UDP** y especifique un número de puerto para el **Puerto UDP**. De forma predeterminada, esta opción está desactivada y se utiliza el puerto TCP. Si esta opción está habilitada, el puerto UDP predeterminado de conexión al Servidor proxy de KSN será 15111.
6. Ponga el botón de alternancia en la posición **Conectar Servidores de administración secundarios a KSN mediante el Servidor de administración principal ACTIVADA**.

   Si se activa esta opción, los Servidores de administración secundarios usarán el Servidor de administración principal como Servidor proxy de KSN. Si se desactiva esta opción, los Servidores de administración secundarios se conectarán a KSN por su propia cuenta. En este caso, los dispositivos administrados usarán los Servidores de administración secundarios como Servidores proxy de KSN.

   Los Servidores de administración secundarios usarán el Servidor de administración principal como servidor proxy si en el panel derecho de la sección **Configuración del proxy de KSN** en las propiedades de los Servidores de administración secundarios el botón de alternancia está puesto en la posición **Activar proxy de KSN en el Servidor de administración ACTIVADA**.
7. Haga clic en el botón **Guardar**.

Se guarda la configuración de acceso a KSN.

También puede configurar el acceso de puntos de distribución a KSN, por ejemplo, si desea reducir la carga sobre el Servidor de administración. El punto de distribución que actúa como Servidor proxy de KSN envía las solicitudes de KSN directamente a Kaspersky desde los dispositivos administrados, sin utilizar el Servidor de administración.

Para configurar el acceso del punto de distribución a Kaspersky Security Network (KSN):

1. Asegúrese que el punto de distribución se asigne manualmente.
2. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.
3. En la pestaña **Control de aplicaciones**, seleccione la sección **Puntos de distribución**.
4. Haga clic en el nombre del punto de distribución para abrir su ventana de propiedades.
5. En la ventana de propiedades del punto de distribución, en la sección **Proxy de KSN**, active la opción **Activar el proxy de KSN en el punto de distribución**, y luego active la opción **Acceder a la nube de KSN/KSN privada directamente a través de Internet**.
6. Haga clic en **Aceptar**.

El punto de distribución actuará como un Servidor proxy de KSN.

Habilitación y deshabilitación de KSN

Para habilitar KSN, siga estos pasos:

1. Haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione la sección **Configuración del proxy de KSN**.
3. Ponga el botón de alternancia en la posición **Activar proxy de KSN en el Servidor de administración ACTIVADA**.

   Se habilita el Servidor proxy de KSN.
4. Ponga el botón de alternancia en la posición **Usar Kaspersky Security Network ACTIVADA**.

   Se habilita KSN.

   Si el botón de alternancia está activado, los dispositivos cliente envían los resultados de la instalación del parche a Kaspersky. Al activar este botón de alternancia, debe leer y aceptar los términos de la declaración de KSN.
5. Haga clic en el botón **Guardar**.

Para deshabilitar KSN, siga estos pasos:

1. Haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.
2. En la pestaña **Control de aplicaciones**, seleccione la sección **Configuración del proxy de KSN**.

3. Cambie el botón de alternancia a la posición **Activar proxy de KSN en el Servidor de administración DESACTIVADA** para desactivar el servicio de proxy de KSN, o cambie el botón a la posición **Usar Kaspersky Security Network DESACTIVADA**.

   Si este botón de alternancia está desactivado, los dispositivos cliente no enviarán resultados de instalación de parches a Kaspersky.

   Si está utilizando KSN privada, cambie el botón de alternancia a la posición **Usar Kaspersky Private Security Network DESACTIVADA**.

   Se deshabilita KSN.

4. Haga clic en el botón **Guardar**.

Ver la declaración de KSN aceptada

Cuando habilita Kaspersky Security Network (KSN), debe leer y aceptar la Declaración de KSN. Puede ver la declaración de KSN aceptada en cualquier momento.

Para ver la declaración de KSN aceptada:

1. Haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Configuración del proxy de KSN**.

3. Haga clic en el enlace **Ver la declaración de Kaspersky Security Network**.

En la ventana que se abre, puede ver el texto de la Declaración de KSN aceptada.

Aceptación de una declaración de KSN actualizada

Utiliza KSN de acuerdo con la Declaración de KSN que lee y acepta cuando habilita KSN. Si la Declaración de KSN se ha actualizado, se la muestra cuando actualiza o el Servidor de administración o pasa a una versión más nueva. Puede aceptar la Declaración de KSN actualizada o rechazarla. Si lo rechaza, sigue utilizando KSN de acuerdo con la versión de la declaración de KSN que aceptó anteriormente.

Después de actualizar o pasar a una nueva versión del Servidor de Administración, la Declaración de KSN actualizada se muestra automáticamente. Si rechaza la Declaración de KSN actualizada, aún puede verla y aceptarla más tarde.

Para ver y luego aceptar o rechazar una Declaración de KSN actualizada:

1. Haga clic en el enlace **Ver notificaciones** en la esquina superior derecha de la ventana principal de la aplicación.

   Se abre la ventana **Notificaciones**.

2. Haga clic en el enlace **Ver la declaración de KSN actualizada**.

   Se abre la ventana **Actualización de la declaración de Kaspersky Security Network**.

3. Lea atentamente la Declaración de KSN y luego tome su decisión haciendo clic en uno de los siguientes botones:

   - **Acepto la declaración actualizada de KSN**

- **Uso de KSN según la declaración anterior**

Dependiendo de su elección, KSN sigue funcionando de acuerdo con los términos de la Declaración de KSN actual o actualizada. Usted puede ver el texto de la declaración de KSN aceptada en las propiedades del Servidor de administración en cualquier momento.

Comprobar si el punto de distribución funciona como KSN Proxy

En un dispositivo administrado asignado para funcionar como punto de distribución, puede habilitar KSN Proxy. Un dispositivo administrado funciona como KSN Proxy cuando el servicio ksnproxy se está ejecutando en el dispositivo. Puede verificar, activar o desactivar este servicio de forma local en el dispositivo.

Para comprobar si el punto de distribución funciona como proxy KSN:

1. En el dispositivo que funciona como punto de distribución, en Windows, abra **Servicios** (**Todos los programas** → **Herramientas administrativas** → **Servicios**).

2. En la lista de servicios, verifique si el servicio ksnproxy se está ejecutando.

   Si el servicio ksnproxy se está ejecutando, entonces el Agente de red en el dispositivo participa en Kaspersky Security Network y funciona como KSN Proxy para los dispositivos administrados incluidos en el alcance del punto de distribución.

Si lo desea, puede desactivar el servicio ksnproxy. En este caso, el Agente de red en el punto de distribución deja de participar en Kaspersky Security Network. Esto requiere derechos de administrador local.

Escenario: Actualización de Kaspersky Security Center y de las aplicaciones de seguridad administradas

Esta sección describe brevemente el escenario principal para pasar a una versión más reciente de Kaspersky Security Center y las aplicaciones de seguridad administradas.

La actualización de Kaspersky Security Center y de las aplicaciones de seguridad administradas se realiza en etapas:

1. **Planificación de los recursos**

   Evalúe cuánto espacio de disco ocupa su base de datos. Asegúrese de tener suficiente espacio en el disco para almacenar la copia de seguridad de la configuración y la base de datos del Servidor de administración.

2. **Obtención del archivo de instalación para Kaspersky Security Center**

   Obtenga el archivo ejecutable de la versión actual de Kaspersky Security Center y guárdelo en el dispositivo que funcionará como Servidor de administración. Lea las Notas de la publicación de la versión de Kaspersky Security Center que desea usar.

3. **Creación de una copia de seguridad de la versión anterior**

   Utilice la utilidad de copia de seguridad y recuperación de datos para crear una copia de seguridad de los datos del Servidor de administración.

4. **Ejecución del instalador**

Ejecute el archivo ejecutable para la última versión de Kaspersky Security Center. Al ejecutar el archivo, especifique que tiene una copia de seguridad y especifique su ubicación. Sus datos serán restaurados desde la copia de seguridad.

5. **Actualización de las aplicaciones administradas**

   Puede actualizar la aplicación si hay una versión disponible más reciente. Lea la lista de aplicaciones admitidas de Kaspersky y asegúrese de que su versión de Kaspersky Security Center sea compatible con esta aplicación. Después, realice la actualización de la aplicación como se describe en sus Notas de publicación.

Resultados

Al finalizar el escenario de actualización, asegúrese de que la nueva versión del Servidor de administración se haya instalado correctamente en Microsoft Management Console. Haga clic en **Ayuda** → **Acerca de Kaspersky Security Center**. Se muestra la versión.

Para asegurarse de que está utilizando la nueva versión del Servidor de administración de Kaspersky Security Center 14 Web Console, en la parte superior de la pantalla haga clic en el icono **Configuración** ( ) junto al nombre del Servidor de administración. En la ventana de propiedades Servidor de administración que se abre, en la pestaña **Control de aplicaciones**, seleccione la sección **Control de aplicaciones**. Se muestra la versión.

Si actualizó una aplicación de seguridad administrada, asegúrese de que esté correctamente instalada en el(los) dispositivo(s) administrado(s). Para más información, consulte la documentación de esta aplicación.

Actualización de bases de datos Kaspersky y aplicaciones

Esta sección describe los pasos que debe seguir para actualizar regularmente lo siguiente:

- Bases de datos y módulos de software de Kaspersky
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad

Escenario: actualización periódica de las bases de datos y aplicaciones de Kaspersky

Esta sección proporciona un escenario para la actualización regular de las bases de datos, módulos de software y aplicaciones de Kaspersky. Una vez completado el escenario de configuración de la protección de red, debe mantener la fiabilidad del sistema de protección para garantizar que los Servidores de administración y los dispositivos administrados estén protegidos contra diversas amenazas, entre ellas virus, ataques de red y ataques de phishing.

La protección de la red se mantiene actualizada mediante actualizaciones periódicas de lo siguiente:

- Bases de datos y módulos de software de Kaspersky
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad

Cuando complete este escenario, puede estar seguro de lo siguiente:

- Su red está protegida por el software más reciente de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad.
- Las bases de datos antivirus y otras bases de datos de Kaspersky críticas para la seguridad de la red estarán siempre actualizadas.

Requisitos previos

Los dispositivos administrados deben tener conexión con el Servidor de administración. Si no tienen conexión, considere actualizar las bases de datos, los módulos de software y las aplicaciones de Kaspersky de forma manual o directamente desde los servidores de actualización de Kaspersky.

El Servidor de administración debe tener una conexión a Internet.

Antes de comenzar, asegúrese de haber hecho lo siguiente:

1. Desplegado las aplicaciones de seguridad de Kaspersky en los dispositivos administrados según el escenario de implementación de aplicaciones de Kaspersky a través de Kaspersky Security Center 14 Web Console.
2. Creado y configurado todas las directivas, perfiles de directivas y tareas requeridas de acuerdo con el escenario de configuración de la protección de red.
3. Asignado una cantidad apropiada de puntos de distribución de acuerdo con la cantidad de dispositivos administrados y la topología de la red.

La actualización de bases de datos y aplicaciones de Kaspersky sucede en etapas:

1. **Elección de un esquema de actualización**

   Hay varios esquemas que puede usar para instalar actualizaciones para los componentes de Kaspersky Security Center y las aplicaciones de seguridad. Elija el esquema o varios esquemas que cumplan con los requisitos de su red.

2. **Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración**

   Esta tarea se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el Asistente, cree la tarea ahora.

   Esta tarea es necesaria para descargar actualizaciones de los servidores de actualización de Kaspersky al repositorio del Servidor de administración, así como para actualizar las bases de datos y módulos de software de Kaspersky para Kaspersky Security Center. Una vez que se descarguen las actualizaciones, se pueden propagar a los dispositivos administrados.

   Si su red tiene puntos de distribución asignados, las actualizaciones se descargan automáticamente desde el repositorio del Servidor de administración a los repositorios de los puntos de distribución. En este caso, los dispositivos administrados incluidos en la cobertura de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.

   Instrucciones:

   - Consola de administración: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración
   - Kaspersky Security Center 14 Web Console: Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración

3. **Creación de la tarea para descargar actualizaciones a los repositorios de los puntos de distribución (opcional)**

De forma predeterminada, las actualizaciones se descargan a los puntos de distribución desde el Servidor de administración. Puede configurar Kaspersky Security Center para descargar las actualizaciones a los puntos de distribución directamente desde los servidores de actualización de Kaspersky. La descarga a los repositorios de puntos de distribución es preferible si el tráfico entre el Servidor de administración y los puntos de distribución es más costoso que el tráfico entre los puntos de distribución y los servidores de actualización de Kaspersky o si su Servidor de administración no tiene acceso a Internet.

Cuando su red ha asignado puntos de distribución y se crea la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*, los puntos de distribución descargan actualizaciones de los servidores de actualización de Kaspersky y no del repositorio del Servidor de administración.

Instrucciones:

- Consola de administración: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución
- Kaspersky Security Center 14 Web Console: Creación de la tarea para descargar actualizaciones en los repositorios de los puntos de distribución

4. **Configurar puntos de distribución**

Cuando su red tenga puntos de distribución asignados, asegúrese de que la opción **Desplegar actualizaciones** esté habilitada en las propiedades de todos los puntos de distribución requeridos. Cuando esta opción está deshabilitada para un punto de distribución, los dispositivos incluidos en la cobertura del punto de distribución se actualizan desde el repositorio del Servidor de administración.

Si desea que los dispositivos administrados reciban actualizaciones solo desde los puntos de distribución, habilite la opción **Distribuir archivos solo mediante puntos de distribución** en la directiva del Agente de red.

5. **Optimización del proceso de actualización con el modelo sin conexión de la descarga de actualizaciones o los archivos diff (opcional)**

Puede optimizar el proceso de actualización utilizando el modelo sin conexión de la descarga de actualizaciones (habilitado de forma predeterminada) o utilizando archivos diff. Para cada segmento de red, debe elegir cuál de estas dos características habilitar, ya que no pueden funcionar simultáneamente.

Cuando el modelo sin conexión de la descarga de actualizaciones está habilitado, el Agente de red descarga las actualizaciones necesarias en el dispositivo administrado una vez que las actualizaciones se descargan en el repositorio del Servidor de administración, antes de que la aplicación de seguridad solicite las actualizaciones. Esto mejora la fiabilidad del proceso de actualización. Para usar esta función, active la opción **Descargar actualizaciones y bases de datos antivirus del Servidor de administración (recomendado)** en la directiva del Agente de red.

Si no utiliza el modelo sin conexión de la descarga de actualizaciones, puede optimizar el tráfico entre el Servidor de administración y los dispositivos administrados mediante el uso de archivos diff. Cuando esta función está habilitada, el Servidor de administración o un punto de distribución descarga archivos diferenciales en lugar de archivos completos de bases de datos o módulos de software de Kaspersky. Un archivo diff describe las diferencias entre dos versiones de un archivo de una base de datos o un módulo de software. Por lo tanto, un archivo diff ocupa menos espacio que un archivo completo. Esto reduce el tráfico entre el Servidor de administración o los puntos de distribución y los dispositivos administrados. Para usar esta función, active la opción **Descargar archivos de comparación** en las propiedades de la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de puntos de distribución.

Instrucciones:

- Utilización de archivos diff para actualizar bases de datos y módulos de software de Kaspersky
- Consola de administración: Activación y desactivación del modelo sin conexión de descarga de actualizaciones
- Kaspersky Security Center 14 Web Console: Activación y desactivación del modelo sin conexión de descarga de actualizaciones

6. **Verificación de las actualizaciones descargadas (opcional)**

   Antes de instalar las actualizaciones descargadas, puede verificar las actualizaciones mediante la tarea de *Verificación de actualizaciones*. Esta tarea ejecuta de forma secuencial las tareas de actualización de dispositivos y las tareas de análisis antivirus configuradas a través de la configuración para la colección especificada de dispositivos de prueba. Al obtener los resultados de la tarea, el Servidor de administración inicia o bloquea la propagación de la actualización a los dispositivos restantes.

   La tarea Verificación de actualizaciones se puede ejecutar como parte de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En las propiedades de la tarea *Descargar actualizaciones en el repositorio de tareas del Servidor de administración*, active la opción **Verificar actualizaciones antes de distribuir** en la Consola de administración o la opción **Ejecutar verificación de actualizaciones** en Kaspersky Security Center 14 Web Console.

   Instrucciones:

   - Consola de administración: Verificación de actualizaciones descargadas
   - Kaspersky Security Center 14 Web Console: Verificación de las actualizaciones descargadas

7. **Aprobar y rechazar actualizaciones de software**

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *No definido*. Puede cambiar el estado a *Aprobado* o *Rechazado*. Las actualizaciones aprobadas siempre están instaladas. Si una actualización requiere revisar y aceptar los términos del Contrato de licencia de usuario final, primero debe aceptar los términos. Después de eso, la actualización se puede propagar a los dispositivos administrados. Las actualizaciones no definidas solo se pueden instalar en el Agente de red y otros componentes de Kaspersky Security Center de acuerdo con la configuración de la directiva del Agente de red. Las actualizaciones para las que establece el estado *Rechazado* no se instalarán en los dispositivos. Si previamente se instaló una actualización rechazada para una aplicación de seguridad, Kaspersky Security Center intentará desinstalar la actualización de todos los dispositivos. Las actualizaciones para los componentes de Kaspersky Security Center no se pueden desinstalar.

   Instrucciones:

   - Consola de administración: Aprobar y rechazar actualizaciones de software
   - Kaspersky Security Center 14 Web Console: Aprobar y rechazar actualizaciones de software

8. **Configuración de la instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center**

   A partir de la versión 10 Service Pack 2, las actualizaciones y parches descargados para el Agente de red y otros componentes de Kaspersky Security Center se instalan automáticamente. Si dejó la opción **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir** activada en las propiedades del Agente de red, entonces todas las actualizaciones se instalarán automáticamente después de que se descarguen en el repositorio (o varios repositorios). Si esta opción está desactivada, los parches de Kaspersky que se hayan descargado y etiquetado con el estado *Indeterminado* solo se instalarán después de que el administrador cambie su estado a *Aprobados*.

   Para versiones del Agente de red anteriores a 10 Service Pack 2, asegúrese de que la opción **Actualizar módulos del Agente de red** esté activada en las propiedades de *Descargar actualizaciones al repositorio de la tarea del Servidor de administración* o *Descargar actualizaciones a los repositorios de puntos de distribución*.

   Instrucciones:

   - Consola de administración: Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center
   - Kaspersky Security Center 14 Web Console: Habilitar y deshabilitar la actualización automática y la aplicación de parches para los componentes de Kaspersky Security Center

9. **Instalación de actualizaciones para el Servidor de administración**

Las actualizaciones de software para el Servidor de administración no dependen de los estados de actualización. No se instalan automáticamente y deben ser aprobados previamente por el administrador en la pestaña **Supervisión** en la Consola de administración (**Servidor de administración** `<nombre del servidor>` → **Supervisión**) o en la sección **NOTIFICACIONES** en Kaspersky Security Center 14 Web Console (**SUPERVISIÓN E INFORMES** → **NOTIFICACIONES**). Después de eso, el administrador debe ejecutar explícitamente la instalación de las actualizaciones.

10. **Configuración de instalación automática de actualizaciones para las aplicaciones de seguridad**

    Cree las tareas de actualización para las aplicaciones administradas para proporcionar actualizaciones oportunas a las aplicaciones, los módulos de software y las bases de datos de Kaspersky, incluidas las bases de datos antivirus. Para garantizar actualizaciones oportunas, le recomendamos que seleccione la opción **Cuando se descargan nuevas actualizaciones en el repositorio** al configurar la planificación de tareas.

    Si su red incluye dispositivos solo IPv6 y quiere actualizar regularmente las aplicaciones de seguridad instaladas en dichos dispositivos, asegúrese de que el Servidor de administración versión que no sea anterior a 13.2 y el Agente de red (versión que no sea anterior a 13.2) estén instalados en los dispositivos administrados.

    De forma predeterminada, las actualizaciones para Kaspersky Endpoint Security para Windows y Kaspersky Endpoint Security para Linux se instalan solo después de cambiar el estado de la actualización a *Aprobado*. Puede cambiar la configuración de actualización en la tarea de actualización.

    Si una actualización requiere revisar y aceptar los términos del Contrato de licencia de usuario final, primero debe aceptar los términos. Después de eso, la actualización se puede propagar a los dispositivos administrados.

    Instrucciones:

    - Consola de administración: Instalación automática de actualizaciones de Kaspersky Endpoint Security en dispositivos
    - Kaspersky Security Center 14 Web Console: Instalación automática de actualizaciones de Kaspersky Endpoint Security en dispositivos

Resultados

Una vez completado el escenario, Kaspersky Security Center se configura para actualizar las bases de datos de Kaspersky y las aplicaciones instaladas de Kaspersky después de que las actualizaciones se descargan en el repositorio del Servidor de administración o en los repositorios de los puntos de distribución. Después, puede proceder a monitorear el estado de la red.

Acerca de la actualización de las bases de datos, módulos de software y aplicaciones de Kaspersky

Para asegurarse de que la protección de sus Servidores de administración y dispositivos administrados esté actualizada, debe proporcionar actualizaciones oportunas de las siguientes:

- Bases de datos y módulos de software de Kaspersky

  Antes de descargar las bases de datos y los módulos de software de Kaspersky, Kaspersky Security Center comprueba si se puede acceder a los servidores de Kaspersky. Si no es posible acceder a los servidores mediante el DNS del sistema, la aplicación utiliza el DNS público. Esto es necesario para asegurarse de que las bases de datos antivirus estén actualizadas y se mantenga el nivel de seguridad para los dispositivos administrados.

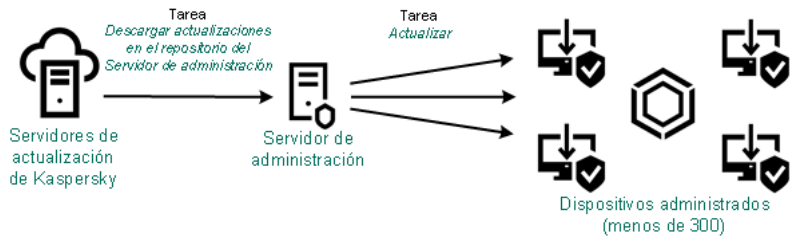
- Aplicaciones instaladas de Kaspersky, incluidos los componentes de Kaspersky Security Center y las aplicaciones de seguridad

Dependiendo de la configuración de su red, puede utilizar los siguientes esquemas de descarga y distribución de las actualizaciones necesarias para los dispositivos administrados:

- Mediante el uso de una sola tarea: *Descargar actualizaciones en el repositorio del Servidor de administración*
- Mediante el uso de dos tareas:
  - La tarea *Descargar actualizaciones en el repositorio del Servidor de administración*
  - La tarea *Descargar actualizaciones en los repositorios de puntos de distribución*
- Manualmente a través de una carpeta local, una carpeta compartida o un servidor FTP
- Directamente desde los servidores de actualización de Kaspersky a Kaspersky Endpoint Security para Windows en los dispositivos administrados

Uso de la tarea Descargar actualizaciones en el repositorio del Servidor de administración

En este esquema, Kaspersky Security Center descarga actualizaciones a través de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. En redes pequeñas que contienen menos de 300 dispositivos administrados en un solo segmento de red o menos de 10 dispositivos administrados en cada segmento de red, las actualizaciones se distribuyen a los dispositivos administrados directamente desde el repositorio del Servidor de administración (ver la siguiente figura).

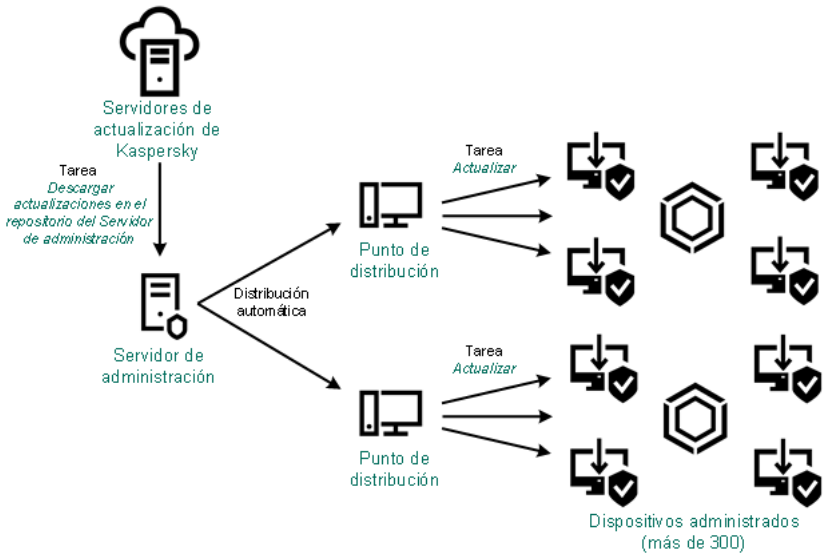


Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración sin puntos de distribución

De forma predeterminada, el Servidor de administración se comunica con los servidores de actualización de Kaspersky y descarga las actualizaciones utilizando el protocolo HTTPS. Puede configurar Servidor de administración para que utilice el protocolo HTTP en lugar del HTTPS.

Si su red contiene más de 300 dispositivos administrados en un solo segmento de red o si su red consta de varios segmentos de red con más de 9 dispositivos administrados en cada segmento de red, le recomendamos que utilice puntos de distribución para propagar las actualizaciones a los dispositivos administrados (ver la siguiente figura). Los puntos de distribución reducen la carga en el Servidor de administración y optimizan el tráfico entre el Servidor de administración y los dispositivos administrados. Puede calcular el número y la configuración de los puntos de distribución necesarios para su red.

En este esquema, las actualizaciones se descargan automáticamente del repositorio del Servidor de administración a los repositorios de los puntos de distribución. Los dispositivos administrados incluidos en la cobertura de un punto de distribución descargan las actualizaciones desde el repositorio del punto de distribución en lugar del repositorio del Servidor de administración.



Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración con puntos de distribución

Una vez que se complete la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las siguientes actualizaciones se descargan en el repositorio del Servidor de administración:

- Bases de datos y módulos de software de Kaspersky para Kaspersky Security Center

  Estas actualizaciones se instalan automáticamente.

- Bases de datos y módulos de software de Kaspersky para las aplicaciones de seguridad en los dispositivos administrados

  Estas actualizaciones se instalan a través de Actualizar tarea de Kaspersky Endpoint Security para Windows.

- Actualizaciones para el Servidor de administración

  Estas actualizaciones no se instalan automáticamente. El administrador debe aprobar y ejecutar explícitamente la instalación de las actualizaciones.

  Se requieren derechos de administrador local para instalar parches en el Servidor de administración.

- Actualizaciones para los componentes de Kaspersky Security Center

  De forma predeterminada, estas actualizaciones se instalan automáticamente. Puede cambiar la configuración en la directiva del Agente de red.

- Actualizaciones para las aplicaciones de seguridad

  De forma predeterminada, Kaspersky Endpoint Security para Windows instala solo las actualizaciones que usted apruebe. (Puede aprobar las actualizaciones a través de la consola de administración o a través de Kaspersky Security Center 14 Web Console). Las actualizaciones se instalan a través de la tarea Actualizar y se pueden configurar en las propiedades de esta tarea.

La tarea del Servidor de administración Descargar actualizaciones en el repositorio no está disponible en los Servidores de administración virtuales. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas en el Servidor de administración principal.

Puede configurar las actualizaciones para verificar su operatividad y errores en un conjunto de dispositivos de prueba. Si la verificación es exitosa, las actualizaciones se distribuyen a otros dispositivos administrados.

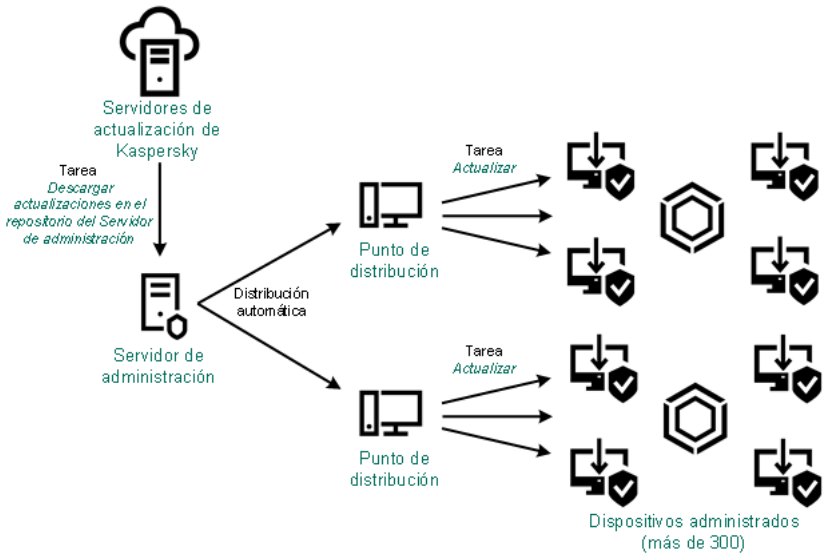
Cada aplicación de Kaspersky solicita actualizaciones requeridas del Servidor de administración. El Servidor de administración añade estas solicitudes y descarga solo aquellas actualizaciones que son solicitadas por cualquier aplicación. Esto garantiza que las mismas actualizaciones no se descarguen varias veces y que las actualizaciones innecesarias no se descarguen en absoluto. Cuando se ejecuta la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, el Servidor de administración envía la siguiente información a los servidores de actualización de Kaspersky automáticamente para garantizar la descarga de versiones relevantes de las bases de datos de Kaspersky y los módulos de software:

- Id. y versión de la aplicación
- ID de instalación de la aplicación
- Id. de clave activa
- Id. de ejecución de la tarea *Descargar actualizaciones al repositorio del Servidor de administración*

Ninguna información transmitida contiene datos personales u otros datos confidenciales. AO Kaspersky Lab protege la información de acuerdo con los requisitos establecidos por la ley.

Usando dos tareas: la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de puntos de distribución

Puede descargar actualizaciones a los repositorios de puntos de distribución directamente desde los servidores de actualizaciones de Kaspersky en lugar del repositorio del Servidor de administración y después distribuir las actualizaciones a los dispositivos administrados (consulte la siguiente figura). La descarga a los repositorios de puntos de distribución es preferible si el tráfico entre el Servidor de administración y los puntos de distribución es más costoso que el tráfico entre los puntos de distribución y los servidores de actualización de Kaspersky o si su Servidor de administración no tiene acceso a Internet.



Actualización utilizando la tarea Descargar actualizaciones en el repositorio del Servidor de administración y la tarea Descargar actualizaciones en los repositorios de puntos de distribución

De forma predeterminada, el Servidor de administración y los puntos de distribución se comunican con los servidores de actualización de Kaspersky y descargan las actualizaciones utilizando el protocolo HTTPS. Puede configurar el Servidor de administración y/o los puntos de distribución para utilizar el protocolo HTTP en lugar de HTTPS.

Para implementar este esquema, cree la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* además de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Después de esto, los puntos de distribución descargarán actualizaciones desde servidores de actualizaciones de Kaspersky y no desde el repositorio del Servidor de administración.

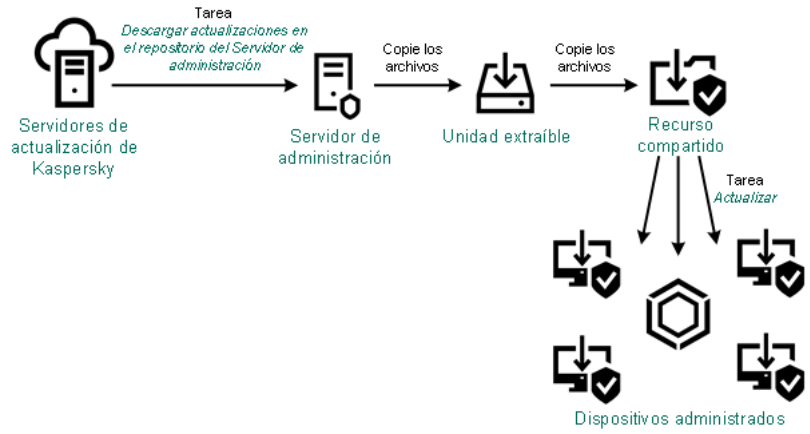
Los dispositivos de punto de distribución con macOS no pueden descargar actualizaciones de los servidores de actualización de Kaspersky.

Si uno o más dispositivos incluidos en la cobertura de la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* ejecutan macOS, la tarea se completa con el estado *Fallo*, incluso si se completa correctamente en todos los dispositivos de Windows.

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* también es necesaria para este esquema, ya que esta tarea se utiliza para descargar las bases de datos y los módulos de software de Kaspersky para Kaspersky Security Center.

Manualmente a través de una carpeta local, una carpeta compartida o un servidor FTP

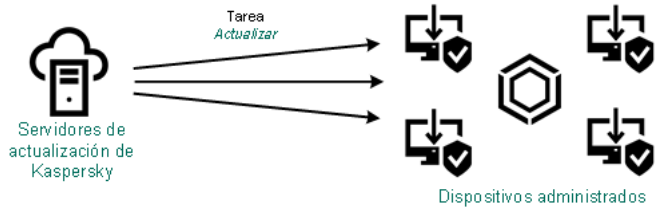
Si los dispositivos cliente no tienen una conexión con el Servidor de administración, puede usar una carpeta local o un recurso compartido como fuente para actualizar las bases de datos, módulos de software y aplicaciones de Kaspersky. En este esquema, debe copiar las actualizaciones requeridas desde el repositorio del Servidor de administración a una unidad extraíble, luego copiar las actualizaciones a la carpeta local o al recurso compartido especificado como origen de actualizaciones en la configuración de Kaspersky Endpoint Security para Windows (ver la siguiente figura).



Actualización a través de una carpeta local, una carpeta compartida o un servidor FTP

Directamente desde los servidores de actualización de Kaspersky a Kaspersky Endpoint Security para Windows en los dispositivos administrados

En los dispositivos administrados, puede configurar Kaspersky Endpoint Security para Windows para recibir actualizaciones directamente desde los servidores de actualización de Kaspersky (ver la siguiente figura).



Actualizar aplicaciones de seguridad directamente desde los servidores de actualización de Kaspersky

En este esquema, la aplicación de seguridad no utiliza los repositorios proporcionados por Kaspersky Security Center. Para recibir actualizaciones directamente de los servidores de actualización de Kaspersky, especifique los servidores de actualización de Kaspersky como origen de actualizaciones en la interfaz de la aplicación de seguridad. Para obtener una descripción completa de la configuración, consulte la documentación de Kaspersky Endpoint Security para Windows.

Creación de la tarea para descargar actualizaciones en el repositorio del Servidor de administración

La tarea *Descargar actualizaciones en el repositorio del Servidor de administración* del Servidor de administración se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Puede crear solo una tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. Por lo tanto, puede crear una tarea *Descargar actualizaciones en el repositorio del Servidor de administración* solo si esta tarea se eliminó de la lista de tareas del Servidor de administración.

Esta tarea es necesaria para descargar actualizaciones de los servidores de actualización de Kaspersky al repositorio del Servidor de administración. La lista de actualizaciones incluye:

- Actualizaciones de bases de datos y módulos de software para el Servidor de administración
- Actualizaciones de bases de datos y módulos de software para aplicaciones de seguridad de Kaspersky
- Actualizaciones a los componentes de Kaspersky Security Center
- Actualizaciones a las aplicaciones de seguridad de Kaspersky

Una vez que se descarguen las actualizaciones, se pueden propagar a los dispositivos administrados.

Antes de distribuir actualizaciones a los dispositivos administrados, puede ejecutar la tarea *Actualizar verificación*. Esto le permite asegurarse de que el Servidor de administración instalará las actualizaciones descargadas correctamente y que el nivel de seguridad no disminuirá debido a las actualizaciones. Para verificarlas antes de distribuirlas, configure la opción **Ejecutar verificación de actualizaciones** en la configuración de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

*Para crear la tarea **Descargar actualizaciones en el repositorio del Servidor de administración**:*

1. En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Descargar actualizaciones en el repositorio del Servidor de administración**.
4. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

6. Haga clic en el botón **Crear**.

   La tarea se crea y se muestra en la lista de tareas.

7. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

8. En la ventana de propiedades de la tarea, en la pestaña **Configuración de la aplicación**, especifique la siguiente configuración:

   - Orígenes de actualizaciones

     Los siguientes recursos pueden utilizarse como un origen de actualizaciones para el Servidor de administración:

     - Servidores de actualización de Kaspersky

       Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación. De forma predeterminada, el Servidor de administración se comunica con los servidores de actualización de Kaspersky y descarga las actualizaciones utilizando el protocolo HTTPS. Puede configurar Servidor de administración para que utilice el protocolo HTTP en lugar del HTTPS.

       Seleccionado de forma predeterminada.

     - Servidor de administración principal

       Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

     - Carpeta local o de red

       Una carpeta local o de red que contiene las últimas actualizaciones. Una carpeta de red puede ser un servidor FTP o HTTP o un recurso compartido SMB. Si una carpeta de red requiere autenticación, solo se admite el protocolo SMB. Cuando se selecciona una carpeta local, debe especificar una carpeta en un dispositivo que tenga el Servidor de administración instalado.

       > Un servidor FTP o HTTP o una carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura creada al usar los servidores de actualización de Kaspersky.

     Si activa la opción **No usar servidor proxy** para los orígenes de actualizaciones Servidores de actualización de Kaspersky o Carpeta local o de red, el Servidor de administración no utilizará un servidor proxy para descargar actualizaciones.

   - Carpeta para almacenar actualizaciones

     La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

   - Otros parámetros:

     - Forzar actualización en los Servidores de administración secundarios

Si esta opción está activada, el Servidor de administración inicia las tareas de actualización en los Servidores de administración secundarios tan pronto como se descargan nuevas actualizaciones. De lo contrario, las tareas de actualización en los Servidores de administración secundarios comienzan de acuerdo con sus programaciones.

Esta opción está desactivada de forma predeterminada.

- Copiar las actualizaciones descargadas en carpetas adicionales

  Una vez que el Servidor de administración recibe actualizaciones, las copia en las carpetas especificadas. Utilice esta opción si desea administrar de manera manual la distribución de actualizaciones en su red.

  Por ejemplo, puede querer usar esta opción en la siguiente situación: la red de su organización consta de varias subredes independientes y los dispositivos de cada una de las subredes no tienen acceso a otras subredes. Sin embargo, los dispositivos en todas las subredes tienen acceso a un recurso compartido de red común. En este caso, configura el Servidor de administración en una de las subredes para descargar actualizaciones de los servidores de actualización de Kaspersky, active esta opción y luego especifique este recurso compartido de red. En las actualizaciones descargadas de las tareas del repositorio para otros Servidores de administración, especifique el mismo recurso compartido de red que el origen de actualización.

  Esta opción está desactivada de forma predeterminada.

- No forzar la actualización de dispositivos y Servidores de administración secundarios a menos que se complete la copia

  Las tareas de descarga de actualizaciones a dispositivos cliente y Servidores de administración secundarios comienzan solo después de que esas actualizaciones se copien de la carpeta de actualización principal a carpetas de actualización adicionales.

  Esta opción debe estar activada si los dispositivos cliente y los Servidores de administración secundarios descargan actualizaciones de carpetas de red adicionales.

  Esta opción está desactivada de forma predeterminada.

- **Contenido de las actualizaciones**:

  - Descargar archivos de comparación

    Esta opción habilita la función de descarga de archivos diff.

    Esta opción está desactivada de forma predeterminada.

- Descargar actualizaciones utilizando el esquema anterior

A partir de la versión 14, Kaspersky Security Center descarga las actualizaciones de bases de datos y los módulos de software utilizando el nuevo esquema. Para que la aplicación descargue actualizaciones utilizando el nuevo esquema, el origen de actualización debe contener los archivos de actualización cuyos metadatos sean compatibles con el nuevo esquema. Si el origen de actualización contiene archivos de actualización cuyos metadatos son compatibles solo con el esquema anterior, active la **Descargar actualizaciones utilizando el esquema anterior** opción. De lo contrario, la tarea de descarga de la actualización no funcionará.

Por ejemplo, debe activar esta opción cuando se especifica una carpeta local o de red como fuente de actualización y los archivos de actualización en esta carpeta fueron descargados por una de las siguientes aplicaciones:

- Utilidad Kaspersky Update

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13.2 o una versión anterior

  Por ejemplo, su Servidor de administración 1 no tiene conexión a Internet. En este caso, puede descargar actualizaciones utilizando un Servidor de administración 2 que tenga conexión a Internet y luego colocar las actualizaciones en una carpeta local o de red para usarlas como fuente de actualización para el Servidor de administración 1. Si el Servidor de administración 2 tiene la versión 13.2 o anterior, active la **Descargar actualizaciones utilizando el esquema anterior** opción en la tarea para el Servidor de administración 1.

Esta opción está desactivada de forma predeterminada.

- **Ejecutar verificación de actualizaciones**

  El Servidor de administración descarga las actualizaciones desde el origen, las guarda en un repositorio temporal y ejecuta la tarea definida en el campo **Tarea de verificación de actualizaciones**. Si la tarea se completa con éxito, las actualizaciones se copian desde el repositorio temporal a una carpeta compartida en el Servidor de administración y luego se distribuyen a todos los dispositivos para los cuales el Servidor de administración actúa como fuente de actualizaciones (tareas con el tipo de programación **Cuando se descargan nuevas actualizaciones en el repositorio** empezada). La tarea de descargar actualizaciones al repositorio se termina solo después de completar la tarea *Verificación de actualizaciones*.

  Esta opción está desactivada de forma predeterminada.

1. En la ventana de propiedades de la tarea, en la pestaña **Programación**, cree una programación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

   - **Inicio programado:**

     Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

     - **Manualmente**

       La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

       Esta opción está activada de forma predeterminada.

     - **Cada N minutos**

La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

- **Cada N horas**

  La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

  De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

- **Cada N días**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

  De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

- **Cada N semanas**

  La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

  De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- **Diario (no compatible con horario de verano)**

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- **Semanalmente**

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- **Por días de la semana**

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- **Mensualmente**

La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

En los meses que faltan el día especificado, la tarea se ejecuta el último día.

De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- Cada mes, en días concretos de las semanas seleccionadas

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- En Brote de virus

  La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

  - Antivirus para estaciones de trabajo y servidores de archivos
  - Antivirus para la protección del perímetro
  - Antivirus para sistemas de correo

  De forma predeterminada, están seleccionados todos los tipos de aplicación.

  Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- Al completar otra tarea

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- Ejecutar tareas no realizadas

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- Usar el retraso aleatorio automáticamente para el inicio de tareas

Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)

  Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

  Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

2. Haga clic en el botón **Guardar**.

   La tarea se crea y se configura.

Cuando un Servidor de administración realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las actualizaciones de las bases de datos y módulos de software se descargan del origen de actualizaciones y se almacenan en la carpeta compartida de un Servidor de administración. Si crea esta tarea para un grupo de administración, solo se aplicará a los Agentes de red incluidos en el grupo de administración especificado.

Las actualizaciones se distribuyen en los dispositivos cliente y en los Servidores de administración secundarios desde la carpeta compartida del Servidor de administración.

Visualización de actualizaciones descargadas

Cuando un Servidor de administración realiza la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, las actualizaciones de las bases de datos y módulos de software se descargan del origen de actualizaciones y se almacenan en la carpeta compartida de un Servidor de administración. Puede ver las actualizaciones descargadas en la sección **ACTUALIZACIONES DE MÓDULOS DE SOFTWARE Y BASES DE DATOS DE KASPERSKY**.

Para ver la lista de actualizaciones descargadas,

En el menú principal, vaya a **OPERACIONES → APLICACIONES DE KASPERSKY → ACTUALIZACIONES DE MÓDULOS DE SOFTWARE Y BASES DE DATOS DE KASPERSKY**.

Aparece una lista de actualizaciones disponibles.

Verificación de las actualizaciones descargadas

Antes de instalar actualizaciones en los dispositivos administrados, primero puede verificar si las actualizaciones son operativas y los errores a través de la tarea de *Verificación de actualizaciones*. La tarea *Verificación de actualizaciones* se realiza automáticamente como parte de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*. El Servidor de administración descarga las actualizaciones del origen, las guarda en el repositorio temporal y ejecuta la tarea de *verificación de actualizaciones*. Si la tarea termina correctamente, las actualizaciones se copiarán del repositorio temporal a la carpeta compartida del Servidor de administración. Se distribuirán a todos los dispositivos cliente que tengan como origen de actualizaciones ese mismo Servidor de administración.

Si, como resultado de la tarea *Verificación de actualizaciones*, se muestra que las actualizaciones ubicadas en el repositorio temporal son incorrectas o si la tarea *Verificación de actualizaciones* se ha completado con errores, las actualizaciones de este tipo no se copiarán a la carpeta compartida. El Servidor de administración guardará el conjunto de actualizaciones anterior. Además, las tareas que tienen el tipo de programación **Cuando se descargan nuevas actualizaciones en el repositorio** no se inician. Si el análisis de las nuevas actualizaciones se realiza con éxito, dichas operaciones se realizarán en el siguiente inicio de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

Se considerará que un conjunto de actualizaciones es incorrecto si se cumple una de las siguientes condiciones en al menos un dispositivo de prueba:

- Se produjo un error en la tarea de actualización.
- El estado de protección en tiempo real de la aplicación de seguridad ha cambiado después de aplicarse las actualizaciones.
- Se ha detectado un objeto infectado mientras se ejecutaba la tarea de análisis a petición.
- Se ha producido un error en el tiempo de ejecución de una aplicación Kaspersky.

Si ninguna de las condiciones indicadas es verdadera para ningún dispositivo de prueba, se considerará que el conjunto de actualizaciones es válido y que la tarea *Verificación de actualizaciones* ha finalizado correctamente.

Antes de empezar a crear la tarea *Verificación de actualizaciones*, realice los requisitos previos:

1. Cree un grupo de administración con varios dispositivos de prueba. Necesitará este grupo para verificar las actualizaciones.

   Recomendamos utilizar los dispositivos con la protección más fiable y con la configuración de aplicaciones más común en la red. Este enfoque aumenta la calidad y la probabilidad de detección de virus durante los análisis y reduce al mínimo el riesgo de falsos positivos. Si se detectan virus en los dispositivos cliente, se considerará que la tarea *Verificación de actualizaciones* no se ha realizado correctamente.

2. Cree las tareas de actualización y análisis de virus para una aplicación compatible con Kaspersky Security Center, por ejemplo, Kaspersky Endpoint Security for Windows o Kaspersky Security for Windows Server. Al crear las tareas de actualización y análisis de virus, especifique el grupo de administración con los dispositivos de prueba.

   La tare *Actualizar verificación* ejecuta secuencialmente las tareas de actualización y análisis de virus en los dispositivos de prueba para verificar que todas las actualizaciones sean válidas. Además, al crear la tarea *Actualizar verificación* debe especificar las tareas de actualización y análisis de virus.

3. Cree la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

Para que Kaspersky Security Center verifique las actualizaciones descargadas antes de distribuirlas a los dispositivos cliente:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en la tarea**Descargar actualizaciones en el repositorio del Servidor de administración**.
3. En la ventana de propiedades de la tarea que se abre, seleccione la pestaña **Configuración de la aplicación** y después active la opción **Ejecutar verificación de actualizaciones**.
4. Si la tarea *Verificar actualizaciones* existe, haga clic en el botón **Elija una tarea**. En la ventana que se abre, seleccione la tarea *Verificar actualizaciones* en el grupo de administración con dispositivos de prueba.
5. Si no creó la tarea *Verificar actualizaciones* anteriormente, haga lo siguiente:
   a. Haga clic en el botón **Nueva tarea**.
   b. En el Asistente para añadir tareas que se abre, especifique el nombre de la tarea si desea cambiar el nombre predeterminado.
   c. Seleccione el grupo de administración con dispositivos de prueba que creó anteriormente.
   d. Primero, seleccione la tarea de actualización de una aplicación requerida compatible con Kaspersky Security Center y luego seleccione la tarea de análisis de virus.
      Después de eso, aparecerán las siguientes opciones. Recomendamos dejarlos activados:
      - **Reiniciar dispositivo después de actualizar las bases de datos**
        Después de actualizar las bases de datos antivirus en un dispositivo, recomendamos reiniciar el dispositivo.
        La opción está activada de forma predeterminada.
      - **Comprobar el estado de la protección en tiempo real tras la actualización de las bases de datos y el reinicio del dispositivo**
        Si esta opción está activada, la tarea *Verificación de actualizaciones* comprueba si las actualizaciones descargadas en el repositorio del Servidor de administración son válidas y si el nivel de protección ha disminuido después de la actualización de la base de datos antivirus y el reinicio del dispositivo.
        Esta opción está activada de forma predeterminada.
   e. Especifique una cuenta desde la cual se ejecutará la tare *Verificación de actualizaciones*. Puede usar su cuenta y dejar activada la opción **Cuenta predeterminada**. Como alternativa, puede especificar que la tarea se ejecute con otra cuenta que tenga los derechos de acceso necesarios. Para ello, seleccione la opción **Especificar cuenta** y luego ingrese las credenciales de esa cuenta.
6. Haga clic en **Guardar** para cerrar la ventana de propiedades de la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*.

La verificación de actualización automática está habilitada. Ahora puede ejecutar la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, que comenzará desde la verificación de actualización.

Creación de la tarea para descargar actualizaciones a los repositorios de los puntos de distribución

La tarea *Descargar actualizaciones en los repositorios de puntos de distribución* solo funciona en dispositivos de punto de distribución que ejecutan Windows. Los dispositivos de punto de distribución con Linux o macOS no pueden descargar actualizaciones de los servidores de actualización de Kaspersky. Si al menos un dispositivo de los que se incluyen en la cobertura de la tarea ejecuta Linux o macOS, dicha tarea mostrará el estado *Fallo*. Incluso si la tarea se completa correctamente en todos los dispositivos de Windows, generará un error en el resto de los dispositivos.

Puede crear la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* para un grupo de administración. Esta tarea se ejecutará para puntos de distribución incluidos en el grupo de administración especificado.

Puede usar esta tarea, por ejemplo, si el tráfico entre el Servidor de administración y los puntos de distribución es más costoso que el tráfico entre los puntos de distribución y los servidores de actualización de Kaspersky o si su Servidor de administración no tiene acceso a Internet.

Esta tarea es necesaria para descargar actualizaciones de los servidores de actualización de Kaspersky a los repositorios de los puntos de distribución. La lista de actualizaciones incluye:

- Actualizaciones de bases de datos y módulos de software para aplicaciones de seguridad de Kaspersky
- Actualizaciones a los componentes de Kaspersky Security Center
- Actualizaciones a las aplicaciones de seguridad de Kaspersky

Una vez que se descarguen las actualizaciones, se pueden propagar a los dispositivos administrados.

*Para crear la tarea **Descargar actualizaciones en los repositorios de puntos de distribución,** para un grupo de administración seleccionado:*

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en el botón **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione **Descargar actualizaciones en los repositorios de puntos de distribución** en el campo **Tipo de tarea**.
4. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Pulse el botón de opción para especificar el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplica la tarea.
6. En el paso **Finalizar la creación de tareas** paso, si desea modificar la configuración predeterminada de la tarea, active la opción **Abrir los detalles de la tarea cuando se complete la creación**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.
7. Haga clic en el botón **Crear**.

La tarea se crea y se muestra en la lista de tareas.

8. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

9. En la ficha **Configuración de la aplicación** de la ventana de propiedades de la tarea, especifique la siguiente configuración:

- **Orígenes de actualizaciones**

  Los recursos siguientes pueden utilizarse como origen de actualizaciones para el punto de distribución:

  - Servidores de actualización de Kaspersky

    Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación.

    Esta opción está seleccionada de forma predeterminada.

  - Servidor de administración principal

    Este recurso se aplica a las tareas creadas para un Servidor de administración secundario o virtual.

  - Carpeta local o de red

    Una carpeta local o de red que contiene las últimas actualizaciones. Una carpeta de red puede ser un servidor FTP o HTTP o un recurso compartido SMB. Si una carpeta de red requiere autenticación, solo se admite el protocolo SMB. Cuando se selecciona una carpeta local, debe especificar una carpeta en un dispositivo que tenga el Servidor de administración instalado.

    > Un servidor FTP o HTTP o una carpeta de red utilizada por un origen de actualizaciones debe contener una estructura de carpetas (con actualizaciones) que coincida con la estructura creada al usar los servidores de actualización de Kaspersky.

  Si activa la opción **No usar servidor proxy** para los orígenes de actualización Servidores de actualización de Kaspersky o Carpeta local o de red, un punto de distribución no usa un servidor proxy para descargar actualizaciones, incluso si ha activado la opción **Usar servidor proxy** la configuración de la directiva del Agente de red para el punto de distribución.

- **Carpeta para almacenar actualizaciones**

  La ruta a la carpeta especificada para almacenar las actualizaciones guardadas. Puede copiar la ruta de la carpeta especificada en el portapapeles. No puede cambiar la ruta a una carpeta específica para una tarea de grupo.

- **Descargar archivos de comparación**

  Esta opción habilita la función de descarga de archivos diff.

  Esta opción está desactivada de forma predeterminada.

- **Descargar actualizaciones utilizando el esquema anterior**

A partir de la versión 14, Kaspersky Security Center descarga las actualizaciones de bases de datos y los módulos de software utilizando el nuevo esquema. Para que la aplicación descargue actualizaciones utilizando el nuevo esquema, el origen de actualización debe contener los archivos de actualización cuyos metadatos sean compatibles con el nuevo esquema. Si el origen de actualización contiene archivos de actualización cuyos metadatos son compatibles solo con el esquema anterior, active la **Descargar actualizaciones utilizando el esquema anterior** opción. De lo contrario, la tarea de descarga de la actualización no funcionará.

Por ejemplo, debe activar esta opción cuando se especifica una carpeta local o de red como fuente de actualización y los archivos de actualización en esta carpeta fueron descargados por una de las siguientes aplicaciones:

- Utilidad Kaspersky Update

  Esta utilidad descarga actualizaciones utilizando el esquema antiguo.

- Kaspersky Security Center 13.2 o una versión anterior

  Por ejemplo, un punto de distribución está configurado para tomar las actualizaciones de una carpeta local o de red. En este caso, puede descargar actualizaciones utilizando un Servidor de administración que tenga conexión a Internet y luego colocar las actualizaciones en la carpeta local en el punto de distribución. Si el Servidor de administración tiene la versión 13.2 o anterior, active la opción **Descargar actualizaciones utilizando el esquema anterior** en la tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*.

Esta opción está desactivada de forma predeterminada.

10. Crear una planificación para el inicio de la tarea. Si es necesario, especifique la siguiente configuración:

- Inicio programado

  Seleccione la programación según la cual se ejecuta la tarea y configure la programación seleccionada.

  - Manualmente

    La tarea no se ejecuta automáticamente. Solo lo puede iniciar de forma manual.

    Esta opción está activada de forma predeterminada.

  - Cada N minutos

    La tarea se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la hora especificada en el día en que se crea la tarea.

    De forma predeterminada, la tarea se ejecuta cada 30 minutos, a partir de la hora actuales del sistema.

  - Cada N horas

    La tarea se ejecuta regularmente, con el intervalo especificado en horas, a partir de la fecha y hora especificadas.

    De forma predeterminada, la tarea se ejecuta cada seis horas, a partir de la fecha y hora actuales del sistema.

  - Cada N días

La tarea se ejecuta regularmente, con el intervalo especificado en días. Además, puede especificar una fecha y hora de la primera tarea ejecutada. Estas opciones adicionales estarán disponibles si son compatibles con la aplicación para la que crea la tarea.

De forma predeterminada, la tarea se ejecuta cada día, a partir de la fecha y hora actuales del sistema.

- Cada N semanas

  La tarea se ejecuta regularmente, con el intervalo especificado en semanas, en el día especificado de la semana y en el tiempo especificado.

  De forma predeterminada, la tarea se ejecuta todos los lunes a la hora actual del sistema.

- Diario (no compatible con horario de verano)

  La tarea se ejecuta regularmente, con el intervalo especificado en días. Este programa no admite el cumplimiento del horario de verano (DST). Esto significa que cuando los relojes saltan una hora hacia adelante o hacia atrás al comienzo o al final del horario de verano, la hora de inicio de la tarea actual no cambia.

  No recomendamos que utilice este horario. Es necesario para la compatibilidad con versiones anteriores de Kaspersky Security Center.

  De forma predeterminada, la tarea se ejecuta cada día a la hora actual del sistema.

- Semanalmente

  La tarea se ejecuta cada semana en el día especificado y a la hora especificada.

- Por días de la semana

  La tarea se ejecuta regularmente, en el día de la semana especificado y a la hora especificada.

  De forma predeterminada, la tarea se ejecuta todos los viernes a las 18:00:00 h.

- Mensualmente

  La tarea se ejecuta regularmente, en el día del mes especificado y a la hora especificada.

  En los meses que faltan el día especificado, la tarea se ejecuta el último día.

  De forma predeterminada, la tarea se ejecuta el primer día de cada mes, a la hora actual del sistema.

- Cada mes, en días concretos de las semanas seleccionadas

  La tarea se ejecuta regularmente, en el día de cada mes especificado y a la hora especificada.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 18:00:00 h.

- Al detectar un foco de virus

La tarea se ejecuta después de que se produzca un evento de *Brote de virus*. Seleccione los tipos de aplicaciones que supervisarán los brotes de virus. Los siguientes tipos de aplicación están disponibles:

- Antivirus para estaciones de trabajo y servidores de archivos
- Antivirus para la protección del perímetro
- Antivirus para sistemas de correo

De forma predeterminada, están seleccionados todos los tipos de aplicación.

Es posible que desee ejecutar diferentes tareas según el tipo de aplicación antivirus que informe sobre un brote de virus. En este caso, elimine la selección de los tipos de aplicaciones que no necesita.

- **Al completar otra tarea**

  La tarea actual se inicia después de que se complete otra tarea. Puede seleccionar cómo debe completarse la tarea anterior (satisfactoriamente o con errores) para activar el inicio de la tarea actual. Por ejemplo, es posible que desee ejecutar la tarea de administración de dispositivos con la opción **Encender dispositivo** y, una vez que se complete, ejecutar la tarea de análisis antivirus.

- **Ejecutar tareas no realizadas**

  Esta opción determina el comportamiento de una tarea si un dispositivo cliente no está visible en la red cuando la tarea vaya a comenzar.

  Si esta opción está activada, el sistema intentará iniciar la tarea la próxima vez que la aplicación Kaspersky se ejecute en un dispositivo cliente. Si la programación de la tarea es **Manualmente**, **Una vez** o **Inmediatamente**, la tarea se inicia inmediatamente después de que el dispositivo se haga visible en la red o inmediatamente después de que el dispositivo se incluya en la cobertura de la tarea.

  Si esta opción está desactivada, solo se ejecutarán en dispositivos cliente las tareas programadas; para **Manualmente**, **Una vez** e **Inmediatamente**, las tareas solo se ejecutarán en aquellos dispositivos cliente que estén visibles en la red. Por ejemplo, es posible que desee desactivar esta opción para una tarea que consuma recursos que desee ejecutar solo fuera del horario comercial.

  Esta opción está activada de forma predeterminada.

- **Usar el retraso aleatorio automáticamente para el inicio de tareas**

  Si esta opción está activada, la tarea se inicia aleatoriamente en los dispositivos cliente, dentro del intervalo de tiempo especificado, es decir, se trata de un *inicio distribuido de tarea*. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

  La hora de inicio distribuido se calcula automáticamente cuando se crea una tarea según el número de dispositivos cliente a los que se la asigna. Más tarde, la tarea se inicia siempre a la hora de inicio calculada. Sin embargo, cuando la configuración de la tarea se edita o la tarea se inicia de forma manual, el valor calculado de la hora de inicio de la tarea cambia.

  Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

- **Usar el retraso aleatorio para el inicio de tareas con un intervalo de (min)**

Si esta opción está activada, la tarea se inicia en los dispositivos cliente aleatoriamente dentro del intervalo de tiempo especificado. El inicio distribuido de tareas ayuda a evitar que los dispositivos cliente hagan una elevada cantidad de peticiones simultáneas al Servidor de administración cuando se inicia una tarea programada.

Si esta opción está desactivada, la tarea se inicia en los dispositivos cliente de acuerdo con la programación.

Esta opción está desactivada de forma predeterminada. El intervalo de tiempo predeterminado es de un minuto.

11. Haga clic en el botón **Guardar**.

    La tarea se crea y se configura.

    Además de la configuración que especifique durante la creación de la tarea, puede cambiar otras propiedades de una tarea creada.

Cuando se realiza la tarea *Descargar actualizaciones en los repositorios de puntos de distribución*, las actualizaciones para bases de datos y módulos del software se descargan desde el origen de actualizaciones y se almacenan en la carpeta compartida. Las actualizaciones descargadas solo se utilizarán por puntos de distribución que se incluyen en el grupo de administración especificado y que no tienen una tarea de descarga de actualización explícitamente definida para ellos.

Habilitación y deshabilitación de actualizaciones automáticas y parches para componentes de Kaspersky Security Center

Las actualizaciones y los parches para el Servidor de administración solo se pueden instalar manualmente, después de obtener la aprobación explícita del administrador.

La instalación automática de actualizaciones y parches para componentes de Kaspersky Security Center está habilitada de forma predeterminada durante la instalación del Agente de red en el dispositivo. Puede deshabilitarla durante la instalación del Agente de red o más adelante usando una directiva.

Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center durante instalación local del Agente de red en un dispositivo, realice lo siguiente:

1. Inicie la instalación local del Agente de red en el dispositivo.

2. En el paso **Configuración avanzada**, desactive la casilla **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir**.

3. Siga las instrucciones del Asistente.

   Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center deshabilitados en el dispositivo. Puede habilitar la actualización automática y los parches más adelante usando una directiva.

Para deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center durante la instalación del Agente de red en el dispositivo mediante un paquete de instalación, realice lo siguiente:

1. En el menú principal, vaya a **OPERACIONES → REPOSITORIOS → PAQUETES DE INSTALACIÓN**.
2. Haga clic en el paquete **Agente de red de Kaspersky Security Center <número de versión>**.
3. En la ventana de propiedades, vaya a la pestaña **Configuración**.
4. Desactive el botón de activación **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir**.

   Se instalará el Agente de red con la actualización automática y los parches para componentes de Kaspersky Security Center deshabilitados de este paquete. Puede habilitar la actualización automática y los parches más adelante usando una directiva.

Si esta casilla se seleccionó (o se desactivó) durante la instalación del Agente de red en el dispositivo, puede habilitar posteriormente (o deshabilitar) la actualización automática usando la directiva del Agente de red.

Para habilitar o deshabilitar la actualización automática y los parches para componentes de Kaspersky Security Center usando la directiva del Agente de red, realice lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en la directiva del Agente de red.
3. En la ventana de propiedades de la directiva, abra la pestaña **Configuración de la aplicación**.
4. En la sección **Administrar parches y actualizaciones**, cambie la posición del botón de activación **Instalar automáticamente actualizaciones y parches aplicables para componentes que tienen el estado Sin definir** para activar o desactivar las actualizaciones y los parches automáticos.
5. Configure el bloqueo (🔒) para esta casilla.

   La directiva se aplicará a los dispositivos seleccionados y la actualización automática y los parches para los componentes de Kaspersky Security Center se habilitarán (o se deshabilitarán) en estos dispositivos.

Instalación automática de actualizaciones para Kaspersky Endpoint Security para Windows

Puede configurar las actualizaciones automáticas de bases de datos y módulos de software de Kaspersky Endpoint Security para Windows en los dispositivos cliente.

Para configurar la descarga y la instalación automática de actualizaciones de Kaspersky Endpoint Security para Windows en dispositivos cliente:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en el botón **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para Kaspersky Endpoint Security para Windows, seleccione **Actualizar** como el subtipo de la tarea.
4. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).

5. Elija la cobertura de la tarea.

6. Especifique el grupo de administración, la selección de dispositivos o los dispositivos a los que se aplica la tarea.

7. En el paso **Finalizar la creación de tareas** paso, si desea modificar la configuración predeterminada de la tarea, active la opción **Abrir los detalles de la tarea cuando se complete la creación**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

8. Haga clic en el botón **Crear**.

   La tarea se crea y se muestra en la lista de tareas.

9. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

10. En la pestaña **Configuración de la aplicación** de la ventana de propiedades de la tarea, defina la configuración de la tarea de actualización en el modo local o móvil:

    - **Modo local**: La conexión está establecida entre el dispositivo y el Servidor de administración.

    - **Modo móvil**: No se establece conexión entre Kaspersky Security Center y el dispositivo (por ejemplo, cuando el dispositivo no está conectado a Internet).

11. Habilite los orígenes de actualizaciones que desee usar para actualizar las bases de datos y los módulos de aplicación para Kaspersky Endpoint Security para Windows. Si es necesario, cambie las posiciones de las fuentes en la lista usando los botones **Subir** y **Bajar**. Si se habilitan varios orígenes de actualizaciones, Kaspersky Endpoint Security para Windows intenta conectarse a ellos uno tras otro, comenzando desde el principio de la lista y realiza la tarea de actualización recuperando el paquete de actualización del primer origen disponible.

12. Habilite la opción **Instalar actualizaciones del módulo de aplicación aprobadas** para descargar e instalar actualizaciones de módulo del software junto con las bases de datos de la aplicación.

    Si esta opción está activada, Kaspersky Endpoint Security para Windows informa al usuario de que existen actualizaciones del módulo de software disponibles y las incluye en el paquete de actualización cuando se ejecuta la tarea correspondiente. Kaspersky Endpoint Security para Windows instala solo aquellas actualizaciones para las cuales ha establecido el estado *Aprobado*; se instalarán localmente a través de la interfaz de la aplicación o de Kaspersky Security Center.

    También puede habilitar la opción **Instalar automáticamente las actualizaciones del módulo de aplicaciones críticas**. Si hay actualizaciones disponibles para los módulos de software, Kaspersky Endpoint Security para Windows instala automáticamente aquellos que tienen un estado *Crítico*; las actualizaciones restantes se instalarán después de que las apruebe.

    Si actualizar el módulo de software requiere revisar y aceptar las condiciones del Contrato de licencia y la Política de privacidad, la aplicación instala las actualizaciones una vez que el usuario ha aceptado las condiciones del Contrato de licencia y la Política de privacidad.

13. Seleccione la casilla de verificación **Copiar actualizaciones en una carpeta** para que la aplicación guarde las actualizaciones descargadas en una carpeta y luego especifique la ruta de la carpeta.

14. Programe la tarea. Para garantizar actualizaciones oportunas, le recomendamos que seleccione la opción **Cuando se descarguen nuevas actualizaciones en el repositorio**.

15. Haga clic en **Guardar**.

Al ejecutar la tarea **Actualizar**, la aplicación envía solicitudes a los servidores de actualización de Kaspersky.

Algunas actualizaciones requieren la instalación de las últimas versiones de complementos de administración.

Aprobar y rechazar actualizaciones de software

La configuración de una tarea de instalación de actualizaciones puede requerir la aprobación de las actualizaciones que se van a instalar. Puede aprobar las actualizaciones que deben instalarse y rechazar las actualizaciones que no deben instalarse.

Por ejemplo, es posible que desee verificar primero la instalación de actualizaciones en un entorno de prueba y asegurarse de que no interfieran con el funcionamiento de los dispositivos y solo entonces permitir la instalación de estas actualizaciones en los dispositivos cliente.

Aprobar o rechazar una o varias actualizaciones:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE KASPERSKY** y, en la lista desplegable, seleccione **ACTUALIZACIONES SIN INTERRUPCIONES**.

   Aparece una lista de actualizaciones disponibles.

   Las actualizaciones de aplicaciones administradas pueden requerir la instalación de una versión mínima específica de Kaspersky Security Center. Si esta versión es posterior a su versión actual, estas actualizaciones se muestran pero no se pueden aprobar. Además, no se pueden crear paquetes de instalación a partir de dichas actualizaciones hasta que actualice Kaspersky Security Center. Se le solicitará que actualice su instancia de Kaspersky Security Center a la versión mínima requerida.

2. Seleccione las actualizaciones que desea aprobar o rechazar.

3. Haga clic en **Aprobar** para aprobar las actualizaciones seleccionadas o **Rechazar** para rechazar las actualizaciones seleccionadas.

   El valor predeterminado es *Sin definir*.

Las actualizaciones para las que se asigna el estado *Aprobado* se colocan en una cola para la instalación.

Las actualizaciones para las cuales asigne el estado *Rechazada* se desinstalarán (si es posible) de todos los dispositivos en los cuales se instalaron anteriormente. Además, no se instalarán en otros dispositivos en el futuro.

Algunas actualizaciones para aplicaciones de Kaspersky no pueden desinstalarse. Si configura el estado *Rechazada* para ellas, Kaspersky Security Center no desinstalará estas actualizaciones de los dispositivos en los cuales se hayan instalado anteriormente. Sin embargo, estas actualizaciones nunca se instalarán en otros dispositivos en el futuro.

Si configura el estado *Rechazada* para las actualizaciones de software de terceros, estas actualizaciones no se instalarán en los dispositivos cuya instalación se haya planeado pero aún no se haya realizado. Las actualizares permanecerán en los dispositivos en los cuales ya se hayan instalado. Si debe eliminar las actualizaciones, puede eliminarlas manualmente en forma local.

Actualización del Servidor de administración

Puede instalar actualizaciones del Servidor de administración mediante el Asistente de actualización del Servidor de administración.

Para instalar una actualización del Servidor de administración:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE KASPERSKY → ACTUALIZACIONES SIN INTERRUPCIONES**.

2. Ejecute Asistente de actualización del Servidor de administración mediante alguno de los siguientes métodos:

   - Haga clic en el nombre de una actualización del Servidor de administración en la lista de actualizaciones y, en la ventana que se abre, haga clic en el enlace **Ejecutar el Asistente de actualización del Servidor de administración**.

   - Haga clic en el enlace **Ejecutar el Asistente de actualización del Servidor de administración** en el campo de notificación en la parte superior de la ventana.

3. En la ventana Asistente de actualización del Servidor de administración, seleccione una de las siguientes opciones para especificar cuándo instalar una actualización:

   - **Instalar ahora**. Seleccione esta opción si desea instalar la actualización ahora.

   - **Posponer la instalación**. Seleccione esta opción si desea instalar la actualización más tarde. En este caso, se mostrará una notificación sobre esta actualización.

   - **Ignorar actualización**. Seleccione esta opción si no desea instalar una actualización y no desea recibir notificaciones sobre esta actualización.

4. Selecciona la opción **Crear copia de seguridad de Servidor de administración antes de la instalación de la actualización** si desea crear una copia de seguridad del Servidor de Administración antes de instalar la actualización.

5. Haga clic en el botón **Aceptar** para finalizar el Asistente.

Si se interrumpe el proceso de copia de seguridad, también se interrumpe el proceso de instalación de la actualización.

Activación y desactivación del modelo de descarga de actualizaciones sin conexión

Recomendamos que evite deshabilitar el modelo de descarga de actualizaciones sin conexión. Desactivarlo puede causar fallos en la entrega de actualización a dispositivos. En ciertos casos, un especialista del Servicio de soporte técnico de Kaspersky puede recomendar que desactive la opción **Descargar por adelantado actualizaciones y bases de datos antivirus desde el Servidor de administración**. Luego, se tendrá que asegurar de que se haya configurado la tarea para recibir actualizaciones para aplicaciones de Kaspersky.

Para habilitar o deshabilitar el modelo de descarga de actualizaciones sin conexión para un grupo de administración:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en **Grupos**.
3. En la estructura del grupo de administración, seleccione el grupo de administración para el que desea configurar el modelo de descarga de actualizaciones sin conexión.
4. Haga clic en la directiva del Agente de red.

   Se abre la ventana de propiedades de la directiva del Agente de red.

   > De forma predeterminada, la configuración de las directivas secundarias se hereda de las directivas principales y no se puede modificar. Si la directiva que desea modificar se hereda, primero debe crear una nueva directiva para el Agente de red en el grupo de administración correspondiente. En la directiva recién creada, podrá modificar las opciones de configuración que no estén bloqueadas en la directiva principal.

5. En la pestaña **Configuración de la aplicación**, seleccione la sección **Administrar parches y actualizaciones**.
6. Active o desactive la opción **Descargar actualizaciones y bases de datos antivirus del Servidor de administración (recomendado)** para activar o desactivar, respectivamente, el modelo de descarga de actualizaciones sin conexión.

   De forma predeterminada, el modelo de descarga de actualizaciones sin conexión está habilitado.

Se habilitará o deshabilitará el modelo de descarga de actualizaciones sin conexión.

Actualización de las bases de datos y módulos de software de Kaspersky en dispositivos desconectados

Actualizar las bases de datos y los módulos de software de Kaspersky en dispositivos administrados es una tarea importante para mantener la protección de los dispositivos contra virus y otras amenazas. Los administradores generalmente configuran actualizaciones regulares mediante el uso del repositorio del Servidor de administración o repositorios de puntos de distribución.

Cuando necesite actualizar las bases de datos y los módulos de software en un dispositivo (o un grupo de dispositivos) que no esté conectado al Servidor de administración (principal o secundario), a un punto de distribución o a Internet, tiene que usar fuentes alternativas de actualizaciones, como un servidor FTP o una carpeta local. En este caso, debe enviar los archivos de las actualizaciones necesarias mediante un dispositivo de almacenamiento masivo, como una unidad flash o un disco duro externo.

Puede copiar las actualizaciones requeridas desde:

- Servidor de administración.

  Para asegurarse de que el repositorio del Servidor de administración contenga las actualizaciones necesarias para la aplicación de seguridad instalada en un dispositivo desconectado, al menos uno de los dispositivos en línea administrados debe tener la misma aplicación de seguridad instalada. Esta aplicación debe estar configurada para recibir las actualizaciones desde el repositorio del Servidor de administración mediante la tarea Descargar actualizaciones en el repositorio del Servidor de administración.

- Cualquier dispositivo que tenga la misma aplicación de seguridad instalada y configurada para recibir las actualizaciones desde el repositorio del Servidor de administración, un repositorio de puntos de distribución o directamente desde los servidores de actualización de Kaspersky.

A continuación se muestra un ejemplo de configuración de actualizaciones de bases de datos y módulos de software al copiarlos desde el repositorio del Servidor de administración.

Para actualizar las bases de datos y módulos de software de Kaspersky en dispositivos desconectados

1. Conecte la unidad extraíble al dispositivo donde está instalado el Servidor de administración.

2. Copie los archivos de las actualizaciones en la unidad extraíble.

   De forma predeterminada, las actualizaciones se localizan en: \\<nombre del servidor>\KLSHARE\Updates.

   O bien, puede configurar Kaspersky Security Center para copiar regularmente las actualizaciones a la carpeta que seleccione. Para este propósito, utilice la opción **Copiar las actualizaciones descargadas en carpetas adicionales** en las propiedades de la tarea Descargar actualizaciones en el repositorio del Servidor de administración. Si especifica una carpeta ubicada en una unidad flash o un disco duro externo como carpeta de destino para esta opción, este dispositivo de almacenamiento masivo siempre contendrá la última versión de las actualizaciones.

3. En los dispositivos desconectados, configure la aplicación de seguridad (por ejemplo, Kaspersky Endpoint Security para Windows) para recibir actualizaciones de una carpeta local o un recurso compartido, como un servidor FTP o una carpeta compartida.

4. Copie los archivos de actualización de la unidad extraíble a la carpeta local o al recurso compartido que desee usar como origen de actualizaciones.

5. En el dispositivo desconectado que requiere una instalación de actualización, inicie la tarea de actualización de Kaspersky Endpoint Security para Windows.

Después de completar la tarea de actualización, las bases de datos de Kaspersky y los módulos de software están actualizados en el dispositivo.

Copia de seguridad y restauración de complementos web

Kaspersky Security Center 14 Web Console le permite hacer una copia de seguridad del estado actual de un complemento web para poder restaurar el estado guardado más adelante. Por ejemplo, puede hacer una copia de seguridad de un complemento web antes de actualizarlo a una versión más nueva. Después de la actualización, si la versión más nueva no cumple con sus requisitos o expectativas, puede restaurar la versión anterior del complemento web desde la copia de seguridad.

Para hacer una copia de seguridad de los complementos web:

1. En el menú principal, vaya a **Configuración de la consola** → **Complementos web**.

   Se abre la ventana **Configuración de la consola**.

2. En la pestaña **Complementos web**, seleccione los complementos web de los que desea realizar una copia de seguridad y, a continuación, haga clic en el botón **Crear una copia de seguridad**.

Se realiza una copia de seguridad de los complementos web seleccionados. Puede ver las copias de seguridad creadas en la pestaña **Copias de seguridad**.

Para restaurar un complemento web desde una copia de seguridad:

1. En el menú principal, vaya a **Configuración de la consola** → **Copias de seguridad**.

   Se abre la ventana **Configuración de la consola**.

2. En la pestaña **Copias de seguridad**, seleccione la copia de seguridad del complemento web que desea restaurar y, a continuación, haga clic en el botón **Restaurar desde la copia de seguridad**.

El complemento web se restaura desde la copia de seguridad seleccionada.

Ajuste de puntos de distribución y puertas de enlace de conexión

Una estructura de grupos de administración en Kaspersky Security Center realiza las funciones siguientes:

- Configura la cobertura de las directivas

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de *perfiles de directiva*. En este caso, define la cobertura de directivas mediante etiquetas, ubicaciones del dispositivo en unidades organizativas de Active Directory o pertenencia a grupos de seguridad de Active Directory.

- Configura la cobertura de las tareas de grupo

  Existe un enfoque para definir la cobertura de las tareas de grupo que no se basan en una jerarquía de los grupos de administración: el uso de tareas para selecciones de dispositivos y tareas para dispositivos específicos.

- Configura los derechos de acceso a dispositivos, Servidores de administración virtuales y Servidores de administración secundarios

- Asigna puntos de distribución

Al construir la estructura de los grupos de administración, debe tener en cuenta la topología de la red de la organización para la asignación óptima de puntos de distribución. La distribución óptima de los puntos de distribución le permite ahorrar tráfico de la red de la organización.

Según el organigrama y la topología de red de la organización, se pueden aplicar las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única

- Varias oficinas remotas pequeñas

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Configuración estándar de puntos de distribución: oficina única

En una configuración de "oficina única" estándar, todos los dispositivos están dentro de la red de la organización. La red de la organización puede consistir en unas partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

Los métodos siguientes de crear la estructura de grupos de administración son posibles:

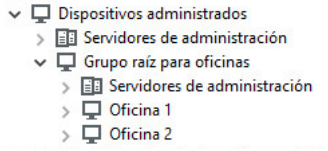
- Crear la estructura de grupos de administración tomando en consideración la topología de red. La estructura de grupos de administración puede no reflejar la topología de red con precisión absoluta. Una coincidencia entre las partes independientes de la red y ciertos grupos de administración sería suficiente. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.

- La creación de la estructura de grupos de administración, sin tomar la topología de red en cuenta. En este caso, debe desactivar la asignación automática de puntos de distribución y luego asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración de raíz en cada una de las partes independientes de la red, por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán al mismo nivel y presentarán la misma cobertura que abarca a todos los dispositivos en la red de la organización. En este caso, cada Agente de red en la versión 10 Service Pack 1 o posterior se conectará con el punto de distribución que tenga la ruta más corta. La ruta a un punto de distribución se puede rastrear con la herramienta tracert.

Configuración estándar de los puntos de distribución: varias oficinas remotas pequeñas

Esta configuración estándar sirve para varias pequeñas oficinas remotas, que se pueden comunicar con la oficina central mediante Internet. Cada oficina remota está ubicada detrás de la NAT, es decir, la conexión de una oficina remota a otra no es posible porque las oficinas están aisladas la una de la otra.

La configuración se debe reflejar en la estructura de los grupos de administración: se debe crear un grupo de administración independiente para cada oficina remota (grupos **Oficina 1** y **Oficina 2** en la imagen a continuación).



Las oficinas remotas se incluyen en la estructura del grupo de administración

Se deben asignar uno o varios puntos de distribución a cada grupo de administración que corresponda a una oficina. Los puntos de distribución deben ser dispositivos en la oficina remota que tienen una cantidad suficiente de espacio libre en disco. Los dispositivos desplegados en el grupo **Oficina 1**, por ejemplo, accederán a los puntos de distribución asignados al grupo de administración de **Oficina 1**.

Si algunos usuarios se mueven entre oficinas físicamente con sus equipos portátiles, debe seleccionar dos o más dispositivos (además de los puntos de distribución existentes) en cada oficina remota y asignarlos para que funcionen como puntos de distribución para un grupo de administración de alto nivel (**Grupo raíz para oficinas** en la imagen anterior).

Ejemplo: Un equipo portátil se despliega en el grupo de administración de la **Oficina 1** y luego se mueve físicamente a la oficina que corresponde al grupo de administración de la **Oficina 2**. Después de que se mueve el equipo portátil, el Agente de red intenta acceder a los puntos de distribución asignados al grupo de la **Oficina 1**, pero esos puntos de distribución no están disponibles. Entonces, el Agente de red empieza a intentar acceder a los puntos de distribución que se han asignado al **Grupo raíz para oficinas**. Como las oficinas remotas están aisladas la una de la otra, los intentos de acceder a los puntos de distribución asignados al grupo de administración del **Grupo raíz para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución en el grupo de la **Oficina 2**. Es decir, el equipo portátil permanecerá en el grupo de administración que corresponde a la oficina inicial, pero el equipo portátil usará el punto de distribución de la oficina donde físicamente se ubica en este momento.

Acerca de cómo asignar puntos de distribución

Puede asignar un dispositivo administrado como punto de distribución manualmente o automáticamente.

Si asigna un dispositivo administrado como punto de distribución manualmente, puede seleccionar cualquier dispositivo en su red.

Si asigna puntos de distribución automáticamente, Kaspersky Security Center puede seleccionar solo el dispositivo administrado que cumple con las siguientes condiciones:

- El dispositivo tiene como mínimo 50 GB de espacio libre en disco.
- El dispositivo administrado está conectado con Kaspersky Security Center directamente (no a través de la puerta de enlace).
- El dispositivo administrado no es un equipo portátil.

> Si su red no tiene dispositivos que cumplen con las condiciones especificadas, Kaspersky Security Center no asignará ningún dispositivo como punto de distribución automáticamente.

Asignar puntos de distribución automáticamente

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center seleccionará por sí mismo a qué dispositivos se les deben asignar puntos de distribución.

Para asignar puntos de distribución automáticamente:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Puntos de distribución**.
3. Seleccione la opción **Asignar automáticamente puntos de distribución**.

   > Si la asignación automática de dispositivos para que actúen como puntos de distribución está activada, no se pueden configurar los puntos de distribución manualmente ni editar la lista de puntos de distribución.

4. Haga clic en el botón **Guardar**.

El Servidor de administración asigna y configura puntos de distribución automáticamente.

Asignar puntos de distribución manualmente

Kaspersky Security Center le permite asignar manualmente dispositivos para actuar como puntos de distribución.

Recomendamos que asigne puntos de distribución automáticamente. En este caso, Kaspersky Security Center seleccionará por sí mismo a qué dispositivos se les deben asignar puntos de distribución. Sin embargo, si tiene que optar por no asignar automáticamente puntos de distribución por cualquier motivo (por ejemplo, si desea usar servidores asignados exclusivamente), puede asignar puntos de distribución manualmente después de calcular su número y configuración.

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Para designar manualmente un dispositivo para actuar como punto de distribución:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Puntos de distribución**.

3. Seleccione la opción **Asignar manualmente puntos de distribución**.

4. Haga clic en el botón **Asignar**.

5. Seleccione el dispositivo que desea convertir en punto de distribución.

   Al seleccionar un dispositivo, recuerde las características de operación de puntos de distribución y el conjunto de requisitos para el dispositivo que actúa como punto de distribución.

6. Seleccione el grupo de administración que desee incluir en la cobertura del punto de distribución seleccionado.

7. Haga clic en el botón **Añadir**.

   El punto de distribución que ha añadido se mostrará en la lista de puntos de distribución, en la sección **Puntos de distribución**.

8. Seleccione el punto de distribución recién añadido en la lista para abrir su ventana de propiedades.

9. Configure el punto de distribución perfil en la ventana de propiedades:

   - La sección **Control de aplicaciones** contiene la configuración de interacción entre el punto de distribución con los dispositivos cliente:

     - **Puerto SSL**

       El número del puerto SSL para la conexión cifrada entre los dispositivos cliente y el punto de distribución usando SSL.

       De forma predeterminada, se utiliza el puerto 13000.

     - **Usar difusión múltiple**

       Si se selecciona esta opción, se utilizará la multidifusión IP para la distribución automática de paquetes de instalación en dispositivos cliente dentro del grupo.

       La multidifusión IP disminuye el tiempo requerido para instalar una aplicación desde un paquete de instalación hacia un grupo de dispositivos cliente, pero aumenta el tiempo de instalación cuando instala una aplicación en un único dispositivo cliente.

- **Dirección IP de difusión múltiple**

  La dirección IP que se utilizará para la multidifusión. Puede definir una dirección IP en el rango de 224.0.0.0 – 239.255.255.255

  De manera predeterminada, Kaspersky Security Center asigna automáticamente una dirección IP de multidifusión única dentro del rango dado.

- **Número de puerto de multidifusión IP**

  Número del puerto para multidifusión IP.

  De forma predeterminada el número de puerto es el 15001. Si el dispositivo que tiene el Servidor de administración instalado está configurado como punto de distribución, de forma predeterminada se utiliza el puerto 13001 para la conexión SSL.

- **Desplegar actualizaciones**

  Las actualizaciones se distribuyen a los dispositivos administrados desde los siguientes orígenes:

  - Este punto de distribución, si esta opción está activada.
  - Otros puntos de distribución, Servidor de administración o servidores de actualización de Kaspersky, si esta opción está desactivada.

  Si usa puntos de distribución para implementar actualizaciones, puede ahorrar tráfico dado que se reduce la cantidad de descargas. Además, puede aliviar la carga en el Servidor de administración y reubicarla entre los puntos de distribución. Puede calcular el número de puntos de distribución de su red para optimizar el tráfico y la carga.

  Si desactiva esta opción, puede aumentar el número de descargas de actualizaciones y la carga en el Servidor de administración. Esta opción está activada de forma predeterminada.

- **Desplegar paquetes de instalación**

  Los paquetes de instalación se distribuyen a los dispositivos administrados desde las siguientes fuentes:

  - Este punto de distribución, si esta opción está activada.
  - Otros puntos de distribución, Servidor de administración o servidores de actualización de Kaspersky, si esta opción está desactivada.

  Si usa puntos de distribución para implementar paquetes de instalación, puede ahorrar tráfico dado que se reduce la cantidad de descargas. Además, puede aliviar la carga en el Servidor de administración y reubicarla entre los puntos de distribución. Puede calcular el número de puntos de distribución de su red para optimizar el tráfico y la carga.

  Si desactiva esta opción, puede aumentar la cantidad de descargas de paquetes de instalación y la carga en el Servidor de administración. Esta opción está activada de forma predeterminada.

- **Ejecutar servidor push**

En Kaspersky Security Center, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y los dispositivos gestionados por Agente de red. Por ejemplo, se debe activar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se activa el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede activar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

- **Puerto del servidor push**

  El número de puerto del servidor push. Puede especificar el número de cualquier puerto desocupado.

- En la sección **Cobertura**, especifique el ámbito en el que el punto de distribución distribuirá actualizaciones (grupos de administración y/o ubicación de la red).

  Solo los dispositivos con sistema operativo Windows pueden determinar su ubicación de red. No se puede determinar la ubicación de red para dispositivos que ejecuten otros sistemas operativos.

- En la sección **Origen de actualizaciones**, puede seleccionar una fuente de actualizaciones para el punto de distribución:

  - **Fuente de actualizaciones**

    Seleccione una fuente de actualizaciones para el punto de distribución:

    - Para permitir al punto de distribución recibir actualizaciones del Servidor de administración, seleccione **Descargar del Servidor de administración**.
    - Para permitir que el punto de distribución reciba actualizaciones mediante una tarea, seleccione **Utilizar la tarea de descarga de actualizaciones** y, a continuación, especifique una tarea *Descargar actualizaciones a los repositorios de los puntos de distribución*:
      - Si dicha tarea ya existe en el dispositivo, selecciónela en la lista.
      - Si aún no existe tal tarea en el dispositivo, haga clic en el enlace **Crear una tarea** para crear una tarea. Se inicia el Asistente para añadir tareas. Siga las instrucciones del Asistente.

  - **Descargar archivos de comparación**

    Esta opción habilita la función de descarga de archivos diff.

    Esta opción está activada de forma predeterminada.

- En la sección **Proxy de KSN**, puede configurar la aplicación para utilizar el punto de distribución para reenviar solicitudes de KSN desde los dispositivos administrados:

  - **Activar el proxy de KSN en el punto de distribución**

El servicio de proxy de KSN se ejecuta en el dispositivo que se utiliza como punto de distribución. Utilice esta función para redistribuir y optimizar el tráfico en la red.

El punto de distribución envía a Kaspersky las estadísticas de KSN, que se incluyen en la declaración de Kaspersky Security Network. De forma predeterminada, la declaración de KSN se guarda en %Archivos de programa%\Kaspersky Lab\Kaspersky Security Center\ksneula.

Esta opción está desactivada de forma predeterminada. Esta opción solo se activa si las opciones **Utilizar el Servidor de administración como servidor proxy** y **Acepto usar Kaspersky Security Network** están activadas en la ventana de propiedades del Servidor de administración.

Puede asignar un nodo de un clúster activo-pasivo a un punto de distribución y activar el proxy de KSN en ese nodo.

- **Reenviar solicitudes de KSN al Servidor de administración**

  El punto de distribución reenvía las solicitudes KSN de los dispositivos administrados al Servidor de administración.

  Esta opción está activada de forma predeterminada.

- **Acceder a la nube de KSN/KSN privada directamente a través de Internet**

  El punto de distribución reenvía las solicitudes de KSN de los dispositivos administrados a KSN Cloud o KSN privada. Las solicitudes de KSN generadas en el punto de distribución también se envían directamente a KSN Cloud o KSN privada.

  Los puntos de distribución que tienen instalado el Agente de red versión 11 (o versiones anteriores) no pueden acceder a KSN Privada directamente. Si desea reconfigurar los puntos de distribución para enviar solicitudes KSN a KSN Privada, active la opción **Reenviar solicitudes de KSN al Servidor de administración** para cada punto de distribución.

  Los puntos de distribución que tienen instalado el Agente de red versión 12 (o versiones posteriores) pueden acceder a KSN privada directamente.

- **Ignorar la configuración del servidor proxy KSC al conectarse a KSN privada**

  Active esta opción si tiene las opciones del servidor proxy configuradas en las propiedades del punto de distribución o en la directiva de Agente de red, pero su arquitectura de red requiere que use KSN privada directamente. De lo contrario, las solicitudes de las aplicaciones administradas no podrán llegar a la KSN privada.

- **Puerto TCP**

  El número del puerto de TCP que los dispositivos administrados utilizarán para conectar al Servidor proxy de KSN. El número de puerto predeterminado es el 13111.

- **Puerto UDP**

  Si necesita que los dispositivos administrados se conecten al Servidor proxy de KSN a través de un puerto UDP, habilite la opción **Usar puerto UDP** y especifique un número de **puerto UDP**. Esta opción está activada de forma predeterminada. El puerto UDP predeterminado de conexión al Servidor proxy de KSN es 15111.

- Configure el sondeo de los dominios de Windows, Active Directory y los rangos de IP según el punto de distribución:
  - **Dominios de Windows**

    Puede habilitar la detección de dispositivos para los dominios de Windows y establecer la programación para el descubrimiento.

  - **Active Directory**

    Puede activar el sondeo de red para Active Directory y establecer la programación para el sondeo.

    Si selecciona la casilla de verificación **Activar sondeo de red**, puede seleccionar una de las siguientes opciones:

    - **Analizar el dominio actual de Active Directory**.
    - **Analizar el bosque de dominio de Active Directory**.
    - **Analizar solo los dominios seleccionados de Active Directory**. Si selecciona esta opción, añada uno o más dominios de Active Directory a la lista.

  - **Rangos IP**

    Puede activar la detección de dispositivos para los rangos IPv4 y las redes IPv6.

    Si activa la opción **Activar rango de sondeo**, puede añadir rangos analizados y establecer la programación para ellos. Puede añadir rangos de IP a la lista de intervalos analizados.

    Si activa la opción **Activar el sondeo con la tecnología Zeroconf**, el punto de distribución automáticamente sondea la red IPv6 mediante el uso de las redes de configuración cero (también denominadas *Zeroconf*). En este caso, los rangos de IP especificados se ignoran, porque el punto de distribución sondea toda la red.

- En la sección **Avanzado**, especifique la carpeta que debe utilizar el punto de distribución para almacenar datos distribuidos:
  - **Usar carpeta predeterminada**

    Si selecciona esta opción, la aplicación usará la carpeta de instalación de Agente de red en el punto de distribución.

  - **Usar carpeta especificada**

    Si se selecciona esta opción, se podrá especificar la ruta de la carpeta en el campo siguiente. Puede ser una carpeta local en el punto de distribución, o bien un directorio remoto en cualquier dispositivo de la red corporativa.

    La cuenta de usuario utilizada en el punto de distribución para ejecutar el Agente de red debe tener acceso de lectura y escritura a la carpeta especificada.

10. Haga clic en el botón **Aceptar**.

Los dispositivos seleccionados se comportan como puntos de distribución.

Modificación de la lista de puntos de distribución para un grupo de administración

Puede ver la lista de puntos de distribución asignados para un grupo de administración específico y modificar la lista añadiendo o eliminando puntos de distribución.

Para ver y modificar la lista de puntos de distribución para un grupo de administración:

1. En el menú principal, vaya a **DISPOSITIVOS** → **Grupos**.
2. En la estructura del grupo de administración, seleccione el grupo de administración para el que desea ver los puntos de distribución asignados.
3. Seleccione la pestaña **PUNTOS DE DISTRIBUCIÓN**.
4. Añada nuevos puntos de distribución para el grupo de administración utilizando el botón **Asignar** o elimine los puntos de distribución asignados utilizando el botón **Desasignar**.

   Según sus modificaciones, los nuevos puntos de distribución se añaden a la lista o los puntos de distribución existentes se eliminan de la lista.

Forzar sincronización

Aunque Kaspersky Security Center sincroniza automáticamente el estado, la configuración, las tareas y las políticas de los dispositivos administrados, en algunos casos es posible que desee ejecutar la sincronización para un dispositivo específico a la fuerza. Puede ejecutar la sincronización forzada para los siguientes dispositivos:

- Dispositivos que tienen instalado el Agente de red
- Dispositivos que ejecutan KasperskyOS

  Antes de ejecutar la sincronización forzada para un dispositivo KasperskyOS, asegúrese de que el dispositivo esté incluido en el alcance de un punto de distribución y que un servidor push esté habilitado en el punto de distribución.
- Dispositivos iOS
- Dispositivos Android

  Antes de ejecutar la sincronización forzada para un dispositivo Android, debe configurar Google Firebase Cloud Messaging.

Sincronización de un solo dispositivo

Para forzar la sincronización entre el Servidor de administración y un dispositivo administrado:

1. En el menú principal, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el nombre del dispositivo que desea sincronizar con el Servidor de administración.

   Se abrirá una ventana de propiedades con la sección **Control de aplicaciones** seleccionada.

3. Haga clic en el botón **Forzar sincronización**.

La aplicación sincroniza el dispositivo seleccionado con el Servidor de administración.

Sincronización de múltiples dispositivos

Para forzar la sincronización entre el Servidor de administración y varios dispositivos administrados:

1. Abra la lista de dispositivos de un grupo de administración o una selección de dispositivos:
   - En el menú principal, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS** → **Grupos** y seleccione el grupo de administración que contiene los dispositivos que desea sincronizar.
   - Ejecute una selección de dispositivos para ver la lista de dispositivos.
2. Seleccione las casillas de verificación junto a los dispositivos que desea sincronizar con el Servidor de administración.
3. Haga clic en el botón **Forzar sincronización**.

   La aplicación sincroniza los dispositivos seleccionados con el Servidor de administración.
4. En la lista de dispositivos, puede ver que la hora de la última conexión al Servidor de administración de los dispositivos seleccionados ha cambiado a la hora actual. Si la hora no ha cambiado, actualice el contenido de la página haciendo clic en el botón **Actualizar**.

Los dispositivos seleccionados se sincronizan con el Servidor de administración.

Visualización del tiempo de entrega de una directiva

Después de cambiar una directiva para una aplicación de Kaspersky en el Servidor de administración, el administrador puede verificar si la directiva modificada se ha entregado a un dispositivo administrado específico. Una directiva se puede entregar durante una sincronización regular o una sincronización forzada.

Para ver la fecha y hora en que se entregó una directiva de la aplicación a un dispositivo administrado, haga lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el nombre del dispositivo que desea sincronizar con el Servidor de administración.

   Se abrirá una ventana de propiedades con la sección **Control de aplicaciones** seleccionada.
3. Seleccione la pestaña **Aplicaciones**.
4. Seleccione la aplicación para la que desea ver la fecha de sincronización de la directiva.

   La ventana de directiva de la aplicación se abre con la sección **Control de aplicaciones** seleccionada y la fecha y hora de entrega de la directiva mostradas.

Habilitación de un servidor push

En Kaspersky Security Center, un punto de distribución puede funcionar como servidor push para los dispositivos administrados a través del protocolo móvil y los dispositivos gestionados por Agente de red. Por ejemplo, se debe activar un servidor push si quiere poder forzar la sincronización de los dispositivos KasperskyOS con el Servidor de administración. Un servidor push tiene el mismo alcance de los dispositivos administrados que el punto de distribución en el que se activa el servidor push. Si tiene varios puntos de distribución asignados para el mismo grupo de administración, puede activar el servidor push en cada uno de los puntos de distribución. En este caso, el Servidor de administración equilibra la carga entre los puntos de distribución.

Se recomienda utilizar puntos de distribución como servidores push para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración. Se necesita conectividad continua para algunas operaciones, como ejecutar y detener tareas locales, recibir estadísticas para una aplicación administrada o crear un túnel. Si utiliza un punto de distribución como servidor push, no es necesario utilizar la opción **No desconectar del Servidor de administración** en dispositivos administrados o enviar paquetes al puerto UDP del Agente de red.

Un servidor push soporta la carga de hasta 50 000 conexiones simultáneas.

Para habilitar el servidor push en un punto de distribución:

1. Haga clic en el icono de **Configuración** (🔧) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Puntos de distribución**.

3. Haga clic en el nombre del punto de distribución en el que desea habilitar el servidor push.

   Se abre la ventana de propiedades del punto de distribución.

4. En la sección **Control de aplicaciones**, active la opción **Ejecutar servidor push**.

5. En el campo **Puerto del servidor push**, escriba el número de puerto. Puede especificar el número de cualquier puerto desocupado.

6. En el campo **Dirección para hosts remotos**, especifique la dirección IP o el nombre del dispositivo del punto de distribución.

7. Haga clic en el botón **Aceptar**.

El servidor push está habilitado en el punto de distribución seleccionado.

Administrar aplicaciones de terceros en dispositivos cliente

Esta sección describe las funciones de Kaspersky Security Center relacionadas con la administración de aplicaciones de terceros instaladas en dispositivos cliente.

Acerca de las aplicaciones de terceros

Kaspersky Security Center puede ayudarle a actualizar el software de terceros, el software instalado en los dispositivos de los clientes, y a corregir las vulnerabilidades del software de terceros. Kaspersky Security Center solo puede actualizar el software de terceros de la versión actual a la versión más reciente. La siguiente lista representa el software de terceros que puede actualizar con Kaspersky Security Center:

La lista de software de terceros se puede actualizar y ampliar con nuevas aplicaciones. Puede comprobar si puede actualizar el software de terceros (instalado en los dispositivos de los usuarios) con Kaspersky Security Center consultando la lista de actualizaciones disponibles en Kaspersky Security Center 14 Web Console.

- 7-Zip Developers: 7-Zip
- Adobe Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple:
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber
- Code Sector: TeraCopy
- DbVis Software AB: DbVisualizer
- Enter Srl: Iperius Backup
- Codec Guide:
  - K-Lite Codec Pack Basic
  - K-Lite Codec Pack Full
  - K-Lite Codec Pack Mega
  - K-Lite Codec Pack Standard

- Decho Corp.:
  - Mozy Enterprise
  - Mozy Home
  - Mozy Pro
- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox
- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Eric Lawrence: Fiddler
- EverNote: EverNote
- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
  - Radmin
  - Administrador remoto
- Far Manager: FAR Manager
- FastStone Soft: FastStone Image Viewer
- Firebird Developers: Firebird
- Foxit Corporation:
  - Foxit Reader
  - Foxit Reader Enterprise
- Free Download Manager.ORG: Free Download Manager
- GIMP project: GIMP
- GlavSoft LLC.: TightVNC
- GNU Project: Gpg4win
- Google:

    - Google Earth
    - Google Chrome
    - Google Chrome Enterprise
    - Google Earth Pro
    - Google Backup and Sync
- Inkscape Project: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- JustSystems Corporation: Ichitaro
- Logitech: SetPoint
- LogMeIn, Inc.:
    - LogMeIn
    - Hamachi
    - LogMeIn Rescue Technician Console
    - RemotelyAnywhere Workstation Edition
- Martin Prikryl: WinSCP
- Mozilla Foundation:
    - Mozilla Firefox
    - Mozilla Firefox ESR
    - Mozilla SeaMonkey
    - Mozilla Thunderbird
- OpenOffice.org: OpenOffice.org
- Opera Software: Opera
- Oracle Corporation:
    - Oracle Java JRE
    - Oracle VirtualBox
- PDF44: PDF24 MSI/EXE
- Piriform:

    - CCleaner
    - Defraggler
    - Recuva
    - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
    - RealVNC Server
    - RealVNC Viewer
- Simon Tatham: PuTTY
- Sober Lemur S.a.s.:
    - PDFsam Basic
    - PDFsam Visual
- Softland: FBackup
- Skype Technologies: Skype for Windows
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:
    - TeamViewer Host
    - TeamViewer
- Telegram Messenger LLP: Telegram Desktop
- The Document Foundation:
    - LibreOffice
    - LibreOffice HelpPack
- The Git Development Community:
    - Git for Windows
    - Git LFS

- The Pidgin developer community: Pidgin
- The qBittorrent project: qBittorrent
- TortoiseSVN Developers: TortoiseSVN
- VideoLAN: VLC media player
- VMware:
  - VMware Player
  - VMware Workstation
- WinRAR Developers: WinRAR
- WinZip: WinZip
- Wireshark Foundation: Wireshark
- Wrike: Wrike
- Zimbra: Zimbra Desktop
- Zoom Video Communications, Inc.: Zoom (MSI Distributions)

Instalar actualizaciones de software de terceros

Esta sección describe las funciones de Kaspersky Security Center relacionadas con la instalación de actualizaciones de aplicaciones de terceros instaladas en dispositivos cliente.

Escenario: actualización de software de terceros

Esta sección proporciona un escenario para actualizar software de terceros instalado en los dispositivos cliente. Software de terceros incluye aplicaciones de Microsoft y de otros proveedores. El servicio de Windows Update proporciona actualizaciones para las aplicaciones de Microsoft.

Requisitos previos

El Servidor de administración debe tener una conexión a Internet para instalar actualizaciones de software de terceros que no sean software de Microsoft.

De forma predeterminada, el Servidor de administración no requiere conexión a Internet para instalar actualizaciones de software de Microsoft en los dispositivos administrados. Por ejemplo, los dispositivos administrados pueden descargar las actualizaciones de software de Microsoft directamente desde los servidores de Microsoft Update o desde Windows Server con Microsoft Windows Server Update Services (WSUS) implementado en la red de su organización. El Servidor de administración debe estar conectado a Internet cuando utilice el Servidor de administración como servidor WSUS.

Etapas

La actualización de software de terceros se efectúa en etapas:

1. **Buscar actualizaciones requeridas**

   Para buscar las actualizaciones de software de terceros necesarias para los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el Asistente de inicio rápido del Servidor de administración. Si no ejecutó el Asistente, cree la tarea o ejecute el Asistente de inicio rápido ahora.

   Instrucciones:

   - Consola de administración: Análisis de aplicaciones para buscar vulnerabilidades, Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center 14 Web Console: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Analizar la lista de actualizaciones encontradas**

   Vea la lista de **ACTUALIZACIONES DE SOFTWARE** y decida las actualizaciones que se instalarán. Para ver información detallada sobre cada actualización, haga clic en el nombre de la actualización en la lista. Para cada actualización de la lista, también puede ver las estadísticas sobre la instalación de la actualización en los dispositivos cliente.

   Instrucciones:

   - Consola de administración: Visualización de información acerca de las actualizaciones disponibles
   - Kaspersky Security Center 14 Web Console: Visualización de información sobre actualizaciones de software de terceros disponibles

3. **Configurar la instalación de actualizaciones**

   Una vez que Kaspersky Security Center recibe la lista de actualizaciones de software de terceros, usted puede instalarlas en los dispositivos cliente mediante las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Instalar actualizaciones de Windows Update*. Cree una de estas tareas. Puede crear estas tareas en la ficha **TAREAS** o desde la lista **ACTUALIZACIONES DE SOFTWARE**.

   La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft, incluidas las actualizaciones que proporciona el servicio Windows Update y las actualizaciones de productos de otros proveedores. Tenga en cuenta que esta tarea se puede crear únicamente si tiene la licencia para la función Administración de vulnerabilidades y parches.

   La tarea *Instalar actualizaciones de Windows Update* no requiere una licencia, pero se puede usar para instalar únicamente actualizaciones de Windows Update.

   Para instalar algunas actualizaciones de software, debe aceptar el Contrato de licencia de usuario final (EULA) para el software de instalación. Si rechaza el EULA, la actualización de software no se instalará.

   Puede iniciar una tarea de instalación de actualizaciones según una programación. Cuando especifique la programación de tareas, asegúrese de que la tarea de instalación de actualización comience después de que se complete la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

   Instrucciones:

   - Consola de administración: Reparación de las vulnerabilidades en las aplicaciones, Visualización de información acerca de las actualizaciones disponibles

- Kaspersky Security Center 14 Web Console: Crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades, Crear la tarea Instalar actualizaciones de Windows Update, Visualización de información sobre actualizaciones de software de terceros disponibles

4. **Programar las tareas**

   Para asegurarse de que la lista de actualizaciones esté siempre actualizada, programe la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para que se ejecute de forma automática ocasionalmente. La frecuencia predeterminada es una vez a la semana.

   Si ha creado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede programarla para que se ejecute con igual o menor frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Al programar la tarea *Instalar actualizaciones de Windows Update*, tenga en cuenta que debe definir la lista de actualizaciones para esta tarea cada vez antes de iniciarla.

   Cuando programe las tareas, asegúrese de que una tarea de instalación de actualización comience después de que se complete la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

5. **Aprobar y rechazar actualizaciones de software (opcional)**

   Si ha creado la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades, puede especificar reglas para instalar la actualización en las propiedades de la tarea. Si ha creado la tarea Instalar actualizaciones de Windows Update, omita este paso.

   Para cada regla, puede definir las actualizaciones que desea instalar según el estado de la actualización: *Sin definir*, *Aprobada* o *Rechazada*. Por ejemplo, puede que quiera crear una tarea específica para servidores y establecer una regla para dicha tarea que permita la instalación únicamente de actualizaciones de Windows Update y de aquellas que tengan el estado *Aprobada*. Después, debe establecer manualmente el estado *Aprobada* para las actualizaciones que desea instalar. En este caso, las actualizaciones de Windows Update que tienen el estado *Sin definir* o *Rechazada* no se instalarán en los servidores que haya especificado en la tarea.

   El uso del estado *Aprobado* para administrar la instalación de actualizaciones es eficiente para una pequeña cantidad de actualizaciones. Para instalar varias actualizaciones, utilice las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y corregir vulnerabilidades*. Le recomendamos que asigne el estado *Aprobado* solo a aquellas actualizaciones específicas que no cumplan con los criterios especificados en las reglas. Cuando aprueba manualmente una gran cantidad de actualizaciones, el rendimiento del Servidor de administración disminuye y puede provocar una sobrecarga en el Servidor de administración.

   De forma predeterminada, las actualizaciones de software descargadas tienen el estado *No definido*. Puede cambiar el estado a *Aprobado* o *Rechazado* en la lista **ACTUALIZACIONES DE SOFTWARE** (**OPERACIONES** → **ADMINISTRACIÓN DE PARCHES** → **ACTUALIZACIONES DE SOFTWARE**).

   Instrucciones:

   - Consola de administración: Aprobar y rechazar actualizaciones de software
   - Kaspersky Security Center 14 Web Console: Aprobar y rechazar actualizaciones de software de terceros

6. **Configuración del Servidor de administración para que funcione como un servidor del Servicio de Windows Server Update (WSUS) (opcional)**

   De manera predeterminada, las actualizaciones de Windows Update se descargan a los dispositivos administrados desde los servidores de Microsoft. Puede cambiar esta configuración para utilizar el Servidor de administración como servidor WSUS. En este caso, el Servidor de administración sincroniza los datos de la actualización con Windows Update en la frecuencia especificada y proporciona actualizaciones de modo centralizado a Windows Update en los dispositivos en red.

   Para utilizar el Servidor de administración como servidor WSUS, cree la tarea Realizar la sincronización de Windows Update y seleccione la casilla de verificación **Utilizar el Servidor de administración como servidor WSUS** en la directiva del Agente de red.

   Instrucciones:

   - Consola de administración: Sincronización de actualizaciones de Windows Update con el Servidor de administración, Configuración de actualizaciones de Windows en una directiva del Agente de red

- Kaspersky Security Center 14 Web Console: Creación de la tarea de sincronización Realizar la actualización de Windows Update

7. **Ejecutar una tarea de instalación de actualización**

   Inicie las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Instalar actualizaciones de Windows Update*. Cuando inicia estas tareas, las actualizaciones se descargan e instalan en los dispositivos administrados. Una vez completada la tarea, asegúrese de que tenga el estado *Completado correctamente* en la lista de tareas.

8. **Crear el informe sobre los resultados de la instalación de actualizaciones de software de terceros (opcional)**

   Para ver estadísticas detalladas sobre la instalación de la actualización, genere **Informe sobre los resultados de la instalación de actualizaciones de software de otros fabricantes**.

   Instrucciones:

   - Consola de administración: Creación y visualización de un informe
   - Kaspersky Security Center 14 Web Console: Generación y visualización de un informe

Resultados

Si ha creado y configurado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las actualizaciones se instalan en los dispositivos administrados automáticamente. Cuando se descargan actualizaciones nuevas en el repositorio del Servidor de administración, Kaspersky Security Center verifica si cumplen con los criterios especificados en las reglas de actualización. Todas las actualizaciones nuevas que cumplan con los criterios se instalarán automáticamente la próxima vez que se ejecute la tarea.

Si ha creado la tarea *Instalar actualizaciones de Windows Update*, solo se instalarán las actualizaciones especificadas en las propiedades de la tarea *Instalar actualizaciones de Windows Update*. En el futuro, si desea instalar nuevas actualizaciones descargadas en el repositorio del Servidor de administración, debe añadir las actualizaciones necesarias a la lista de actualizaciones en la tarea existente o crear una nueva tarea *Instalar actualizaciones de Windows Update*.

Acerca de las actualizaciones de software de terceros

Kaspersky Security Center le permite administrar las actualizaciones de software de terceros instaladas en los dispositivos administrados y reparar vulnerabilidades en las aplicaciones de Microsoft y los productos de otros desarrolladores de software mediante la instalación de las actualizaciones requeridas.

Kaspersky Security Center busca actualizaciones a través de la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Servidor de administración recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea. Después de examinar la información sobre las actualizaciones disponibles, puede instalarlas en los dispositivos.

> Kaspersky Security Center actualiza algunas aplicaciones quitando la versión anterior de la aplicación e instalando la nueva.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Por razones de seguridad, las tecnologías de Kaspersky analizan automáticamente en busca de malware cualquier actualización de software de terceros que instale mediante la función Administración de vulnerabilidades y parches. Estas tecnologías se utilizan para la verificación automática de archivos e incluyen análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno aislado y aprendizaje automático.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Además, los expertos de Kaspersky no buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en dichas actualizaciones, ni realizan otros tipos de análisis de las actualizaciones distintos a los especificados en el párrafo anterior.

Tareas para la instalación de actualizaciones de software de terceros

Cuando se descargan metadatos de las actualizaciones de software de terceros en el repositorio, puede instalar dichas actualizaciones en los dispositivos cliente mediante las siguientes tareas:

- La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*

  La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para instalar actualizaciones para aplicaciones de Microsoft, incluidas las actualizaciones que proporciona el servicio Windows Update y las actualizaciones de productos de otros proveedores. Tenga en cuenta que esta tarea se puede crear únicamente si tiene la licencia para la función Administración de vulnerabilidades y parches.

  Una vez completada esta tarea, las actualizaciones se instalan en los dispositivos administrados automáticamente. Cuando se descargan metadatos de nuevas actualizaciones en el repositorio del Servidor de administración, Kaspersky Security Center verifica si estas actualizaciones cumplen con los criterios especificados en las reglas de actualización. Todas las actualizaciones nuevas que cumplan con los criterios se descargarán e instalarán automáticamente la próxima vez que se ejecute la tarea.

- La tarea *Instalar actualizaciones de Windows Update*

  La tarea *Instalar actualizaciones de Windows Update* no requiere una licencia, pero se puede usar para instalar únicamente actualizaciones de Windows Update.

  Una vez completada esta tarea, solo se instalarán aquellas actualizaciones que se especifican en las propiedades de la tarea. En el futuro, si desea instalar nuevas actualizaciones descargadas en el repositorio del Servidor de administración, debe añadir las actualizaciones necesarias a la lista de actualizaciones en la tarea existente o crear una nueva tarea Instalar actualizaciones de Windows Update.

Utilizar el Servidor de administración como servidor WSUS

La información sobre las actualizaciones disponibles para Microsoft Windows la proporciona el servicio de Windows Update. El Servidor de administración se puede usar como servidor de Windows Server Update Services (WSUS). Para utilizar el Servidor de administración como servidor WSUS, debe crear la tarea Realizar la sincronización de Windows Update y seleccionar la opción **Utilizar el Servidor de administración como servidor WSUS** en la directiva del Agente de red. Tras configurar la sincronización de los datos con Windows Update, el Servidor de administración proporciona actualizaciones a los servicios de Windows Update en los dispositivos de forma centralizada y con la frecuencia definida.

Instalar actualizaciones de software de terceros

Puede instalar actualizaciones de software de terceros en dispositivos administrados mediante la creación o ejecución de las siguientes tareas:

- *Instalar actualizaciones requeridas y reparar vulnerabilidades*

  La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se puede crear únicamente si tiene una licencia para la función Administración de vulnerabilidades y parches. Puede utilizar esta tarea para instalar las actualizaciones de Windows Update proporcionadas por Microsoft y las actualizaciones de los productos de otros proveedores.

- *Instalar actualizaciones de Windows Update*

  Puede usar la tarea *Instalar actualizaciones de Windows Update* para instalar solo las actualizaciones de Windows Update.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Como opción, puede crear una tarea para instalar las actualizaciones necesarias de las siguientes formas:

- Abra la lista de actualizaciones y especifique qué actualizaciones instalar.

  Como resultado, se crea una nueva tarea para instalar las actualizaciones seleccionadas. Como opción, puede añadir las actualizaciones seleccionadas a una tarea existente.

- Ejecute el Asistente de instalación de actualizaciones.

  El Asistente de instalación de actualizaciones solo están disponibles bajo la licencia de Administración de vulnerabilidades y parches.

  El Asistente simplifica la creación y configuración de una tarea de instalación de actualizaciones y le permite excluir la creación de tareas redundantes que contienen las mismas actualizaciones para instalar.

Instalación de actualizaciones de software de terceros utilizando la lista de actualizaciones

Para instalar actualizaciones de software de terceros utilizando la lista de actualizaciones:

1. Abra una de las listas de actualizaciones:

   - Para abrir la lista general de actualizaciones, vaya a **OPERACIONES** → **ADMINISTRACIÓN DE PARCHES** → **ACTUALIZACIONES DE SOFTWARE**.

   - Para abrir la lista de actualizaciones de un dispositivo administrado, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS** → <nombre del dispositivo> → **Avanzado** → **Actualizaciones disponibles**.

   - Para abrir la lista de actualizaciones de una aplicación específica, vaya a **OPERACIONES** → **APLICACIONES DE TERCEROS** → **REGISTRO DE APLICACIONES** → <nombre de la aplicación> → **Actualizaciones disponibles**.

   Aparece una lista de actualizaciones disponibles.

2. Seleccione las casillas al lado de las actualizaciones que desea instalar.

3. Haga clic en el botón **Instalar actualizaciones**.

Para instalar algunas actualizaciones de software, debe aceptar el Contrato de licencia de usuario final (EULA). Si rechaza el EULA, la actualización de software no se instalará.

4. Seleccione una de las siguientes opciones:

   - **Nueva tarea**

     Se inicia Asistente para añadir tarea. Si tiene la licencia de Administración de vulnerabilidades y parches, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* está preseleccionada. Si no tiene la licencia, la tarea *Instalar actualizaciones de Windows Update* está preseleccionada. Siga los pasos del Asistente para completar la creación de la tarea.

   - **Instalar actualización (añadir regla a tarea específica)**

     Seleccione una tarea a la que desee añadir las actualizaciones seleccionadas. Si tiene la licencia de Administración de vulnerabilidades y parches, seleccione una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Una nueva regla para instalar las actualizaciones seleccionadas se añadirá automáticamente a la tarea seleccionada. Si no tiene la licencia, seleccione una tarea *Instalar actualizaciones de Windows Update*. Las actualizaciones seleccionadas se añadirán a las propiedades de la tarea.

     Se abrirá la ventana de propiedades de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, la tarea se crea y se muestra en la lista de tareas en **DISPOSITIVOS → TAREAS**. Si eligió añadir las actualizaciones a una tarea existente, las actualizaciones se guardan en las propiedades de la tarea.

Para instalar las actualizaciones de software de terceros, inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Instalar actualizaciones de Windows Update*. Puede iniciar cualquiera de estas tareas de forma manual o especificar la configuración de programación en las propiedades de la tarea que inicia. Cuando especifique la programación de tareas, asegúrese de que la tarea de instalación de actualización comience después de que se complete la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

Instalación de actualizaciones de software de terceros mediante el Asistente de instalación de actualizaciones

El Asistente de instalación de actualizaciones solo están disponibles bajo la licencia de Administración de vulnerabilidades y parches.

Para crear una tarea para instalar actualizaciones de software de terceros utilizando el Asistente de instalación de actualizaciones:

1. Seleccione **OPERACIONES → ADMINISTRACIÓN DE PARCHES** y, en la lista desplegable, seleccione **ACTUALIZACIONES DE SOFTWARE**.

   Aparece una lista de actualizaciones disponibles.

2. Seleccione la casilla de verificación al lado de la actualización que desea instalar.

3. Haga clic en el botón **Ejecutar Asistente de instalación de actualización**.

   Se inicia el Asistente de instalación de actualizaciones. La página **Seleccionar la tarea de instalación de actualizaciones** muestra la lista de todas las tareas existentes de los siguientes tipos:

   - *Instalar actualizaciones requeridas y reparar vulnerabilidades*
   - *Instalar actualizaciones de Windows Update*
   - *Reparar vulnerabilidades*

No puede modificar las tareas de los dos últimos tipos para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

4. Si desea que el Asistente muestre solo las tareas que instalan la actualización que ha seleccionado, habilite la opción **Mostrar solo las tareas que instalan esta actualización**.

5. Elija lo que quiere hacer:

   - Para iniciar una tarea, seleccione la casilla de verificación junto al nombre de la tarea y luego haga clic en el botón **Iniciar**.

   - Para añadir una nueva regla a una tarea existente:

     a. Seleccione la casilla de verificación junto al nombre de la tarea y luego haga clic en el botón **Añadir regla**.

     b. En la página que se abre, configure la nueva regla:

     - **Regla de instalación para actualizaciones de este nivel de importancia**

       A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

       Si esta opción está activada, las actualizaciones solucionan solo las vulnerabilidades cuyo nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

       Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

       Esta opción está desactivada de forma predeterminada.

     - **Regla de instalación para actualizaciones de este nivel de importancia según MSRC**

       A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

       Si esta opción está activada (disponible solo para las actualizaciones de Windows Update), las actualizaciones solucionan solo aquellas vulnerabilidades para las cuales el nivel de gravedad establecido por el Centro de respuesta de seguridad de Microsoft (MSRC) es igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

       Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

       Esta opción está desactivada de forma predeterminada.

     - **Regla de instalación para las actualizaciones según este proveedor**

       Esta opción está disponible solo para las actualizaciones de aplicaciones de terceros. Kaspersky Security Center instala solo las actualizaciones relacionadas con las aplicaciones del mismo proveedor que la actualización seleccionada. Las actualizaciones rechazadas y las actualizaciones de las aplicaciones de otros proveedores no se instalan.

       Esta opción está desactivada de forma predeterminada.

- **Regla de instalación para las actualizaciones de tipo**
- **Regla de instalación para la actualización seleccionada**
- Aprobar actualizaciones seleccionadas

  La actualización seleccionada será aprobada para su instalación. Active esta opción si algunas reglas aplicadas de instalación de actualizaciones solo permiten la instalación de actualizaciones aprobadas.

  Esta opción está desactivada de forma predeterminada.

- Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas

  Mantenga esta opción activada si está de acuerdo con la instalación de versiones de aplicaciones provisionales cuando sea necesario para instalar las actualizaciones seleccionadas.

  Si esta opción está desactivada, solo se instalarán las versiones seleccionadas de las aplicaciones. Desactive esta opción si desea actualizar las aplicaciones de una manera directa, sin intentar instalar versiones sucesivas de forma progresiva. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

  Por ejemplo, tiene la versión 3 de una aplicación instalada en un dispositivo y desea actualizarla a la versión 5, pero la versión 5 de esta aplicación solo se puede instalar sobre la versión 4. Si esta opción está activada, el software instala primero la versión 4 y luego la versión 5. Si esta opción está desactivada, el software no actualiza la aplicación.

  Esta opción está activada de forma predeterminada.

c. Haga clic en el botón **Añadir**.

- Para crear una tarea:

  a. Haga clic en el botón **Nueva tarea**.

  b. En la página que se abre, configure la nueva regla:

  - Regla de instalación para actualizaciones de este nivel de importancia

    A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

    Si esta opción está activada, las actualizaciones solucionan solo las vulnerabilidades cuyo nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

    Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

    Esta opción está desactivada de forma predeterminada.

  - Regla de instalación para actualizaciones de este nivel de importancia según MSRC

A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

Si esta opción está activada (disponible solo para las actualizaciones de Windows Update), las actualizaciones solucionan solo aquellas vulnerabilidades para las cuales el nivel de gravedad establecido por el Centro de respuesta de seguridad de Microsoft (MSRC) es igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

Esta opción está desactivada de forma predeterminada.

- Regla de instalación para las actualizaciones según este proveedor

  Esta opción está disponible solo para las actualizaciones de aplicaciones de terceros. Kaspersky Security Center instala solo las actualizaciones relacionadas con las aplicaciones del mismo proveedor que la actualización seleccionada. Las actualizaciones rechazadas y las actualizaciones de las aplicaciones de otros proveedores no se instalan.

  Esta opción está desactivada de forma predeterminada.

- **Regla de instalación para las actualizaciones de tipo**

- **Regla de instalación para la actualización seleccionada**

- Aprobar actualizaciones seleccionadas

  La actualización seleccionada será aprobada para su instalación. Active esta opción si algunas reglas aplicadas de instalación de actualizaciones solo permiten la instalación de actualizaciones aprobadas.

  Esta opción está desactivada de forma predeterminada.

- Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas

  Mantenga esta opción activada si está de acuerdo con la instalación de versiones de aplicaciones provisionales cuando sea necesario para instalar las actualizaciones seleccionadas.

  Si esta opción está desactivada, solo se instalarán las versiones seleccionadas de las aplicaciones. Desactive esta opción si desea actualizar las aplicaciones de una manera directa, sin intentar instalar versiones sucesivas de forma progresiva. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

  Por ejemplo, tiene la versión 3 de una aplicación instalada en un dispositivo y desea actualizarla a la versión 5, pero la versión 5 de esta aplicación solo se puede instalar sobre la versión 4. Si esta opción está activada, el software instala primero la versión 4 y luego la versión 5. Si esta opción está desactivada, el software no actualiza la aplicación.

  Esta opción está activada de forma predeterminada.

c. Haga clic en el botón **Añadir**.

Si ha elegido iniciar una tarea, puede cerrar el Asistente. La tarea se completará en modo de segundo plano. No se requieren más acciones.

Si eligió añadir una regla a una tarea existente, se abre la ventana de propiedades de la tarea. La nueva regla ya se añadió a las propiedades de la tarea. Puede ver o modificar la regla u otros ajustes de la configuración de tareas. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, siga creando la tarea en el Asistente para añadir tareas. La nueva regla que añadió en el Asistente para la instalación de actualizaciones se muestra en el Asistente para añadir tareas. Cuando completa el Asistente, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se añade a la lista de tareas.

Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas

A través de la tarea Buscar vulnerabilidades y actualizaciones requeridas, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones requeridas para el software de terceros instalado en los dispositivos administrados.

La tarea Buscar vulnerabilidades y actualizaciones requeridas se crea automáticamente cuando se ejecuta el Asistente de inicio rápido. Si no ejecutó el Asistente, puede crear la tarea manualmente.

Para crear la tarea Buscar vulnerabilidades y actualizaciones requeridas:

1. En la ventana principal de la aplicación, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Buscar vulnerabilidades y actualizaciones requeridas**.
4. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Seleccionar dispositivos a los que se asignará la tarea.
6. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.
7. Haga clic en el botón **Crear**.

   La tarea se crea y se muestra en la lista de tareas.
8. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.
9. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea.
10. En la pestaña **Configuración de la aplicación**, especifique la siguiente configuración:

    - **Buscar vulnerabilidades y actualizaciones en la lista de Microsoft**

Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

Por ejemplo, es posible que desee desactivar esta opción si tiene diferentes tareas con diferentes configuraciones para las actualizaciones de Microsoft y las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- **Conectar al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update en un dispositivo administrado se conecta al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como origen de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center (consulte la configuración de la directiva del Agente de red)
- Windows Server con Servicio de Windows Server Update (WSUS) de Microsoft desplegado en la red de su organización
- Servidores de actualización de Microsoft

Si se activa esta opción, el Agente de Windows Update en un dispositivo administrado se conecta al origen de actualizaciones de Microsoft para actualizar la información sobre las actualizaciones aplicables de Microsoft Windows.

Si se desactiva esta opción, el Agente de Windows Update en un dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que se recibió desde el origen de actualizaciones de Microsoft anteriormente y que se almacena en el caché del dispositivo.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Es posible que quiera desactivar esta opción si establece una conexión periódica a este origen de actualizaciones en otra tarea o en las propiedades de la directiva del Agente de red, en la sección **Vulnerabilidades y actualizaciones de software**. Si no desea desactivar esta opción, para reducir la sobrecarga del servidor, puede configurar la programación de tareas para aleatorizar el retraso del inicio de la tarea en 360 minutos.

Esta opción está activada de forma predeterminada.

La combinación de las siguientes opciones de la configuración de la directiva del Agente de red define el modo de obtener actualizaciones:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada y se selecciona la opción **Activo** en el grupo de configuración **Modo de búsqueda de Windows Update**.
- El Agente de Windows Update en un dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que se recibió del origen de actualizaciones de Microsoft anteriormente y que se almacena en el caché del dispositivo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada y se selecciona la opción **Pasivo** en el grupo de configuración **Modo de búsqueda de Windows Update** o si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está desactivada y se selecciona la opción **Activo** en el grupo de configuración **Modo de búsqueda de Windows Update**.
- Independientemente del estado de la opción **Conectar al servidor de actualizaciones para actualizar los datos** (activado o desactivado), si la opción **Desactivado**, se selecciona en el grupo de configuración **Modo de búsqueda de Windows Update**, Kaspersky Security Center no solicita ninguna información sobre actualizaciones.

- **Buscar vulnerabilidades y actualizaciones de terceros en la lista de Kaspersky**

  Si esta opción está activada, Kaspersky Security Center busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especificar rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky gestiona la lista completa de aplicaciones de terceros compatibles.

  Si esta opción está deshabilitada, Kaspersky Security Center no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Por ejemplo, es posible que desee desactivar esta opción si tiene diferentes tareas con diferentes configuraciones para las actualizaciones de Microsoft Windows y las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

- **Especifique rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Las carpetas en las que Kaspersky Security Center busca aplicaciones de terceros que requieren reparación de la vulnerabilidad e instalaciones de actualizaciones. Puede usar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- **Activar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe los seguimientos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los seguimientos se escriben en dos archivos a su vez; el tamaño total de ambos archivos se determina por el valor **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando ambos archivos están llenos, el Agente de red comienza a escribirles de nuevo. Los archivos con seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se escriben rastros adicionales.

  Al crear una tarea, no tiene que habilitar los diagnósticos avanzados. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está desactivada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky le pidan que cambie el valor predeterminado cuando la información de los archivos de diagnóstico avanzado que les envía no es suficiente para solucionar el problema.

11. Haga clic en el botón **Guardar**.

La tarea se crea y se configura.

Si los resultados de la tarea contienen una advertencia del error 0x80240033 "Error del Agente de Windows Update 80240033 ("No se pudieron descargar los términos de licencia")", puede resolver este problema a través del registro de Windows.

Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente cuando se ejecuta el Asistente de inicio rápido. Si no ejecutó el Asistente, puede crear la tarea manualmente.

Además de la configuración de tarea general, puede especificar la siguiente configuración al crear la tarea *Buscar vulnerabilidades y actualizaciones requeridas* o más adelante, al configurar las propiedades de la tarea creada:

- **Buscar vulnerabilidades y actualizaciones en la lista de Microsoft**

  Al buscar vulnerabilidades y actualizaciones, Kaspersky Security Center utiliza la información sobre las actualizaciones de Microsoft aplicables desde la fuente de actualizaciones de Microsoft, las cuales están disponibles en este momento.

  Por ejemplo, es posible que desee desactivar esta opción si tiene diferentes tareas con diferentes configuraciones para las actualizaciones de Microsoft y las actualizaciones de aplicaciones de terceros.

  Esta opción está activada de forma predeterminada.

- **Conectar al servidor de actualizaciones para actualizar los datos**

El Agente de Windows Update en un dispositivo administrado se conecta al origen de actualizaciones de Microsoft. Los siguientes servidores pueden actuar como origen de actualizaciones de Microsoft:

- Servidor de administración de Kaspersky Security Center (consulte la configuración de la directiva del Agente de red)
- Windows Server con Servicio de Windows Server Update (WSUS) de Microsoft desplegado en la red de su organización
- Servidores de actualización de Microsoft

Si se activa esta opción, el Agente de Windows Update en un dispositivo administrado se conecta al origen de actualizaciones de Microsoft para actualizar la información sobre las actualizaciones aplicables de Microsoft Windows.

Si se desactiva esta opción, el Agente de Windows Update en un dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que se recibió desde el origen de actualizaciones de Microsoft anteriormente y que se almacena en el caché del dispositivo.

Conectarse al origen de actualizaciones de Microsoft puede consumir muchos recursos. Es posible que quiera desactivar esta opción si establece una conexión periódica a este origen de actualizaciones en otra tarea o en las propiedades de la directiva del Agente de red, en la sección **Vulnerabilidades y actualizaciones de software**. Si no desea desactivar esta opción, para reducir la sobrecarga del servidor, puede configurar la programación de tareas para aleatorizar el retraso del inicio de la tarea en 360 minutos.

Esta opción está activada de forma predeterminada.

La combinación de las siguientes opciones de la configuración de la directiva del Agente de red define el modo de obtener actualizaciones:

- El Agente de Windows Update en un dispositivo administrado se conecta al Servidor de actualizaciones para obtener actualizaciones solo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada y se selecciona la opción **Activo** en el grupo de configuración **Modo de búsqueda de Windows Update**.
- El Agente de Windows Update en un dispositivo administrado usa la información sobre las actualizaciones de Microsoft Windows aplicables que se recibió del origen de actualizaciones de Microsoft anteriormente y que se almacena en el caché del dispositivo si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está activada y se selecciona la opción **Pasivo** en el grupo de configuración **Modo de búsqueda de Windows Update** o si la opción **Conectar al servidor de actualizaciones para actualizar los datos** está desactivada y se selecciona la opción **Activo** en el grupo de configuración **Modo de búsqueda de Windows Update**.
- Independientemente del estado de la opción **Conectar al servidor de actualizaciones para actualizar los datos** (activado o desactivado), si la opción **Desactivado**, se selecciona en el grupo de configuración **Modo de búsqueda de Windows Update**, Kaspersky Security Center no solicita ninguna información sobre actualizaciones.

- Buscar vulnerabilidades y actualizaciones de terceros en la lista de Kaspersky

Si esta opción está activada, Kaspersky Security Center busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) en el Registro de Windows y en las carpetas especificadas en **Especificar rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**. Kaspersky gestiona la lista completa de aplicaciones de terceros compatibles.

Si esta opción está deshabilitada, Kaspersky Security Center no busca vulnerabilidades y actualizaciones necesarias para aplicaciones de terceros. Por ejemplo, es posible que desee desactivar esta opción si tiene diferentes tareas con diferentes configuraciones para las actualizaciones de Microsoft Windows y las actualizaciones de aplicaciones de terceros.

Esta opción está activada de forma predeterminada.

- **Especifique rutas para la búsqueda avanzada de aplicaciones en el sistema de archivos**

  Las carpetas en las que Kaspersky Security Center busca aplicaciones de terceros que requieren reparación de la vulnerabilidad e instalaciones de actualizaciones. Puede usar variables del sistema.

  Especifique las carpetas en las que se instalan las aplicaciones. De forma predeterminada, la lista contiene carpetas del sistema en las que se instalan la mayoría de las aplicaciones.

- **Activar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe los seguimientos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los seguimientos se escriben en dos archivos a su vez; el tamaño total de ambos archivos se determina por el valor **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando ambos archivos están llenos, el Agente de red comienza a escribirles de nuevo. Los archivos con seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se escriben rastros adicionales.

  Al crear una tarea, no tiene que habilitar los diagnósticos avanzados. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está desactivada de forma predeterminada.

- **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky le pidan que cambie el valor predeterminado cuando la información de los archivos de diagnóstico avanzado que les envía no es suficiente para solucionar el problema.

Recomendaciones sobre la programación de tareas

Al programar la tarea *Buscar vulnerabilidades y actualizaciones requeridas*, asegúrese de que estén activadas dos opciones: **Ejecutar tareas no realizadas** y **Usar el retraso aleatorio automáticamente para el inicio de tareas**.

De forma predeterminada, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* está configurada para que comience a las 18:00. Si las reglas del espacio de trabajo de la organización estipulan que todos los dispositivos se apagan a esa hora, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará una vez que los dispositivos se enciendan nuevamente, es decir, la mañana siguiente. Tal actividad puede ser indeseable porque un análisis de vulnerabilidades puede aumentar la carga en los subsistemas del disco y las CPU. Debe configurar la programación más cómoda para la tarea según las reglas del lugar de trabajo adoptadas en la organización.

Crear la tarea Instalar actualizaciones necesarias y corregir vulnerabilidades

La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para actualizar y corregir vulnerabilidades en software de terceros, incluido el software de Microsoft, instalado en los dispositivos administrados. Esta tarea le permite instalar múltiples actualizaciones y corregir múltiples vulnerabilidades de acuerdo con ciertas reglas.

Para instalar actualizaciones o reparar vulnerabilidades por medio de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede realizar una de las acciones siguientes:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.
- Crear de una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Añada una regla para la instalación de actualizaciones a una tarea existente de *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.
4. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Seleccionar dispositivos a los que se asignará la tarea.
6. Especifique las reglas para la instalación de la actualización y luego especifique los siguientes ajustes:

   - **Iniciar la instalación al reiniciar o apagar el dispositivo**

     Si esta opción está activada, las actualizaciones se instalan cuando el dispositivo se reinicia o se apaga. De lo contrario, las actualizaciones se instalan de acuerdo con una programación.

     Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento del dispositivo.

     Esta opción está desactivada de forma predeterminada.

- Instalar los componentes generales del sistema necesarios

  Si esta opción está activada, antes de instalar una actualización, la aplicación instala automáticamente todos los componentes generales del sistema (requisitos previos) que se requieren para instalar la actualización. Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo

  Si esta opción está desactivada, es posible que tenga que instalar los requisitos previos de manera manual.

  Esta opción está desactivada de forma predeterminada.

- Autorizar la instalación de las nuevas versiones de la aplicación durante las actualizaciones

  Si esta opción está activada, las actualizaciones se permiten cuando dan lugar a la instalación de una nueva versión de una aplicación de software.

  Si esta opción se desactiva, el software no se actualiza. A continuación, puede instalar nuevas versiones del software de manera manual o mediante otra tarea. Por ejemplo, puede usar esta opción si la infraestructura de su empresa no es compatible con una nueva versión del software o si desea verificar una actualización en una infraestructura de prueba.

  Esta opción está activada de forma predeterminada.

  > La actualización de una aplicación puede causar un mal funcionamiento de las aplicaciones dependientes instaladas en los dispositivos cliente.

- Descargar actualizaciones en el dispositivo sin instalarlas

  Si esta opción está activada, la aplicación descarga actualizaciones en el dispositivo pero no las instala automáticamente. A continuación, puede instalar las actualizaciones descargadas de manera manual.

  Las actualizaciones de Microsoft se descargan al sistema de almacenamiento de Windows. Las actualizaciones de aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) se descargan en la carpeta especificada en el campo de **Carpeta para la descarga de actualizaciones**.

  Si esta opción está desactivada, las actualizaciones se instalan en el dispositivo automáticamente.

  Esta opción está desactivada de forma predeterminada.

  - Carpeta para la descarga de actualizaciones

    Esta carpeta se utiliza para descargar actualizaciones de aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft).

- Activar diagnóstico avanzado

Si esta función está habilitada, el Agente de red escribe los seguimientos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los seguimientos se escriben en dos archivos a su vez; el tamaño total de ambos archivos se determina por el valor **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando ambos archivos están llenos, el Agente de red comienza a escribirles de nuevo. Los archivos con seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se escriben rastros adicionales.

Al crear una tarea, no tiene que habilitar los diagnósticos avanzados. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

Esta opción está desactivada de forma predeterminada.

- Tamaño máximo, en MB, de los archivos de diagnóstico avanzado

  El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky le pidan que cambie el valor predeterminado cuando la información de los archivos de diagnóstico avanzado que les envía no es suficiente para solucionar el problema.

7. Especifique la configuración de reinicio del sistema operativo:

- No reiniciar el dispositivo

  Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- Reiniciar el dispositivo

  Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- Solicitar al usuario una acción

  En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

  Esta opción está seleccionada de forma predeterminada.

- Repetir solicitud cada (min)

Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

Si esta opción está desactivada, la solicitud se muestra solo una vez.

- **Reiniciar después de (min)**

  Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

  Las aplicaciones se cierran a la fuerza cuando el dispositivo del usuario se bloquea (bien manualmente o bien automáticamente cuando transcurre el intervalo de inactividad especificado).

  Si se selecciona esta opción, las aplicaciones del dispositivo bloqueado se cierran a la fuerza cuando transcurre el intervalo de tiempo especificado en el campo de entrada.

  Si esta opción está desactivada, las aplicaciones del dispositivo bloqueado no se cerrarán.

  Esta opción está desactivada de forma predeterminada.

8. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.
9. Haga clic en el botón **Finalizar**.

   La tarea se crea y se muestra en la lista de tareas.
10. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.
11. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea que se ajuste a sus necesidades.
12. Haga clic en el botón **Guardar**.

    La tarea se crea y se configura.

Si los resultados de la tarea contienen una advertencia del error 0x80240033 "Error del Agente de Windows Update 80240033 ("No se pudieron descargar los términos de licencia")", puede resolver este problema a través del registro de Windows.

Añadir una regla para la instalación de actualizaciones

Esta función solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

Al instalar actualizaciones de software o reparar vulnerabilidades de software utilizando la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, debe especificar reglas para la instalación de la actualización. Estas reglas determinan qué actualizaciones instalar y qué vulnerabilidades reparar.

La configuración exacta depende de si añade una regla para todas las actualizaciones de Windows Update o para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft). Al añadir una regla para aplicaciones de Windows Update o aplicaciones de terceros, puede seleccionar aplicaciones específicas y versiones de aplicaciones para las que desee instalar actualizaciones. Al añadir una regla para todas las actualizaciones, puede seleccionar las actualizaciones específicas que desee instalar y las vulnerabilidades que desee reparar mediante la instalación de actualizaciones.

Puede añadir una regla para la instalación de actualizaciones de las siguientes formas:

- Añada una regla al crear una nueva tarea de Instalar actualizaciones requeridas y reparar vulnerabilidades.
- Añada una regla en la pestaña **Configuración de la aplicación** en la ventana de propiedades de una tarea de *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.
- Mediante el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

Para añadir una nueva regla para todas las actualizaciones:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el Asistente utilizando el botón Siguiente.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página de **criterios generales**, use las listas desplegables para especificar las siguientes configuraciones:

   - **Conjunto de actualizaciones para instalar**

     Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:
     - **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

   - **Reparar vulnerabilidades con un nivel de gravedad igual o mayor que**

     A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

     Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

     Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

     Esta opción está desactivada de forma predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones para instalar:

- **Instalar todas las actualizaciones pertinentes**

  Instalar todas las actualizaciones de software que cumplan con los criterios especificados en la página de **Criterios generales** del Asistente. Seleccionado de forma predeterminada.

- **Instalar solo las actualizaciones de la lista**

  Instalar solo actualizaciones de software que seleccione manualmente desde la lista. Esta lista contiene todas las actualizaciones de software disponibles.

  Por ejemplo, puede desear seleccionar actualizaciones específicas en los casos siguientes: comprobar su instalación en un entorno de prueba, actualizar solo aplicaciones críticas o actualizar solo aplicaciones específicas.

  - **Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas**

    Mantenga esta opción activada si está de acuerdo con la instalación de versiones de aplicaciones provisionales cuando sea necesario para instalar las actualizaciones seleccionadas.

    Si esta opción está desactivada, solo se instalarán las versiones seleccionadas de las aplicaciones. Desactive esta opción si desea actualizar las aplicaciones de una manera directa, sin intentar instalar versiones sucesivas de forma progresiva. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

    Por ejemplo, tiene la versión 3 de una aplicación instalada en un dispositivo y desea actualizarla a la versión 5, pero la versión 5 de esta aplicación solo se puede instalar sobre la versión 4. Si esta opción está activada, el software instala primero la versión 4 y luego la versión 5. Si esta opción está desactivada, el software no actualiza la aplicación.

    Esta opción está activada de forma predeterminada.

5. En la página de **Vulnerabilidades**, seleccione las vulnerabilidades que se corregirán al instalar las actualizaciones seleccionadas:

- **Reparar todas las vulnerabilidades que coinciden con otros criterios**

  Reparar todas las vulnerabilidades que cumplan con los criterios especificados en la página de **Criterios generales** del Asistente. Seleccionado de forma predeterminada.

- **Reparar solo las vulnerabilidades de la lista**

  Solucione solo las vulnerabilidades que seleccione manualmente de la lista. Esta lista contiene todas las vulnerabilidades detectadas.

  Por ejemplo, es posible que desee seleccionar vulnerabilidades específicas en los siguientes casos: para verificar su corrección en un entorno de prueba, para corregir vulnerabilidades solo en aplicaciones críticas o para corregir vulnerabilidades solo en aplicaciones específicas.

6. En la página **Nombre**, especifique el nombre de la regla que está añadiendo. Más tarde, puede cambiar este nombre en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para añadir tareas.

Para añadir una nueva regla para las actualizaciones de Windows Update:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el Asistente utilizando el botón Siguiente.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página de **criterios generales**, especifique la siguiente configuración:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:

     - **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

   - Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

     A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

     Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

     Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

     Esta opción está desactivada de forma predeterminada.

   - Reparar vulnerabilidades con un nivel de gravedad MSRC igual o mayor que

     A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

     Si esta opción está activada, las actualizaciones solucionan solo aquellas vulnerabilidades para las cuales el nivel de gravedad establecido por el Centro de respuesta de seguridad de Microsoft (MSRC) es igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

     Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

     Esta opción está desactivada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desea instalar actualizaciones. De forma predeterminada, todas las aplicaciones están seleccionadas.

5. En la página **Categorías de actualizaciones**, seleccione las actualizaciones para instalar. Estas categorías están igual que en Microsoft Update Catalog. De forma predeterminada, todas las categorías están seleccionadas.

6. En la página **Nombre**, especifique el nombre de la regla que está añadiendo. Más tarde, puede cambiar este nombre en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para añadir tareas.

Para añadir una nueva regla para las actualizaciones de aplicaciones de terceros:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el Asistente utilizando el botón Siguiente.

2. En la página **Tipo de regla**, seleccione **Regla para actualizaciones de terceros**.

3. En la página de **criterios generales**, especifique la siguiente configuración:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:

     - **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

   - Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

     A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

     Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

     Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

     Esta opción está desactivada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desea instalar actualizaciones. De forma predeterminada, todas las aplicaciones están seleccionadas.

5. En la página **Nombre**, especifique el nombre de la regla que está añadiendo. Más tarde, puede cambiar este nombre en la sección Configuración de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para añadir tareas.

Crear la tarea Instalar actualizaciones de Windows Update

La tarea *Instalar actualizaciones de Windows Update* le permite instalar actualizaciones de software que proporciona el servicio de Windows Update en dispositivos administrados.

Si no tiene la licencia de Administración de vulnerabilidades y parches, no puede crear nuevas tareas del tipo *Instalar actualizaciones de Windows Update*. Para instalar nuevas actualizaciones, puede añadirlas a una tarea *Instalar actualizaciones de Windows Update* existente. Le recomendamos que utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en lugar de la tarea *Instalar actualizaciones de Windows Update*. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* le permite instalar varias actualizaciones y corregir varias vulnerabilidades automáticamente, de acuerdo con las reglas que defina. Además, esta tarea le permite instalar actualizaciones de proveedores de software distintos de Microsoft.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Para crear la tarea Instalar actualizaciones de Windows Update:

1. En la ventana principal de la aplicación, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Instalar actualizaciones de Windows Update**.
4. Especifique el nombre para la tarea que está creando.

   El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Seleccionar dispositivos a los que se asignará la tarea.
6. Haga clic en el botón **Añadir**.

   Se abre la lista de actualizaciones.
7. Especifique las actualizaciones de Windows Update que desea instalar. A continuación, haga clic en **Aceptar**.
8. Especifique la configuración de reinicio del sistema operativo:

   - **No reiniciar el dispositivo**

     Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

   - **Reiniciar el dispositivo**

Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

  En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  Si esta opción está desactivada, la solicitud se muestra solo una vez.

- **Reiniciar después de (min)**

  Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

9. Especifique la configuración de la cuenta:

- **Cuenta predeterminada**

  La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

  Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

- **Cuenta**

  Cuenta bajo la que se ejecuta la tarea.

- **Contraseña**

  La contraseña de la cuenta bajo la cual la tarea se ejecutará.

10. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

11. Haga clic en el botón **Finalizar**.

    La tarea se crea y se muestra en la lista de tareas.

12. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea que se ajuste a sus necesidades.

14. Haga clic en el botón **Guardar**.

La tarea se crea y se configura.

Visualización de información sobre actualizaciones de software de terceros disponibles

Puede ver la lista de actualizaciones disponibles para el software de terceros, incluido el software de Microsoft, instalado en los dispositivos cliente.

Para ver una lista de actualizaciones disponibles para las aplicaciones de terceros instaladas en dispositivos cliente:

1. Seleccione **OPERACIONES** → **ADMINISTRACIÓN DE PARCHES**.

2. Seleccione **ACTUALIZACIONES DE SOFTWARE** en la lista desplegable.

   Aparece una lista de actualizaciones disponibles.

Puede especificar un filtro para ver la lista de actualizaciones de software. Haga clic en el icono **Filtro** ( ) en la esquina superior derecha de la lista de actualizaciones de software para administrar el filtro. También puede seleccionar uno de los filtros preestablecidos de la lista desplegable de **Preestablecer filtros** en la lista de vulnerabilidades de software.

Para consultar las propiedades de una actualización:

1. Haga clic en el nombre de la actualización de software requerida.

2. Se abre la ventana de propiedades de la actualización, que muestra las siguientes pestañas:

- **Control de aplicaciones**

  Esta pestaña muestra los detalles generales de la actualización seleccionada:

  - Estado de aprobación de la actualización (se puede cambiar de forma manual, basta con seleccionar un nuevo estado en la lista desplegable)
  - Categoría de Windows Server Update Services (WSUS) a la que pertenece la actualización
  - Fecha y hora en que se registró la actualización
  - Fecha y hora en que se creó la actualización
  - Nivel de importancia de la actualización
  - Requisitos de instalación impuestos por la actualización
  - Familia de aplicaciones a la que pertenece la actualización
  - Aplicación a la que se aplica la actualización
  - Número de revisión de la actualización

- **Atributos**

  Esta pestaña muestra un conjunto de atributos que puede utilizar para obtener más información sobre la actualización seleccionada. Este conjunto es diferente si la actualización la publica Microsoft o un proveedor externo.

  La pestaña muestra la siguiente información para una actualización de Microsoft:

  - Nivel de importancia de la actualización definido por Microsoft Security Response Center (MSRC)
  - Enlace al artículo de Microsoft Knowledge Base que describe la actualización
  - Enlace al artículo del boletín de seguridad de Microsoft que describe la actualización
  - Identificador de la actualización (ID).

  La pestaña muestra la siguiente información para una actualización de terceros:

  - Si la actualización es un parche o un paquete de distribución completo
  - Idioma de localización de la actualización
  - Si la actualización se instala automática o manualmente
  - Si la actualización se revocó después de aplicarse
  - Enlace para descargar la actualización

- **Dispositivos**

  Esta pestaña muestra una lista de dispositivos en donde se instaló la actualización seleccionada.

- **Vulnerabilidades reparadas**

  Esta pestaña muestra una lista de vulnerabilidades que la actualización seleccionada puede corregir.

- **Cruce de actualizaciones**

  Esta pestaña muestra posibles solapamientos entre varias actualizaciones publicadas para la misma aplicación, es decir, si la actualización seleccionada puede reemplazar a otras actualizaciones o, viceversa, ser reemplazada por otras actualizaciones (disponible solo para actualizaciones de Microsoft).

- **Tareas para instalar esta actualización**

  Esta pestaña muestra una lista de tareas cuyo alcance incluye la instalación de la actualización seleccionada. La pestaña también le permite crear una nueva tarea de instalación remota para la actualización.

Siga estos pasos para consultar las estadísticas de una instalación de actualización:

1. Seleccione la casilla de verificación junto a la actualización de software requerida.
2. Haga clic en el botón **Estadísticas del estado de instalación de las actualizaciones**.

Se muestra el diagrama de los estados de instalación de la actualización. Al hacer clic en un estado, se abre una lista de dispositivos en los que la actualización tiene el estado seleccionado.

Puede ver información sobre las actualizaciones de software disponibles para el software de terceros, incluido el software de Microsoft, instalado en el dispositivo administrado seleccionado que ejecuta Windows.

Para ver una lista de actualizaciones disponibles para el software de terceros instalado en el dispositivo administrado seleccionado:

1. Seleccione **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el enlace con el nombre del dispositivo para el que desea ver las actualizaciones de software de terceros.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades de la cuenta de usuario, seleccione la pestaña **Avanzado**.
4. En el panel izquierdo, seleccione la sección **Actualizaciones disponibles**. Si desea ver solo las actualizaciones instaladas, seleccione la casilla de verificación **Mostrar las actualizaciones instaladas**.

Se muestra la lista de actualizaciones de software de terceros disponibles para el dispositivo seleccionado.

Exportación de la lista de actualizaciones de software disponibles a un archivo

Puede exportar la lista de actualizaciones para software de terceros, incluido el software de Microsoft, que se muestra en este momento a los archivos CSV o TXT. Puede utilizar estos archivos, por ejemplo, para enviarlos a su administrador de seguridad de la información o para almacenarlos con fines estadísticos.

Para exportar a un archivo de texto la lista de actualizaciones disponibles para software de terceros instalado en todos los dispositivos administrados, realice lo siguiente:

1. En la pestaña **OPERACIONES**, en la lista desplegable **ADMINISTRACIÓN DE PARCHES**, seleccione **ACTUALIZACIONES DE SOFTWARE**.

   La página muestra una lista de actualizaciones disponibles para software de terceros instalado en todos los dispositivos administrados.

2. Haga clic en el botón **Exportar filas a un archivo TXT** o **Exportar filas a un archivo CSV**, según el formato al que prefiera exportar.

El archivo que contiene la lista de actualizaciones disponibles para software de terceros, incluido el software de Microsoft, se descarga en el dispositivo que está utilizando.

Para exportar a un archivo de texto la lista de actualizaciones disponibles para software de terceros instalado en el dispositivo administrado seleccionado, realice lo siguiente:

1. Abra la lista de actualizaciones de software de terceros disponibles en el dispositivo administrado seleccionado.

2. Seleccione las actualizaciones de software que desea exportar.

   Omita este paso si desea exportar una lista completa de actualizaciones de software.

   Si desea exportar una lista completa de actualizaciones de software, solo se exportarán las actualizaciones que se muestran en la página actual.

   Si desea exportar solo las actualizaciones instaladas, seleccione la casilla de verificación **Mostrar las actualizaciones instaladas**.

3. Haga clic en el botón **Exportar filas a un archivo TXT** o **Exportar filas a un archivo CSV**, según el formato al que prefiera exportar.

El archivo que contiene la lista de actualizaciones de software de terceros instaladas en el dispositivo administrado seleccionado, incluido el software de Microsoft, se descarga en el dispositivo que está utilizando.

Aprobar y rechazar actualizaciones de software de terceros

Cuando configura la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede crear una regla que requiera que las actualizaciones que están por instalarse tengan un estado específico. Por ejemplo, una regla de actualizaciones puede permitir la instalación de lo siguiente:

- Solo actualizaciones aprobadas
- Solo actualizaciones aprobadas e indefinidas

- Todas las actualizaciones independientemente de los estados de actualización

Puede aprobar las actualizaciones que deben instalarse y rechazar las actualizaciones que no deben instalarse.

El uso del estado *Aprobado* para administrar la instalación de actualizaciones es eficiente para una pequeña cantidad de actualizaciones. Para instalar varias actualizaciones, utilice las reglas que puede configurar en la tarea *Instalar actualizaciones requeridas y corregir vulnerabilidades*. Le recomendamos que asigne el estado *Aprobado* solo a aquellas actualizaciones específicas que no cumplan con los criterios especificados en las reglas. Cuando aprueba manualmente una gran cantidad de actualizaciones, el rendimiento del Servidor de administración disminuye y puede provocar una sobrecarga en el Servidor de administración.

Aprobar o rechazar una o varias actualizaciones:

1. En el menú principal, vaya a **OPERACIONES → ADMINISTRACIÓN DE PARCHES** y, en la lista desplegable, seleccione **ACTUALIZACIONES DE SOFTWARE**.

   Aparece una lista de actualizaciones disponibles.

2. Seleccione las actualizaciones que desea aprobar o rechazar.

3. Haga clic en **Aprobar** para aprobar las actualizaciones seleccionadas o **Rechazar** para rechazar las actualizaciones seleccionadas.

   El valor predeterminado es *Sin definir*.

Las actualizaciones seleccionadas tienen los estados que usted haya definido.

Como opción, puede cambiar el estado de aprobación en las propiedades de una actualización específica.

Para aprobar o rechazar una actualización en sus propiedades:

1. En el menú principal, vaya a **OPERACIONES → ADMINISTRACIÓN DE PARCHES** y, en la lista desplegable, seleccione **ACTUALIZACIONES DE SOFTWARE**.

   Aparece una lista de actualizaciones disponibles.

2. Haga clic en el nombre de la actualización que desea aprobar o rechazar.

   Se abrirá la ventana de propiedades de la actualización.

3. En la sección **Control de aplicaciones**, seleccione un estado para la actualización cambiando la opción **Estado de aprobación de la actualización**. Puede seleccionar el estado *Aprobada*, *Rechazada* o *Sin definir*.

4. Haga clic en el botón **Guardar** para guardar los cambios.

La actualización seleccionada tiene el estado que usted definió.

Si configura el estado **Rechazada** para las actualizaciones de software de terceros, estas actualizaciones no se instalarán en los dispositivos cuya instalación se haya planeado pero aún no se haya realizado. Las actualizares permanecerán en los dispositivos en los cuales ya se hayan instalado. Si debe eliminarlas, puede eliminarlas manualmente en forma local.

Crear la tarea Realizar la sincronización de Windows Update

La tarea *Realizar la sincronización de Windows Update* solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

La tarea *Realizar la sincronización de Windows Update* es necesaria si desea utilizar el Servidor de administración como servidor WSUS. En este caso, el Servidor de administración descarga las actualizaciones de Windows a la base de datos y proporciona las actualizaciones de Windows Update a los dispositivos cliente en el modo centralizado a través de Agentes de red. Si la red no usa ningún servidor WSUS, cada dispositivo cliente descargará por su cuenta las actualizaciones de Microsoft desde servidores externos.

La tarea *Realizar la sincronización de Windows Update* solo descarga metadatos de los servidores de Microsoft. Durante la tarea de instalación de la actualización, Kaspersky Security Center descarga solo las actualizaciones que usted ha elegido instalar.

Al ejecutar la tarea **Realizar la sincronización de Windows Update**, la aplicación recibe una lista de actualizaciones en vigor desde un servidor de actualizaciones de Microsoft. A continuación, Kaspersky Security Center recopila una lista de actualizaciones que se han quedado obsoletas. En el próximo inicio de la tarea **Buscar vulnerabilidades y actualizaciones requeridas**, Kaspersky Security Center marca todas las actualizaciones obsoletas y define un plazo para eliminarlas. En el próximo inicio de la tarea **Realizar la sincronización de Windows Update**, se eliminan todas las actualizaciones marcadas para su eliminación hace 30 días. Kaspersky Security Center también comprueba si hay actualizaciones obsoletas que se marcaron para su eliminación hace más de 180 días y luego elimina esas actualizaciones más antiguas.

Cuando se completa la tarea **Realizar la sincronización de Windows Update** y se eliminan las actualizaciones obsoletas, la base de datos puede seguir teniendo los códigos hash correspondientes a los archivos de las actualizaciones eliminadas, así como los archivos correspondientes en los archivos %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (si se descargaron antes). Puede ejecutar la tarea **Mantenimiento del Servidor de administración** para eliminar estos registros obsoletos de la base de datos y los archivos correspondientes.

Para crear la tarea Realizar la sincronización de Windows Update:

1. En la ventana principal de la aplicación, vaya a **DISPOSITIVOS → TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Realizar la sincronización de Windows Update**.
4. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Active la opción **Descargar archivos de instalación rápida** si desea que los archivos de actualización rápida se descarguen al ejecutar la tarea.

   Cuando Kaspersky Security Center sincroniza actualizaciones con Servidores de actualizaciones de Microsoft Windows, la información sobre todos los archivos se guarda en la base de datos del Servidor de administración. Todos los archivos necesarios para una actualización también se descargan en la unidad de disco durante la interacción con el Agente de Windows Update. En particular, Kaspersky Security Center guarda la información sobre archivos de actualización express en la base de datos y los descarga cuando sea necesario. Descargar archivos de actualización express supone reducir el espacio libre en la unidad de disco.

   Para evitar que disminuya el volumen del espacio de disco y reducir el tráfico, desactive la opción **Descargar archivos de instalación rápida**.
6. Seleccione las aplicaciones cuyas actualizaciones desea descargar.

Si la casilla **Todas las aplicaciones** se selecciona, las actualizaciones se descargarán para todas las aplicaciones existentes y para todas las aplicaciones que se puedan lanzar en el futuro.

7. Seleccione las categorías de actualizaciones que desea descargar en el Servidor de administración.

   Si la casilla **Todas las categorías** se selecciona, las actualizaciones se descargarán para todas las categorías de actualizaciones existentes y para todas las categorías que puedan aparecer en el futuro.

8. Seleccione los idiomas de localización de las actualizaciones que desea descargar en el Servidor de administración. Seleccione una de las siguientes opciones:

   - **Descargar todos los idiomas, incluso los nuevos**

     Si esta opción está seleccionada, todos los idiomas de localización disponibles de las actualizaciones que se descargarán en el Servidor de administración. Esta opción está seleccionada de forma predeterminada.

   - **Descargar los idiomas seleccionados**

     Si esta opción está seleccionada, puede realizar selecciones en la lista de idiomas de localización de las actualizaciones que se deben descargar en el Servidor de administración.

9. Especifique qué cuenta usar al ejecutar la tarea. Seleccione una de las siguientes opciones:

   - **Cuenta preconfigurada**

     La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

     Esta opción está seleccionada de forma predeterminada.

   - **Especificar cuenta**

     Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

10. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

11. Haga clic en el botón **Finalizar**.

    La tarea se crea y se muestra en la lista de tareas.

12. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea que se ajuste a sus necesidades.

14. Haga clic en el botón **Guardar**.

La tarea se crea y se configura.

Actualización automática de aplicaciones de terceros

Algunas aplicaciones de terceros se pueden actualizar automáticamente. El proveedor de aplicaciones define si la aplicación es compatible o no con la función de actualización automática. Si una aplicación de terceros instalada en un dispositivo administrado es compatible con la actualización automática, puede especificar la configuración de actualización automática en las propiedades de la aplicación. Después de cambiar la configuración de actualización automática, los Agentes de red aplican la nueva configuración en cada dispositivo administrado en el que está instalada la aplicación.

La configuración de actualización automática es independiente de los otros objetos y las configuraciones de la función Administración de vulnerabilidades y parches. Por ejemplo, esta configuración no depende del estado de aprobación de la actualización o de las tareas de instalación de la actualización, como *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

Para configurar la configuración de actualización automática de una aplicación de terceros:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → REGISTRO DE APLICACIONES**.

2. Haga clic en el nombre de la aplicación para la que desea cambiar la configuración de actualización automática.

   Para simplificar la búsqueda, puede filtrar la lista mediante la columna **Estado de las actualizaciones automáticas**.

   Se abrirá la ventana de propiedades de la aplicación.

3. En la sección **Control de aplicaciones**, seleccione un valor para la siguiente configuración:

   Estado de las actualizaciones automáticas

   Seleccione una de las siguientes opciones:

   - **Sin definir**

     La función de actualización automática está desactivada. Kaspersky Security Center instala actualizaciones de aplicaciones de terceros mediante el uso de las siguientes tareas: *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

   - **Permitido**

     Una vez que el proveedor lanza una actualización para la aplicación, esta actualización se instala en los dispositivos administrados automáticamente. No se requieren acciones adicionales.

   - **Bloqueado**

     Las actualizaciones de la aplicación no se instalan automáticamente. Kaspersky Security Center instala actualizaciones de aplicaciones de terceros mediante el uso de las siguientes tareas: *Instalar actualizaciones requeridas y reparar vulnerabilidades*, *Instalar actualizaciones de Windows Update* y *Reparar vulnerabilidades*.

4. Haga clic en el botón **Guardar** para guardar los cambios.

La configuración de actualización automática se aplica a la aplicación seleccionada.

Arreglar vulnerabilidades de software de terceros

Esta sección describe las características de Kaspersky Security Center que se relacionan con la reparación de vulnerabilidades en el software instalado en dispositivos administrados.

Escenario: búsqueda y reparación de vulnerabilidades de software de terceros

Esta sección proporciona un escenario para encontrar y corregir vulnerabilidades en los dispositivos administrados que ejecutan Windows. Puede encontrar y corregir vulnerabilidades de software en el sistema operativo y en el software de terceros, incluido el software de Microsoft.

Requisitos previos

- Kaspersky Security Center se ha implementado en su organización.
- Hay dispositivos administrados que ejecutan Windows en su organización.
- Se requiere conexión a Internet para que el Servidor de administración realice las siguientes tareas:
  - Para hacer una lista de reparaciones recomendadas para vulnerabilidades en el software de Microsoft. Los especialistas de Kaspersky crean y actualizan periódicamente la lista.
  - Para reparar vulnerabilidades en software de terceros que no sea el software de Microsoft.

Etapas

Encontrar y corregir vulnerabilidades de software transcurre en etapas:

1. **Análisis en busca de vulnerabilidades en el software instalado en los dispositivos administrados**

   Para buscar vulnerabilidades en el software instalado en los dispositivos administrados, ejecute la tarea *Buscar vulnerabilidades y actualizaciones requeridas*. Cuando se completa esta tarea, Kaspersky Security Center recibe las listas de vulnerabilidades detectadas y las actualizaciones necesarias para el software de terceros instalado en los dispositivos que especificó en las propiedades de la tarea.

   La tarea *Buscar vulnerabilidades y actualizaciones requeridas* se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Si no ejecutó el Asistente, hágalo ahora o cree la tarea manualmente.

   Instrucciones:

   - Consola de administración: Análisis de aplicaciones para buscar vulnerabilidades, Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas
   - Kaspersky Security Center 14 Web Console: Crear la tarea Buscar vulnerabilidades y actualizaciones requeridas, Configuración de la tarea Buscar vulnerabilidades y actualizaciones requeridas

2. **Análisis de la lista de vulnerabilidades de software detectadas**

Vea la lista de **Vulnerabilidades de software** y decida qué vulnerabilidades se repararán. Para ver información detallada sobre cada vulnerabilidad, haga clic en el nombre de la vulnerabilidad en la lista. Para cada vulnerabilidad de la lista, también puede ver las estadísticas sobre la vulnerabilidad en los dispositivos administrados.

Instrucciones:

- Consola de administración: visualización de vulnerabilidades de software de información, visualización de estadísticas de vulnerabilidades en dispositivos administrados
- Kaspersky Security Center 14 Web Console: Consultar información sobre vulnerabilidades de software, Visualización de estadísticas de vulnerabilidades en dispositivos administrados

3 Configuración de reparación de vulnerabilidades

Cuando se detectan las vulnerabilidades de software, puede corregirlas en los dispositivos administrados mediante la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o la tarea *Reparar vulnerabilidades*.

La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para actualizar y corregir vulnerabilidades en software de terceros, incluido el software de Microsoft, instalado en los dispositivos administrados. Esta tarea le permite instalar múltiples actualizaciones y corregir múltiples vulnerabilidades de acuerdo con ciertas reglas. Tenga en cuenta que esta tarea se puede crear únicamente si tiene la licencia para la función Administración de vulnerabilidades y parches. Para corregir vulnerabilidades de software, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* utiliza actualizaciones de software recomendadas.

La tarea *Reparar vulnerabilidades* no requiere la opción de licencia para la función Administración de vulnerabilidades y parches. Para utilizar esta tarea, debe especificar manualmente las correcciones del usuario para las vulnerabilidades en el software de terceros que figuran en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza correcciones recomendadas para el software de Microsoft y correcciones de usuario para software de terceros.

Puede iniciar el Asistente de reparación de vulnerabilidades que crea una de estas tareas automáticamente, o puede crear una de estas de forma manual.

Instrucciones:

- Consola de administración: selección de soluciones de usuario para vulnerabilidades en software de terceros, reparación de vulnerabilidades en aplicaciones
- Kaspersky Security Center 14 Web Console: selección de soluciones de usuario para vulnerabilidades en el software de terceros, reparación de vulnerabilidades en software de terceros, creación de la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades

4 Programar las tareas

Para asegurarse de que la lista de vulnerabilidades esté siempre actualizada, programe la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para ejecutarla automáticamente de vez en cuando. La frecuencia media recomendada es de una vez a la semana.

Si ha creado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* puede programarla para que se ejecute con la misma frecuencia que la tarea *Buscar vulnerabilidades y actualizaciones requeridas* o con menos frecuencia. Al programar la tarea *Reparar vulnerabilidades*, tenga en cuenta que debe seleccionar soluciones para el software de Microsoft o especificar soluciones de usuario para el software de terceros cada vez antes de comenzar la tarea.

Cuando programe las tareas, asegúrese de que una tarea para solucionar una vulnerabilidad comience después de que se complete la tarea *Buscar vulnerabilidades y actualizaciones requeridas*.

5 Ignorar las vulnerabilidades de software (opcional)

Si lo desea, puede ignorar vulnerabilidades de software que reparar en todos los dispositivos administrados o solo en determinados dispositivos administrados.

Instrucciones:

- Consola de administración: ignorar las vulnerabilidades de software
- Kaspersky Security Center 14 Web Console: Ignorar las vulnerabilidades de software

6. **Ejecución de una tarea de reparación de la vulnerabilidad**

   Inicie las tareas *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Reparar vulnerabilidad*. Cuando complete la tarea, asegúrese de que tenga el estado *Completado correctamente* en la lista de tareas.

7. **Crear un informe de los resultados de la reparación de vulnerabilidades de software (opcional)**

   Para ver estadísticas detalladas sobre la reparación de vulnerabilidades, genere el Informe de vulnerabilidades. El informe muestra detalles acerca de vulnerabilidades de software que no se corrigen. De esta manera, puede aprender cómo buscar y corregir vulnerabilidades de software de terceros, incluido el software de Microsoft, en su organización.

   Instrucciones:

   - Consola de administración: Creación y visualización de un informe
   - Kaspersky Security Center 14 Web Console: Generación y visualización de un informe

8. **Comprobar la configuración de la búsqueda y reparar vulnerabilidades en software de terceros**

   Asegúrese de haber hecho lo siguiente:

   - Obtenido y revisado la lista de vulnerabilidades de software detectadas en los dispositivos administrados
   - Ignorado las vulnerabilidades de software si así lo deseaba
   - Configurado la tarea para reparar vulnerabilidades
   - Programado las tareas de encontrar y reparar vulnerabilidades de software para que comiencen secuencialmente
   - Comprobado que se haya ejecutado la tarea para reparar vulnerabilidades de software

Resultados

Si ha creado y configurado la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, las vulnerabilidades se reparan automáticamente en los dispositivos administrados. Cuando se ejecuta la tarea, esta compara la lista de actualizaciones de software disponibles con las reglas especificadas en la configuración de la tarea. Todas las actualizaciones de software que cumplan con los criterios especificados en las reglas se descargarán en el repositorio del Servidor de administración y se instalarán para reparar las vulnerabilidades de software.

Si ha creado la tarea *Reparar vulnerabilidades*, solo se corrigen las vulnerabilidades de software de Microsoft.

Acerca de encontrar y corregir vulnerabilidades de software

Kaspersky Security Center detecta y corrige vulnerabilidades de software en dispositivos administrados que ejecutan los sistemas operativos de las familias Microsoft Windows. Se detectan vulnerabilidades en el sistema operativo y en el software de terceros, incluido el software de Microsoft.

Encontrar vulnerabilidades de software

Para encontrar vulnerabilidades de software, Kaspersky Security Center utiliza características de la base de datos de vulnerabilidades conocidas. Esta base de datos es creada por especialistas de Kaspersky. Contiene información sobre vulnerabilidades, como descripción de vulnerabilidades, fecha de detección de vulnerabilidades, nivel de gravedad de vulnerabilidades. Puede consultar los detalles de las vulnerabilidades de software en el sitio web de Kaspersky.

Kaspersky Security Center utiliza la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para buscar vulnerabilidades de software.

Corregir vulnerabilidades de software

Para corregir vulnerabilidades de software, Kaspersky Security Center utiliza actualizaciones de software emitidas por los proveedores de software. Los metadatos de las actualizaciones de software se descargan en el repositorio del Servidor de administración después de que se ejecuten las siguientes tareas:

- *Descargar actualizaciones en el repositorio del Servidor de administración*. Esta tarea tiene como objetivo la descarga de metadatos de actualizaciones para software de Kaspersky y de terceros. Esta tarea se crea automáticamente con el Asistente de inicio rápido de Kaspersky Security Center. Puede crear la tarea Descargar actualizaciones en el repositorio del Servidor de administración manualmente.

- *Realizar la sincronización de Windows Update*. Esta tarea tiene como objetivo la descarga de metadatos de actualizaciones para software de Microsoft.

Las actualizaciones de software para corregir vulnerabilidades se pueden representar como paquetes de distribución completos o parches. Las actualizaciones de software que corrigen vulnerabilidades de software se denominan *correcciones*. Las *soluciones recomendadas* son aquellas que los especialistas de Kaspersky recomiendan para la instalación. Las *correcciones de usuario* son aquellas que se especifican manualmente para la instalación por parte de los usuarios. Para instalar un arreglo de usuario, debe crear un paquete de instalación que contenga este arreglo.

Si tiene la licencia de Kaspersky Security Center con la función Administración de vulnerabilidades y parches para corregir las vulnerabilidades de software, puede usar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Esta tarea corrige automáticamente múltiples vulnerabilidades instalando las correcciones recomendadas. Para esta tarea, puede configurar manualmente ciertas reglas para corregir múltiples vulnerabilidades.

Si no tiene la licencia de Kaspersky Security Center con la función Administración de vulnerabilidades y parches para corregir las vulnerabilidades de software, puede usar la tarea *Reparar vulnerabilidades*. Mediante esta tarea, puede corregir vulnerabilidades instalando correcciones recomendadas para el software de Microsoft y correcciones de usuario para otro software de terceros.

Por razones de seguridad, las tecnologías de Kaspersky analizan automáticamente en busca de malware cualquier actualización de software de terceros que instale mediante la función Administración de vulnerabilidades y parches. Estas tecnologías se utilizan para la verificación automática de archivos e incluyen análisis antivirus, análisis estático, análisis dinámico, análisis de comportamiento en un entorno aislado y aprendizaje automático.

Los expertos de Kaspersky no realizan análisis manuales de las actualizaciones de software de terceros que puedan instalarse mediante la función Administración de vulnerabilidades y parches. Además, los expertos de Kaspersky no buscan vulnerabilidades (conocidas o desconocidas) o funciones no documentadas en dichas actualizaciones, ni realizan otros tipos de análisis de las actualizaciones distintos a los especificados en el párrafo anterior.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Para reparar algunas vulnerabilidades de software, debe aceptar el Contrato de licencia de usuario final (EULA) para instalar el software si se solicita la aceptación del EULA. Si rechaza el EULA, la vulnerabilidad de software no se repara.

Arreglar vulnerabilidades de software de terceros

Después de obtener la lista de vulnerabilidades de software, puede corregirlas en los dispositivos administrados que ejecutan Windows. Puede corregir las vulnerabilidades de software en el sistema operativo y en software de terceros, incluido el software de Microsoft, mediante la creación y ejecución de la tarea *Reparar vulnerabilidades* o la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

> Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Como opción, puede crear una tarea para corregir las vulnerabilidades de software de las siguientes maneras:

- Abra la lista de vulnerabilidades y especifique qué vulnerabilidades hay que corregir.

  Como resultado, se crea una nueva tarea para corregir las vulnerabilidades de software. Como opción, puede añadir las vulnerabilidades seleccionadas a una tarea existente.

- Abra el Asistente de reparación de vulnerabilidades.

  > El Asistente de reparación de vulnerabilidades solo está disponibles bajo la licencia de Administración de vulnerabilidades y parches.

  El Asistente simplifica la creación y configuración de una tarea de reparación de la vulnerabilidad y le permite eludir la creación de tareas redundantes que contienen las mismas actualizaciones para instalar.

Solucionar vulnerabilidades de software mediante el uso de la lista de vulnerabilidades

Para corregir vulnerabilidades de software:

1. Abra una de las listas de vulnerabilidades:

   - Para abrir la lista general de vulnerabilidades, vaya a **OPERACIONES** → **ADMINISTRACIÓN DE PARCHES** → **Vulnerabilidades de software**.

   - Para abrir la lista de vulnerabilidades de un dispositivo administrado, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS** → <nombre del dispositivo> → **Avanzado** → **Vulnerabilidades de software**.

   - Para abrir la lista de vulnerabilidades de una aplicación específica, vaya a **OPERACIONES** → **APLICACIONES DE TERCEROS** → **REGISTRO DE APLICACIONES** → <nombre de la aplicación> → **Vulnerabilidades**.

   Se muestra una página con una lista de vulnerabilidades en el software de terceros.

2. Seleccione una o varias vulnerabilidades en la lista y liego haga clic en el botón **Reparar vulnerabilidad**.

Si la actualización de software recomendada para reparar una de las vulnerabilidades seleccionadas está ausente, se muestra un mensaje de información.

Para reparar algunas vulnerabilidades de software, debe aceptar el Contrato de licencia de usuario final (EULA) para el software de instalación si se solicita la aceptación del EULA. Si rechaza el EULA, la vulnerabilidad de software no se repara.

3. Seleccione una de las siguientes opciones:

   - **Nueva tarea**

     Se inicia Asistente para añadir tarea. Si tiene la licencia de Administración de vulnerabilidades y parches, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* está preseleccionada. Si no tiene la licencia, la tarea *Reparar vulnerabilidades* está preseleccionada. Siga los pasos del Asistente para completar la creación de la tarea.

   - **Reparar vulnerabilidad (añadir regla a tarea específica)**

     Seleccione una tarea a la que desee añadir las vulnerabilidades seleccionadas. Si tiene la licencia de Administración de vulnerabilidades y parches, seleccione una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Una nueva regla para reparar las vulnerabilidades seleccionadas se añadirá automáticamente a la tarea seleccionada. Si no tiene la licencia, seleccione una tarea *Reparar vulnerabilidades*. Las vulnerabilidades seleccionadas se añadirán a las propiedades de la tarea.

     Se abrirá la ventana de propiedades de la tarea. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, la tarea se crea y se muestra en la lista de tareas en **DISPOSITIVOS** → **TAREAS**. Si eligió añadir las vulnerabilidades a una tarea existente, las vulnerabilidades se guardan en las propiedades de la tarea.

Para reparar las vulnerabilidades de software de terceros, inicie la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* o *Reparar vulnerabilidades*. Si ha creado la tarea *Reparar vulnerabilidades*, debe especificar manualmente las actualizaciones de software para reparar las vulnerabilidades de software que figuran en la configuración de tarea.

Solucionar vulnerabilidades de software mediante el Asistente de reparación de vulnerabilidades

El Asistente de reparación de vulnerabilidades solo está disponibles bajo la licencia de Administración de vulnerabilidades y parches.

Para corregir las vulnerabilidades de software mediante el Asistente de reparación de vulnerabilidades:

1. En la pestaña **OPERACIONES**, en la lista desplegable **ADMINISTRACIÓN DE PARCHES**, seleccione **Vulnerabilidades de software**.

   Se muestra una página con una lista de vulnerabilidades en el software de terceros instalado en dispositivos administrados.

2. Seleccione la casilla de verificación al lado de las vulnerabilidades que desea reparar.

3. Haga clic en el botón **Ejecutar Asistente de reparación de vulnerabilidades**.

   Se inicia el Asistente de reparación de vulnerabilidades. La página **Seleccionar tarea de reparación de la vulnerabilidad** muestra la lista de todas las tareas existentes de los siguientes tipos:

   - *Instalar actualizaciones requeridas y reparar vulnerabilidades*
   - *Instalar actualizaciones de Windows Update*

- *Reparar vulnerabilidades*

No puede modificar los dos últimos tipos de tareas para instalar nuevas actualizaciones. Para instalar nuevas actualizaciones, solo puede utilizar la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

4. Si desea que el Asistente muestre solo las tareas que reparan la vulnerabilidad que ha seleccionado, habilite la opción **Mostrar solo las tareas que reparen esta vulnerabilidad**.

5. Elija lo que quiere hacer:

   - Para iniciar una tarea, seleccione la casilla de verificación junto al nombre de la tarea y luego haga clic en el botón **Iniciar**.

   - Para añadir una nueva regla a una tarea existente:

     a. Seleccione la casilla de verificación junto al nombre de la tarea y luego haga clic en el botón **Añadir regla**.

     b. En la página que se abre, configure la nueva regla:

     - Regla para reparar vulnerabilidades de este nivel de gravedad

       A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

       Si esta opción está activada, las actualizaciones solucionan solo las vulnerabilidades cuyo nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

       Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

       Esta opción está desactivada de forma predeterminada.

     - **Regla para reparar vulnerabilidades mediante actualizaciones del mismo tipo que la actualización definida como recomendada para la vulnerabilidad seleccionada** (disponible solo para vulnerabilidades de software de Microsoft)

     - **Regla para reparar vulnerabilidades en aplicaciones del proveedor seleccionado** (disponible solo para las vulnerabilidades de software de terceros)

     - **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada** (disponible solo para las vulnerabilidades de software de terceros)

     - **Regla para reparar vulnerabilidad seleccionada**

     - Aprobar actualizaciones que reparen esta vulnerabilidad

       La actualización seleccionada será aprobada para su instalación. Active esta opción si algunas reglas aplicadas de instalación de actualizaciones solo permiten la instalación de actualizaciones aprobadas.

       Esta opción está desactivada de forma predeterminada.

     c. Haga clic en el botón **Añadir**.

- Para crear una tarea:

  a. Haga clic en el botón **Nueva tarea**.

  b. En la página que se abre, configure la nueva regla:

  - Regla para reparar vulnerabilidades de este nivel de gravedad

    A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

    Si esta opción está activada, las actualizaciones solucionan solo las vulnerabilidades cuyo nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

    Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

    Esta opción está desactivada de forma predeterminada.

  - **Regla para reparar vulnerabilidades mediante actualizaciones del mismo tipo que la actualización definida como recomendada para la vulnerabilidad seleccionada** (disponible solo para vulnerabilidades de software de Microsoft)

  - **Regla para reparar vulnerabilidades en aplicaciones del proveedor seleccionado** (disponible solo para las vulnerabilidades de software de terceros)

  - **Regla para reparar una vulnerabilidad en todas las versiones de la aplicación seleccionada** (disponible solo para las vulnerabilidades de software de terceros)

  - **Regla para reparar vulnerabilidad seleccionada**

  - Aprobar actualizaciones que reparen esta vulnerabilidad

    La actualización seleccionada será aprobada para su instalación. Active esta opción si algunas reglas aplicadas de instalación de actualizaciones solo permiten la instalación de actualizaciones aprobadas.

    Esta opción está desactivada de forma predeterminada.

  c. Haga clic en el botón **Añadir**.

Si ha elegido iniciar una tarea, puede cerrar el Asistente. La tarea se completará en modo de segundo plano. No se requieren más acciones.

Si eligió añadir una regla a una tarea existente, se abre la ventana de propiedades de la tarea. La nueva regla ya se añadió a las propiedades de la tarea. Puede ver o modificar la regla u otros ajustes de la configuración de tareas. Haga clic en el botón **Guardar** para guardar los cambios.

Si eligió crear una tarea, siga creando la tarea en el Asistente para añadir tareas. La nueva regla que añadió en el Asistente de reparación de vulnerabilidades se muestra en el Asistente para añadir tareas. Cuando completa el Asistente, la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se añade a la lista de tareas.

Crear la tarea Reparar vulnerabilidades.

La tarea *Reparar vulnerabilidades* le permite corregir vulnerabilidades de software en dispositivos administrados que ejecutan Windows. Puede corregir vulnerabilidades de software en el software de terceros, incluido el software de Microsoft.

Si no tiene la licencia de Administración de vulnerabilidades y parches, no puede crear nuevas tareas del tipo *Reparar vulnerabilidades*. Para corregir nuevas vulnerabilidades, puede añadirlas a una tarea existente *Reparar vulnerabilidades*. Le recomendamos que utilice la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* en lugar de la tarea *Reparar vulnerabilidades*. La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* le permite instalar varias actualizaciones y corregir varias vulnerabilidades automáticamente, de acuerdo con las reglas que defina.

Es posible que se requiera una interacción del usuario al actualizar una aplicación de terceros o corregir una vulnerabilidad en una aplicación de terceros en un dispositivo administrado. Por ejemplo, se le puede solicitar al usuario que cierre la aplicación de terceros si se encuentra abierta.

Para crear la tarea Reparar vulnerabilidades:

1. En la ventana principal de la aplicación, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance por el Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Reparar vulnerabilidades**.
4. Especifique el nombre para la tarea que está creando.

   El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Seleccionar dispositivos a los que se asignará la tarea.
6. Haga clic en el botón **Añadir**.

   Se abre la lista de vulnerabilidades.
7. Especifique las vulnerabilidades que desea reparar. A continuación, haga clic en **Aceptar**.

   Las vulnerabilidades de software de Microsoft suelen tener reparaciones recomendadas. No se requieren acciones adicionales para ellas. Para las vulnerabilidades de software de otros proveedores, primero debe especificar una reparación de usuario para cada vulnerabilidad que desee reparar. Después de eso, podrá añadir esas vulnerabilidades a la tarea *Reparar vulnerabilidades*.
8. Especifique la configuración de reinicio del sistema operativo:

   - **No reiniciar el dispositivo**

     Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- **Reiniciar el dispositivo**

  Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

  En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  Si esta opción está desactivada, la solicitud se muestra solo una vez.

- **Reiniciar después de (min)**

  Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Forzar el cierre de las aplicaciones en sesiones bloqueadas**

  La ejecución de aplicaciones puede impedir el reinicio del dispositivo cliente. Por ejemplo, si se está editando un documento en una aplicación de procesamiento de textos y no se lo guarda, la aplicación no permitirá que el dispositivo se reinicie.

  Si esta opción está activada, dichas aplicaciones en un dispositivo bloqueado son forzadas a cerrar antes de reiniciar el dispositivo. Como resultado, los usuarios pueden perder los cambios no guardados.

  Si esta opción está desactivada, no se reiniciará un dispositivo bloqueado. El estado de la tarea en este dispositivo indica que se requiere un reinicio del dispositivo. Los usuarios tienen que cerrar de forma manual todas las aplicaciones que se ejecutan en dispositivos bloqueados y reiniciar estos dispositivos.

  Esta opción está desactivada de forma predeterminada.

9. Especifique la configuración de la cuenta:

- **Cuenta predeterminada**

La tarea se ejecutará bajo la misma cuenta donde se ejecuta la aplicación de esta tarea.

Esta opción está seleccionada de forma predeterminada.

- **Especificar cuenta**

  Rellene los campos **Cuenta** y **Contraseña** para especificar los detalles de la cuenta en la que se ejecuta la tarea. La cuenta debe tener los derechos suficientes para esta tarea.

- **Cuenta**

  Cuenta bajo la que se ejecuta la tarea.

- **Contraseña**

  La contraseña de la cuenta bajo la cual la tarea se ejecutará.

10. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

11. Haga clic en el botón **Finalizar**.

    La tarea se crea y se muestra en la lista de tareas.

12. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

13. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea que se ajuste a sus necesidades.

14. Haga clic en el botón **Guardar**.

La tarea se crea y se configura.

Crear la tarea Instalar actualizaciones necesarias y corregir vulnerabilidades

La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

La tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades* se utiliza para actualizar y corregir vulnerabilidades en software de terceros, incluido el software de Microsoft, instalado en los dispositivos administrados. Esta tarea le permite instalar múltiples actualizaciones y corregir múltiples vulnerabilidades de acuerdo con ciertas reglas.

Para instalar actualizaciones o reparar vulnerabilidades por medio de la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, puede realizar una de las acciones siguientes:

- Ejecute el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

- Crear de una tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*.
- Añada una regla para la instalación de actualizaciones a una tarea existente de *Instalar actualizaciones requeridas y reparar vulnerabilidades*.

Para crear la tarea Instalar actualizaciones requeridas y reparar vulnerabilidades:

1. En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
3. Para la aplicación Kaspersky Security Center, seleccione el tipo de tarea **Instalar actualizaciones requeridas y reparar vulnerabilidades**.
4. Especifique el nombre para la tarea que está creando. El nombre de la tarea no puede contener más de 100 caracteres y no puede incluir ningún carácter especial (como "*<>?\:|).
5. Seleccionar dispositivos a los que se asignará la tarea.
6. Especifique las reglas para la instalación de la actualización y luego especifique los siguientes ajustes:
   - **Iniciar la instalación al reiniciar o apagar el dispositivo**

     Si esta opción está activada, las actualizaciones se instalan cuando el dispositivo se reinicia o se apaga. De lo contrario, las actualizaciones se instalan de acuerdo con una programación.

     Utilice esta opción si la instalación de las actualizaciones podría afectar el rendimiento del dispositivo.

     Esta opción está desactivada de forma predeterminada.
   - **Instalar los componentes generales del sistema necesarios**

     Si esta opción está activada, antes de instalar una actualización, la aplicación instala automáticamente todos los componentes generales del sistema (requisitos previos) que se requieren para instalar la actualización. Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo

     Si esta opción está desactivada, es posible que tenga que instalar los requisitos previos de manera manual.

     Esta opción está desactivada de forma predeterminada.
   - **Autorizar la instalación de las nuevas versiones de la aplicación durante las actualizaciones**

Si esta opción está activada, las actualizaciones se permiten cuando dan lugar a la instalación de una nueva versión de una aplicación de software.

Si esta opción se desactiva, el software no se actualiza. A continuación, puede instalar nuevas versiones del software de manera manual o mediante otra tarea. Por ejemplo, puede usar esta opción si la infraestructura de su empresa no es compatible con una nueva versión del software o si desea verificar una actualización en una infraestructura de prueba.

Esta opción está activada de forma predeterminada.

La actualización de una aplicación puede causar un mal funcionamiento de las aplicaciones dependientes instaladas en los dispositivos cliente.

- **Descargar actualizaciones en el dispositivo sin instalarlas**

  Si esta opción está activada, la aplicación descarga actualizaciones en el dispositivo pero no las instala automáticamente. A continuación, puede instalar las actualizaciones descargadas de manera manual.

  Las actualizaciones de Microsoft se descargan al sistema de almacenamiento de Windows. Las actualizaciones de aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft) se descargan en la carpeta especificada en el campo de **Carpeta para la descarga de actualizaciones**.

  Si esta opción está desactivada, las actualizaciones se instalan en el dispositivo automáticamente.

  Esta opción está desactivada de forma predeterminada.

  - **Carpeta para la descarga de actualizaciones**

    Esta carpeta se utiliza para descargar actualizaciones de aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft).

- **Activar diagnóstico avanzado**

  Si esta función está habilitada, el Agente de red escribe los seguimientos incluso si el seguimiento está desactivado para el Agente de red en la Utilidad de diagnóstico remoto de Kaspersky Security Center. Los seguimientos se escriben en dos archivos a su vez; el tamaño total de ambos archivos se determina por el valor **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**. Cuando ambos archivos están llenos, el Agente de red comienza a escribirles de nuevo. Los archivos con seguimiento se almacenan en la carpeta %WINDIR%\Temp. Se puede acceder a estos archivos en la utilidad de diagnóstico remoto, puede descargarlos o eliminarlos allí.

  Si esta función está desactivada, el Agente de red escribe rastros de acuerdo con la configuración de la Utilidad de diagnóstico remoto de Kaspersky Security Center. No se escriben rastros adicionales.

  Al crear una tarea, no tiene que habilitar los diagnósticos avanzados. Es posible que desee utilizar esta función más adelante si, por ejemplo, una ejecución de tarea falla en algunos de los dispositivos y desea recopilar información adicional durante otra ejecución de tarea.

  Esta opción está desactivada de forma predeterminada.

  - **Tamaño máximo, en MB, de los archivos de diagnóstico avanzado**

    El valor predeterminado es 100 MB, y los valores disponibles están entre 1 MB y 2048 MB. Es posible que los especialistas del Servicio de soporte técnico de Kaspersky le pidan que cambie el valor predeterminado cuando la información de los archivos de diagnóstico avanzado que les envía no es suficiente para solucionar el problema.

7. Especifique la configuración de reinicio del sistema operativo:

- **No reiniciar el dispositivo**

  Los dispositivos cliente no se reinician automáticamente después de la operación. Para completar la operación, debe reiniciar un dispositivo (por ejemplo, manualmente o a través de la tarea de administración de un dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas en servidores y otros dispositivos donde la operación continua tiene importancia crítica.

- **Reiniciar el dispositivo**

  Los dispositivos cliente siempre se reinician automáticamente si se requiere un reinicio para completar la operación. Esta opción es útil para las tareas en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**

  En la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). Esta opción es más adecuada para estaciones de trabajo donde los usuarios deben poder seleccionar el momento más conveniente para un reinicio.

  Esta opción está seleccionada de forma predeterminada.

- **Repetir solicitud cada (min)**

  Si esta opción está activada, la aplicación solicita al usuario que reinicie el sistema operativo con la frecuencia especificada.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 5 minutos. Los valores disponibles están entre 1 y 1440 minutos.

  Si esta opción está desactivada, la solicitud se muestra solo una vez.

- **Reiniciar después de (min)**

  Después de preguntar al usuario, la aplicación fuerza el reinicio del sistema operativo al expirar el intervalo de tiempo especificado.

  Esta opción está activada de forma predeterminada. El intervalo predeterminado es 30 minutos. Los valores disponibles están entre 1 y 1440 minutos.

- **Tiempo de espera antes del cierre forzado de aplicaciones en sesiones bloqueadas (min)**

  Las aplicaciones se cierran a la fuerza cuando el dispositivo del usuario se bloquea (bien manualmente o bien automáticamente cuando transcurre el intervalo de inactividad especificado).

  Si se selecciona esta opción, las aplicaciones del dispositivo bloqueado se cierran a la fuerza cuando transcurre el intervalo de tiempo especificado en el campo de entrada.

  Si esta opción está desactivada, las aplicaciones del dispositivo bloqueado no se cerrarán.

  Esta opción está desactivada de forma predeterminada.

8. Si desea modificar la configuración de tareas predeterminada, active la opción **Abrir los detalles de la tarea cuando se complete la creación** en la página **Finalizar la creación de tareas**. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

9. Haga clic en el botón **Finalizar**.

   La tarea se crea y se muestra en la lista de tareas.

10. Haga clic en el nombre de la tarea creada para abrir la ventana de propiedades de la tarea.

11. En la ventana de propiedades de la tarea, especifique la configuración general de la tarea que se ajuste a sus necesidades.

12. Haga clic en el botón **Guardar**.

    La tarea se crea y se configura.

Si los resultados de la tarea contienen una advertencia del error 0x80240033 "Error del Agente de Windows Update 80240033 ("No se pudieron descargar los términos de licencia")", puede resolver este problema a través del registro de Windows.

Añadir una regla para la instalación de actualizaciones

Esta función solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

Al instalar actualizaciones de software o reparar vulnerabilidades de software utilizando la tarea *Instalar actualizaciones requeridas y reparar vulnerabilidades*, debe especificar reglas para la instalación de la actualización. Estas reglas determinan qué actualizaciones instalar y qué vulnerabilidades reparar.

La configuración exacta depende de si añade una regla para todas las actualizaciones de Windows Update o para aplicaciones de terceros (aplicaciones creadas por proveedores de software distintos de Kaspersky y Microsoft). Al añadir una regla para aplicaciones de Windows Update o aplicaciones de terceros, puede seleccionar aplicaciones específicas y versiones de aplicaciones para las que desee instalar actualizaciones. Al añadir una regla para todas las actualizaciones, puede seleccionar las actualizaciones específicas que desee instalar y las vulnerabilidades que desee reparar mediante la instalación de actualizaciones.

Puede añadir una regla para la instalación de actualizaciones de las siguientes formas:

- Añada una regla al crear una nueva tarea de Instalar actualizaciones requeridas y reparar vulnerabilidades.
- Añada una regla en la pestaña **Configuración de la aplicación** en la ventana de propiedades de una tarea de *Instalar actualizaciones requeridas y reparar vulnerabilidades* existente.
- Mediante el Asistente de instalación de actualizaciones o el Asistente de reparación de vulnerabilidades.

Para añadir una nueva regla para todas las actualizaciones:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el Asistente utilizando el botón Siguiente.

2. En la página **Tipo de regla**, seleccione **Regla para todas las actualizaciones**.

3. En la página de **criterios generales**, use las listas desplegables para especificar las siguientes configuraciones:

- Conjunto de actualizaciones para instalar

  Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:

  - **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
  - **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
  - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

- Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

  A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

  Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

  Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

  Esta opción está desactivada de forma predeterminada.

4. En la página **Actualizaciones**, seleccione las actualizaciones para instalar:

- Instalar todas las actualizaciones pertinentes

  Instalar todas las actualizaciones de software que cumplan con los criterios especificados en la página de **Criterios generales** del Asistente. Seleccionado de forma predeterminada.

- Instalar solo las actualizaciones de la lista

  Instalar solo actualizaciones de software que seleccione manualmente desde la lista. Esta lista contiene todas las actualizaciones de software disponibles.

  Por ejemplo, puede desear seleccionar actualizaciones específicas en los casos siguientes: comprobar su instalación en un entorno de prueba, actualizar solo aplicaciones críticas o actualizar solo aplicaciones específicas.

  - Instalar automáticamente todas las actualizaciones anteriores de la aplicación que se requieren para instalar las actualizaciones seleccionadas

Mantenga esta opción activada si está de acuerdo con la instalación de versiones de aplicaciones provisionales cuando sea necesario para instalar las actualizaciones seleccionadas.

Si esta opción está desactivada, solo se instalarán las versiones seleccionadas de las aplicaciones. Desactive esta opción si desea actualizar las aplicaciones de una manera directa, sin intentar instalar versiones sucesivas de forma progresiva. Si no es posible instalar las actualizaciones seleccionadas sin instalar versiones anteriores de las aplicaciones, la actualización de la aplicación fallará.

Por ejemplo, tiene la versión 3 de una aplicación instalada en un dispositivo y desea actualizarla a la versión 5, pero la versión 5 de esta aplicación solo se puede instalar sobre la versión 4. Si esta opción está activada, el software instala primero la versión 4 y luego la versión 5. Si esta opción está desactivada, el software no actualiza la aplicación.

Esta opción está activada de forma predeterminada.

5. En la página de **Vulnerabilidades**, seleccione las vulnerabilidades que se corregirán al instalar las actualizaciones seleccionadas:

   - **Reparar todas las vulnerabilidades que coinciden con otros criterios**

     Reparar todas las vulnerabilidades que cumplan con los criterios especificados en la página de **Criterios generales** del Asistente. Seleccionado de forma predeterminada.

   - **Reparar solo las vulnerabilidades de la lista**

     Solucione solo las vulnerabilidades que seleccione manualmente de la lista. Esta lista contiene todas las vulnerabilidades detectadas.

     Por ejemplo, es posible que desee seleccionar vulnerabilidades específicas en los siguientes casos: para verificar su corrección en un entorno de prueba, para corregir vulnerabilidades solo en aplicaciones críticas o para corregir vulnerabilidades solo en aplicaciones específicas.

6. En la página **Nombre**, especifique el nombre de la regla que está añadiendo. Más tarde, puede cambiar este nombre en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para añadir tareas.

Para añadir una nueva regla para las actualizaciones de Windows Update:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el Asistente utilizando el botón Siguiente.

2. En la página **Tipo de regla**, seleccione **Regla para Windows Update**.

3. En la página de **criterios generales**, especifique la siguiente configuración:

   - **Conjunto de actualizaciones para instalar**

Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:

- **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
- **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
- **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

- Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

  A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

  Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

  Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

  Esta opción está desactivada de forma predeterminada.

- Reparar vulnerabilidades con un nivel de gravedad MSRC igual o mayor que

  A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

  Si esta opción está activada, las actualizaciones solucionan solo aquellas vulnerabilidades para las cuales el nivel de gravedad establecido por el Centro de respuesta de seguridad de Microsoft (MSRC) es igual o superior al valor seleccionado en la lista (**Bajo**, **Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

  Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

  Esta opción está desactivada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desea instalar actualizaciones. De forma predeterminada, todas las aplicaciones están seleccionadas.
5. En la página **Categorías de actualizaciones**, seleccione las actualizaciones para instalar. Estas categorías están igual que en Microsoft Update Catalog. De forma predeterminada, todas las categorías están seleccionadas.
6. En la página **Nombre**, especifique el nombre de la regla que está añadiendo. Más tarde, puede cambiar este nombre en la sección **Configuración** de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para añadir tareas.

Para añadir una nueva regla para las actualizaciones de aplicaciones de terceros:

1. Haga clic en el botón **Agregar**.

   Se inicia el Asistente de creación de reglas. Avance por el Asistente utilizando el botón Siguiente.

2. En la página **Tipo de regla**, seleccione **Regla para actualizaciones de terceros**.

3. En la página de **criterios generales**, especifique la siguiente configuración:

   - Conjunto de actualizaciones para instalar

     Seleccione las actualizaciones que deben instalarse en los dispositivos cliente:

     - **Instalar solo las actualizaciones aprobadas**: Esto instala solo las actualizaciones aprobadas.
     - **Instalar todas las actualizaciones (excepto las rechazadas)**. Esto instala actualizaciones con el estado de la aprobación *Aprobado* o *Indeterminado*.
     - **Instalar todas las actualizaciones (incluidas las rechazadas)**. Esto instala todas las actualizaciones, sin tener en cuenta su estado de aprobación. Seleccione esta opción con la precaución. Por ejemplo, utilice esta opción si desea comprobar la instalación de algunas actualizaciones rechazadas en una infraestructura de prueba.

   - Reparar vulnerabilidades con un nivel de gravedad igual o mayor que

     A veces las actualizaciones de software pueden perjudicar la experiencia del usuario con el software. En tales casos, puede decidir instalar solo esas actualizaciones que son críticas para el funcionamiento del software y omitir otras actualizaciones.

     Si esta opción se activa, las actualizaciones solucionan solo esas vulnerabilidades para las cuales el nivel de gravedad configurado por Kaspersky es igual o superior que el valor seleccionado en la lista (**Medio**, **Alto**, o **Crítico**). Las vulnerabilidades con un nivel de gravedad más bajo que el valor seleccionado no se solucionan.

     Si esta opción se desactiva, las actualizaciones solucionan todas las vulnerabilidades sin tener en cuenta su nivel de gravedad.

     Esta opción está desactivada de forma predeterminada.

4. En la página **Aplicaciones**, seleccione las aplicaciones y las versiones de las aplicaciones para las que desea instalar actualizaciones. De forma predeterminada, todas las aplicaciones están seleccionadas.

5. En la página **Nombre**, especifique el nombre de la regla que está añadiendo. Más tarde, puede cambiar este nombre en la sección Configuración de la ventana de propiedades de la tarea creada.

Una vez que el Asistente de creación de reglas finaliza su operación, la nueva regla se añade y se muestra en el campo del Asistente para añadir tareas.

Selección de soluciones de usuario para vulnerabilidades en software de terceros

Para usar la tarea *Reparar vulnerabilidades*, debe especificar manualmente las actualizaciones de software para reparar las vulnerabilidades en el software de terceros que se enumera en la configuración de la tarea. La tarea *Reparar vulnerabilidades* utiliza correcciones recomendadas para el software de Microsoft y correcciones de usuario para otro software de terceros. Las *correcciones de usuario* son actualizaciones de software para reparar vulnerabilidades que el administrador especifica manualmente para la instalación.

Para seleccionar las soluciones de usuario para vulnerabilidades en software de terceros:

1. En la pestaña **OPERACIONES**, en la lista desplegable **ADMINISTRACIÓN DE PARCHES**, seleccione **Vulnerabilidades de software**.

   La página muestra la lista de vulnerabilidades de software detectadas en los dispositivos cliente.

2. En la lista de vulnerabilidades de software, haga clic en el enlace con el nombre de la vulnerabilidad de software para la que desea especificar una corrección de usuario.

   Se abrirá la ventana de propiedades de la vulnerabilidad.

3. En el panel izquierdo, seleccione la sección **Reparaciones del usuario u otras reparaciones**.

   Se muestra la lista de soluciones de usuario para la vulnerabilidad de software seleccionada.

4. Haga clic en **Añadir**.

   Se muestra una lista disponible de paquetes de instalación. La lista de paquetes de instalación mostrados corresponde a la lista **OPERACIONES → REPOSITORIOS → PAQUETES DE INSTALACIÓN**. Si no ha creado un paquete de instalación que contenga la reparación del usuario para la vulnerabilidad seleccionada, ahora puede crear el paquete iniciando el Asistente de nuevo paquete.

5. Seleccione uno o más paquetes de instalación que contengan una o más reparaciones del usuario para la vulnerabilidad en el software de terceros.

6. Hacer clic en **Guardar**.

Se especifican los paquetes de instalación que contienen reparaciones de usuario para la vulnerabilidad de software. Cuando se inicie la tarea *Reparar vulnerabilidades*, se instalará el paquete de instalación y se reparará la vulnerabilidad de software.

Visualización de información sobre vulnerabilidades de software detectadas en todos los dispositivos administrados

Después de haber escaneado el software en los dispositivos administrados en busca de vulnerabilidades, puede ver la lista de vulnerabilidades de software detectadas en todos los dispositivos administrados.

Para ver una lista de las vulnerabilidades de software detectadas en todos los dispositivos administrados,

En la pestaña **OPERACIONES**, en la lista desplegable **ADMINISTRACIÓN DE PARCHES**, seleccione **Vulnerabilidades de software**.

La página muestra la lista de vulnerabilidades de software detectadas en los dispositivos cliente.

También puede generar y ver el Informe de vulnerabilidades.

Puede especificar un filtro para ver la lista de vulnerabilidades de software. Haga clic en el icono **Filtro** ( ) en la esquina superior derecha de la lista de vulnerabilidades de software para administrar el filtro. También puede seleccionar uno de los filtros preestablecidos de la lista desplegable de **Preestablecer filtros** en la lista de vulnerabilidades de software.

Puede obtener información detallada sobre cualquier vulnerabilidad de la lista.

Siga estos pasos para obtener información acerca de una vulnerabilidad de software:

En la lista de vulnerabilidades de software, haga clic en el enlace con el nombre de la vulnerabilidad.

Se abrirá la ventana de propiedades de la vulnerabilidad de software.

Visualización de información sobre vulnerabilidades de software detectadas en el dispositivo administrado seleccionado

Puede ver información sobre vulnerabilidades de software detectadas en el dispositivo administrado seleccionado que ejecuta Windows.

Para ver una lista de las vulnerabilidades de software detectadas en los dispositivos administrados seleccionados:

1. En el menú principal, vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el enlace con el nombre del dispositivo para el que desea ver las vulnerabilidades de software detectadas.

   Se muestra la ventana de propiedades del dispositivo seleccionado.

3. En la ventana de propiedades de la cuenta de usuario, seleccione la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

   Si desea ver solo las vulnerabilidades de software que se pueden reparar, seleccione la opción **Mostrar solo las vulnerabilidades que se pueden reparar.**

Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo administrado seleccionado.

Para ver las propiedades de la vulnerabilidad de software seleccionada,

haga clic en el enlace con el nombre de la vulnerabilidad de software en la lista de vulnerabilidades de software.

Se mostrará la ventana de propiedades de la vulnerabilidad de software seleccionado.

Visualización de estadísticas de vulnerabilidades en dispositivos administrados

Puede ver estadísticas para cada vulnerabilidad de software en dispositivos administrados. Las estadísticas se representan como un diagrama. El diagrama muestra la cantidad de dispositivos con los siguientes estados:

- *Ignorado en: <número de dispositivos>*. El estado se asigna si, en las propiedades de vulnerabilidad, ha configurado manualmente la opción para ignorar la vulnerabilidad.
- *Reparado en: <número de dispositivos>*. El estado se asigna si la tarea para reparar la vulnerabilidad se ha completado correctamente.
- *Arreglo programado en:<número de dispositivos>*. El estado se asigna si ha creado la tarea para corregir la vulnerabilidad pero la tarea aún no se ha realizado.

- *Parche aplicado en:* <número de dispositivos>. El estado se asigna si ha seleccionado manualmente una actualización de software para corregir la vulnerabilidad pero este software actualizado no ha solucionado la vulnerabilidad.

- *Arreglo requerido en:<número de dispositivos>*. El estado se asigna si la vulnerabilidad se reparó solo en la parte de los dispositivos administrados y se requiere que se repare en la parte restante de los dispositivos administrados.

Para ver las estadísticas de una vulnerabilidad en dispositivos administrados:

1. En la pestaña **OPERACIONES**, en la lista desplegable **ADMINISTRACIÓN DE PARCHES**, seleccione **Vulnerabilidades de software**.

   La página muestra una lista de vulnerabilidades en las aplicaciones detectadas en dispositivos administrados.

2. Seleccione la casilla de verificación junto a la vulnerabilidad requerida.

3. Haga clic en el botón **Estadísticas de vulnerabilidades en dispositivos**.

Se muestra un diagrama de los estados de vulnerabilidad. Al hacer clic en un estado, se abre una lista de dispositivos en los que la vulnerabilidad tiene el estado seleccionado.

Exportación de una lista de vulnerabilidades de software a un archivo

Puede exportar la lista de vulnerabilidades que se muestra a los archivos CSV o TXT. Puede utilizar estos archivos, por ejemplo, para enviarlos a su administrador de seguridad de la información o para almacenarlos con fines estadísticos.

Para exportar una lista de las vulnerabilidades de software detectadas en todos los dispositivos administrados a un archivo de texto:

1. En la pestaña **OPERACIONES**, en la lista desplegable **ADMINISTRACIÓN DE PARCHES**, seleccione **Vulnerabilidades de software**.

   La página muestra una lista de vulnerabilidades en las aplicaciones detectadas en dispositivos administrados.

2. Haga clic en el botón **Exportar filas a un archivo TXT** o **Exportar filas a un archivo CSV**, según el formato al que prefiera exportar.

El archivo que contiene la lista de vulnerabilidades de software se descarga en el dispositivo que utiliza en este momento.

Para exportar una lista de las vulnerabilidades de software detectadas en el dispositivo administrado seleccionado a un archivo de texto:

1. Abra la lista de las vulnerabilidades de software detectadas en todos los dispositivos administrados.

2. Seleccione las vulnerabilidades de software que desea exportar.

   Omita este paso si desea exportar una lista completa de vulnerabilidades de software detectadas en el dispositivo administrado.

   Si desea exportar la lista completa de vulnerabilidades de software detectadas en el dispositivo administrado, solo se exportarán las vulnerabilidades que se muestran en la página actual.

3. Haga clic en el botón **Exportar filas a un archivo TXT** o **Exportar filas a un archivo CSV**, según el formato al que prefiera exportar.

El archivo que contiene la lista de vulnerabilidades de software detectadas en el dispositivo administrado seleccionado se descarga en el dispositivo que está utilizando en este momento.

Ignorar las vulnerabilidades de software

Puede ignorar las vulnerabilidades de software que se corregirán. Las razones para ignorar las vulnerabilidades de software pueden ser, por ejemplo, las siguientes:

- No considera que la vulnerabilidad de software sea crítica para su organización.
- Comprende que la reparación de la vulnerabilidad de software puede dañar los datos relacionados con el software que causaron la reparación de la vulnerabilidad.
- Está seguro de que la vulnerabilidad de software no es peligrosa para la red de su organización porque utiliza otras medidas para proteger sus dispositivos administrados.

Puede ignorar una vulnerabilidad de software en todos los dispositivos administrados o solo en determinados dispositivos administrados.

Para ignorar una vulnerabilidad de software en todos los dispositivos administrados:

1. En la pestaña **OPERACIONES**, en la lista desplegable **ADMINISTRACIÓN DE PARCHES**, seleccione **Vulnerabilidades de software**.

   La página muestra la lista de vulnerabilidades de software detectadas en los dispositivos administrados.

2. En la lista de vulnerabilidades de software, haga clic en el enlace con el nombre de la vulnerabilidad de software que desea ignorar.

   Se abre la ventana de propiedades de vulnerabilidades de software.

3. En la pestaña **Control de aplicaciones**, active la opción **Ignorar vulnerabilidad**.

4. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de vulnerabilidad de software.

La vulnerabilidad de software se ignora en todos los dispositivos administrados.

Para ignorar una vulnerabilidad de software en los dispositivos administrados seleccionados:

1. En la pestaña **DISPOSITIVOS**, seleccione la pestaña **DISPOSITIVOS ADMINISTRADOS**.

   Se muestra la lista de dispositivos administrados.

2. En la lista de dispositivos administrados, haga clic en el enlace con el nombre del dispositivo en el que desea ignorar una vulnerabilidad de software.

   Se abre la ventana de propiedades del dispositivo.

3. En la ventana de propiedades del dispositivo, seleccione la pestaña **Avanzado**.

4. En el panel izquierdo, seleccione la sección **Vulnerabilidades de software**.

Se muestra la lista de vulnerabilidades de software detectadas en el dispositivo.

5. En la lista de vulnerabilidades de software, seleccione la vulnerabilidad que desea ignorar en el dispositivo seleccionado.

   Se abre la ventana de propiedades de vulnerabilidades de software.

6. En la ventana de propiedades de vulnerabilidad de software, en la pestaña **Control de aplicaciones**, active la opción **Ignorar vulnerabilidad**.

7. Haga clic en el botón **Guardar**.

   Se cierra la ventana de propiedades de vulnerabilidad de software.

8. Cierre la ventana de propiedades del dispositivo.

La vulnerabilidad de software se ignora en el dispositivo seleccionado.

La vulnerabilidad de software ignorada no se reparará una vez que se hayan completado las tareas *Reparar vulnerabilidades* o *Instalar actualizaciones requeridas y reparar vulnerabilidades*. Puede excluir vulnerabilidades de software ignoradas de la lista de vulnerabilidades mediante el filtro.

Administrar la ejecución de aplicaciones en los dispositivos cliente

Esta sección describe las funciones de Kaspersky Security Center relacionadas con la administración de aplicaciones ejecutadas en dispositivos cliente.

Escenario: administración de aplicaciones

Puede administrar el inicio de aplicaciones en dispositivos de usuario. Puede permitir o bloquear aplicaciones para que se ejecuten en dispositivos administrados. Esta funcionalidad se ejecuta mediante el componente Control de aplicaciones. Solo puede administrar aplicaciones instaladas en dispositivos Windows.

Requisitos previos

- Kaspersky Security Center se ha implementado en su organización.
- Entre los dispositivos administrados en su organización hay dispositivos que ejecutan Windows.
- Se crea la directiva Kaspersky Endpoint Security para Windows y se activa.

Etapas

El escenario de uso de Control de aplicaciones procede en etapas:

1. **Formar y ver la lista de aplicaciones en dispositivos cliente**

Esta etapa le ayuda a encontrar las aplicaciones que están instaladas en los dispositivos administrados. Puede ver la lista de aplicaciones y decidir las aplicaciones que desea permitir y prohibir, de acuerdo con las directivas de seguridad de su organización. Las restricciones pueden estar relacionadas con las directivas de seguridad de la información en su organización. Puede omitir esta etapa si sabe exactamente las aplicaciones que están instaladas en los dispositivos administrados.

Instrucciones:

- Consola de administración: visualización del registro de aplicaciones
- Kaspersky Security Center 14 Web Console: obtención y visualización de una lista de aplicaciones instaladas en dispositivos cliente

2. **Formar y ver la lista de archivos ejecutables en dispositivos cliente**

   Esta etapa le ayuda a descubrir qué archivos ejecutables se encuentran en los dispositivos administrados. Examine la lista de los archivos ejecutables y compárela con las listas de archivos ejecutables permitidos y prohibidos. Las restricciones sobre el uso de archivos ejecutables pueden estar relacionadas con las directivas de seguridad de la información de su organización. Puede omitir esta etapa si sabe exactamente los archivos ejecutables están instalados en los dispositivos administrados.

   Instrucciones:

   - Consola de administración: inventario de archivos ejecutables
   - Kaspersky Security Center 14 Web Console: obtención y visualización de una lista de archivos ejecutables almacenados en dispositivos cliente

3. **Crear categorías de aplicaciones para las aplicaciones utilizadas en su organización**

   Analizar las listas de aplicaciones y archivos ejecutables almacenados en los dispositivos administrados. Basándose en el análisis, crear categorías de aplicaciones. Se recomienda crear una categoría de «Aplicaciones de trabajo» que cubra el conjunto estándar de aplicaciones que se utilizan en su organización. Si diferentes grupos de usuarios usan diferentes conjuntos de aplicaciones en su trabajo, se puede crear una categoría de aplicación separada para cada grupo de usuarios.

   Según el conjunto de criterios para crear una categoría de aplicación, puede crear categorías de aplicación de tres tipos.

   Instrucciones:

   - Consola de administración: Crear categorías de aplicaciones para las directivas de Kaspersky Endpoint Security para Windows, Crear una categoría de aplicaciones con contenido agregado manualmente, Crear una categoría de aplicaciones con contenido agregado automáticamente
   - Kaspersky Security Center 14 Web Console: Crear categoría de aplicación con contenido agregado manualmente, Crear una categoría de aplicación que incluya archivos ejecutables de dispositivos seleccionados, Crear una categoría de aplicación que incluya archivos ejecutables de la carpeta seleccionada

4. **Configuración del Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows**

   Configure el componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows utilizando las categorías de aplicaciones que creó en la etapa anterior.

   Instrucciones:

   - Consola de administración: configuración de administración de inicio de aplicaciones en los dispositivos cliente
   - Kaspersky Security Center 14 Web Console: Configuración de Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows

5. **Activación del componente de control de aplicaciones en modo de prueba**

A fin de garantizar que las reglas de Control de aplicaciones no bloqueen las aplicaciones necesarias para el trabajo, se recomienda habilitar la prueba de las reglas de Control de aplicaciones y analizar su funcionamiento después de crear nuevas reglas. Cuando la prueba está activada, Kaspersky Endpoint Security para Windows no bloqueará las aplicaciones cuyo inicio esté prohibido por las reglas de Control de aplicaciones, sino que enviará notificaciones sobre su inicio al Servidor de administración.

Al probar las reglas de Control de aplicaciones, se recomienda realizar las siguientes acciones:

- Determinar el periodo de prueba. El periodo de prueba puede variar de varios días a dos meses.
- Examinar los eventos resultantes de la prueba del funcionamiento del Control de aplicaciones.

Instrucciones para Kaspersky Security Center 14 Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y active la opción **Modo de prueba** en el proceso de configuración.

6. **Cambiar la configuración de categorías de aplicaciones del componente Control de aplicaciones**

   Si es necesario, realice cambios en la configuración de Control de aplicaciones. En función de los resultados de la prueba, puede agregar archivos ejecutables relacionados con eventos del componente Control de aplicaciones a una categoría de aplicación con contenido agregado manualmente.

   Instrucciones:

   - Consola de administración: Añadir archivos ejecutables relacionados con eventos a la categoría de la aplicación
   - Kaspersky Security Center 14 Web Console: Agregar archivos ejecutables relacionados con eventos a la categoría de aplicación

7. **Aplicar las reglas de Control de aplicaciones en modo operación**

   Después de probar las reglas de Control de aplicaciones y completar la configuración de las categorías de aplicaciones, puede aplicar las reglas de Control de aplicaciones en el modo de operación.

   Instrucciones para Kaspersky Security Center 14 Web Console: Configuración del componente Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows. Siga estas instrucciones y desactive la opción **Modo de prueba** en el proceso de configuración.

8. **Verificación de la configuración de Control de aplicaciones**

   Asegúrese de haber hecho lo siguiente:

   - Creado categorías de aplicaciones.
   - Configurado Control de aplicaciones mediante las categorías de aplicaciones.
   - Aplicado de las reglas de Control de aplicaciones en modo de operación.

Resultados

Cuando se completa el escenario, se controla el inicio de aplicaciones en dispositivos administrados. Los usuarios solo pueden iniciar las aplicaciones que estén permitidas en su organización y no aquellas que estén prohibidas.

Para obtener información detallada acerca de Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Acerca del Control de aplicaciones

El componente Control de aplicaciones supervisa los intentos de los usuarios de iniciar aplicaciones y regula el inicio de las aplicaciones mediante el uso de reglas.

El componente Control de aplicaciones está disponible para Kaspersky Endpoint Security para Windows y para Kaspersky Security for Virtualization Light Agent. Todas las instrucciones de esta sección describen la configuración del Control de aplicaciones para Kaspersky Endpoint Security para Windows.

El inicio de las aplicaciones cuya configuración no coincide con ninguna de las reglas de Control de aplicaciones está regulado por el modo operativo seleccionado del componente:

- *Lista de rechazados*. Este modo se utiliza si desea permitir el inicio de todas las aplicaciones, excepto las aplicaciones especificadas en las reglas de bloqueo. Este modo está seleccionado de forma predeterminada.
- *Lista de admitidos*. El modo se utiliza si desea bloquear el inicio de todas las aplicaciones, excepto las aplicaciones especificadas en las reglas de permiso.

Las Reglas de control de aplicaciones se implementan las mediante categorías de aplicaciones. Crea categorías de aplicaciones que definen criterios específicos. En Kaspersky Security Center hay tres tipos de categorías de aplicaciones:

- Categoría con contenido agregado manualmente. Defina condiciones, por ejemplo, metadatos de archivo, código hash de archivo, certificado de archivo, categoría KL y ruta de archivo, para incluir archivos ejecutables en la categoría.
- Categoría que incluye archivos ejecutables de los dispositivos seleccionados. Especifica un dispositivo cuyos archivos ejecutables se incluyen automáticamente en la categoría.
- Categoría que incluye archivos ejecutables de la carpeta seleccionada. Especifica una carpeta cuyos archivos ejecutables se incluyen automáticamente en la categoría.

Para obtener información detallada acerca de Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Obtener y ver una lista de aplicaciones instalada en dispositivos cliente

Kaspersky Security Center hace un inventario de todo el software instalado en los dispositivos cliente administrados que ejecutan Windows.

El Agente de red elabora una lista de las aplicaciones instaladas en un dispositivo cliente y luego transmite la lista al Servidor de administración. Agente de red recibe automáticamente información acerca de las aplicaciones instaladas desde el registro de Windows.

De manera predeterminada, para ahorrar recursos en el dispositivo cliente, el Agente de red comienza a recibir información acerca de las aplicaciones instaladas 10 minutos después de que se inicia el servicio del Agente de red.

Para visualizar la lista de aplicaciones instaladas en los dispositivos administrados:

En la lista desplegable **OPERACIONES → APLICACIONES DE TERCEROS**, seleccione **Registro de aplicaciones**.

La página muestra la lista de aplicaciones instaladas en los dispositivos administrados.

Para obtener información detallada acerca de Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Obtener y ver una lista de archivos ejecutables almacenados en dispositivos cliente

Puede obtener una lista de archivos ejecutables almacenados en dispositivos administrados. Para inventariar archivos ejecutables, debe crear una tarea de inventario.

La característica de inventariar archivos ejecutables está disponible para Kaspersky Endpoint Security 10 para Windows y versiones posteriores, y para Kaspersky Security for Virtualization 4.0 Light Agent y versiones posteriores.

Para crear una tarea de inventario de archivos ejecutables en dispositivos cliente:

1. En el menú principal, vaya a **DISPOSITIVOS → TAREAS**.

   Se muestra la lista de tareas.

2. Haga clic en el botón **Añadir**.

   Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.

3. En la página **Nueva tarea**, en la lista desplegable **Aplicación**, seleccione Kaspersky Endpoint Security para Windows.

4. En la lista desplegable **Tipo de tarea**, seleccione **Inventario**.

5. En la página **Finalizar la creación de tareas**, haga clic en el botón **Finalizar**.

   Una vez que se completa el Asistente para añadir tareas, se crea y configura la tarea **Inventario**. Si lo desea, puede cambiar la configuración de la tarea creada. La nueva tarea creada se muestra en la lista de tareas.

Para obtener una descripción detallada de la tarea de inventario, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Después de realizar la tarea de **Inventario**, se forma la lista de archivos ejecutables almacenados en los dispositivos administrados y puede consultarla.

Durante el inventario, se detectan archivos ejecutables de los siguientes formatos: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR y HTML.

haga lo siguiente para ver una lista de los archivos ejecutables almacenados en dispositivos cliente:

En la lista desplegable **OPERACIONES → APLICACIONES DE TERCEROS**, seleccione **ARCHIVOS EJECUTABLES**.

La página muestra la lista de los archivos ejecutables almacenados en dispositivos cliente.

Para enviar el archivo ejecutable del dispositivo administrado a Kaspersky:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → ARCHIVOS EJECUTABLES**.
2. Haga clic en el enlace del archivo ejecutable que desea enviar a Kaspersky.
3. En la ventana que se abre, vaya a la sección **Dispositivos** y seleccione la casilla del dispositivo administrado desde el que desea enviar el archivo ejecutable.

   Antes de enviar el archivo ejecutable, elija la casilla **No desconectar del Servidor de administración** para asegurarse de que el dispositivo administrado tenga una conexión directa con el Servidor de administración.

4. Haga clic en el botón **Enviar a Kaspersky**.

El archivo ejecutable seleccionado se descarga para su posterior envío a Kaspersky.

Crear categoría de aplicación con contenido agregado manualmente

Puede especificar un conjunto de criterios como una plantilla de archivos ejecutables cuyo inicio desea permitir o bloquear en su organización. Según los archivos ejecutables correspondientes a los criterios, puede crear una categoría de aplicaciones y usarla en la configuración del componente Control de aplicaciones.

Para crear una categoría de aplicaciones con contenido agregado manualmente, haga lo siguiente:

1. En la lista desplegable **OPERACIONES → APLICACIONES DE TERCEROS**, seleccione **CATEGORÍAS DE APLICACIONES**.

   Se muestra la página con una lista de categorías de aplicaciones.

2. Haga clic en el botón **Añadir**.

   Se inicia el Asistente para crear nueva categoría. Avance a través del Asistente utilizando el botón **Siguiente**.

3. En la página del Asistente **Seleccione el método de creación de la categoría**, seleccione la opción **Categoría con contenido añadido manualmente. Los datos de los archivos ejecutables se agregan manualmente a la categoría**.

4. En la página **Condiciones** del Asistente, haga clic en el botón **Añadir** a fin de añadir un criterio de condición para incluir archivos en la categoría que se crea.

5. En la página **Criterios de condición**, seleccione un tipo de regla para la creación de categoría de la lista:

   - **De categoría KL**

     Si se selecciona esta opción, puede especificar una categoría de aplicación de Kaspersky como condición para agregar aplicaciones a la categoría personalizada. Las aplicaciones de la categoría Kaspersky especificada se agregarán a la categoría de aplicación personalizada.

   - **Seleccionar el certificado del repositorio**

Si esta opción está seleccionada, puede especificar los certificados del almacenamiento. Los archivos ejecutables que se han firmado de acuerdo con los certificados especificados se agregarán a la categoría de usuario.

- Especificar la ruta a la aplicación (se admiten máscaras)

  Si se selecciona esta opción, se puede especificar la ruta a la carpeta del dispositivo cliente que contiene los archivos ejecutables que se agregarán a la categoría de aplicación personalizada.

- Unidad extraíble

  Si se selecciona esta opción, se puede especificar el tipo de medio (cualquier unidad o disco extraíble) en el que se ejecutará la aplicación. Las aplicaciones que se hayan ejecutado en el tipo selecciona de unidad de disco se agregarán a la categoría de aplicación personalizada.

- **Hash, metadatos o certificado**:

  - Seleccionar de la lista de archivos ejecutables

    Si esta opción está seleccionada, puede usar la lista de archivos ejecutables en el dispositivo cliente para seleccionar aplicaciones y agregarlas a la categoría.

  - Seleccionar del registro de aplicaciones

    Si se selecciona esta opción, se muestra el registro de la aplicación. Puede seleccionar una aplicación del registro y especificar los siguientes metadatos de archivo:

    - Nombre del archivo.
    - Versión del archivo. Puede especificar el valor preciso de la versión o describir una condición, por ejemplo, «mayor que 5.0».
    - Nombre de la aplicación.
    - Versión de la aplicación. Puede especificar el valor preciso de la versión o describir una condición, por ejemplo, «mayor que 5.0».
    - Proveedor.

  - Especificar manualmente

Si se selecciona esta opción, debe especificar archivo hash, metadatos o certificado como condición para agregar aplicaciones a la categoría de usuario.

Archivo hash

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores de hash calculados se almacena en la base de datos del Servidor de administración. El almacenamiento de valores de hash no aumenta significativamente el tamaño de la base de datos.

SHA-256 es una función hash criptográfica: no se ha encontrado ninguna vulnerabilidad en su algoritmo, y por lo que se la considera como la función criptográfica más fiable hoy en día. Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores admiten el cálculo de SHA-256. El cálculo de la función hash MD5 es compatible con todas las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center para archivos en la categoría:

- Si todas los instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, seleccione la casilla **Calcular SHA-256 para archivos en esta categoría (admitido por Kaspersky Endpoint Security 10 Service Pack 2 for Windows o posterior)**. No es aconsejable agregar categorías creadas según el criterio de hash SHA-256 de un archivo ejecutable para versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows. Esto puede causar fallos en el funcionamiento de la aplicación de seguridad. En ese caso, puede usar la función hash criptográfica MD5 para archivos de la categoría.

- Si alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows está instalada en su red, seleccione **Calcular MD5 para archivos de esta categoría (admitido por Kaspersky Endpoint Security, versiones anteriores a 10 Service Pack 2 para Windows)**. No puede agregar una categoría cuyo criterio de creación sea la suma de comprobación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. En ese caso, puede usar la función hash criptográfica SHA-256 para archivos de la categoría.

- Si distintos dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, seleccione la casilla **Calcular SHA-256 para archivos en esta categoría** y la casilla **Calcular MD5 para archivos en esta categoría**.

Metadatos

Si se selecciona esta opción, puede especificar metadatos de archivo como nombre de archivo, versión de archivo y proveedor. Los metadatos se enviarán al Servidor de administración. Los archivos ejecutables que contienen los mismos metadatos se agregarán a la categoría de la aplicación.

Certificado

Si esta opción está seleccionada, puede especificar los certificados del almacenamiento. Los archivos ejecutables que se han firmado de acuerdo con los certificados especificados se agregarán a la categoría de usuario.

- Desde archivo o desde paquete MSI/carpeta archivada

Si se selecciona esta opción, puede especificar un archivo de instalación MSI como condición para agregar aplicaciones a la categoría personalizada. Los metadatos del instalador de la aplicación se enviarán al Servidor de administración. Las aplicaciones cuyos metadatos de instalador sean los mismos que los del programa de instalación MSI especificado se agregarán a la categoría de aplicaciones personalizada.

El criterio seleccionado se agrega a la lista de condiciones.

Puede agregar tantos criterios para la categoría de aplicación de creación como necesite.

6. En la página **Exclusiones** del Asistente, haga clic en el botón **Añadir** a fin de añadir un criterio de condición exclusiva para excluir archivos en la categoría que se crea.

7. En la página **Criterios de condición**, seleccione un tipo de regla de la lista del mismo modo que seleccionó un tipo de regla para la creación de la categoría.

Cuando finaliza el Asistente, se crea la categoría de aplicaciones. Se muestra en la lista de categorías de aplicaciones. Puede usar la categoría de aplicaciones creada cuando configura el Control de aplicaciones.

Para obtener información detallada acerca de Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Crear una categoría de aplicación que incluya archivos ejecutables de dispositivos seleccionados

Puede usar archivos ejecutables de dispositivos seleccionados como una plantilla de archivos ejecutables que desee permitir o bloquear. Según los archivos ejecutables de los dispositivos seleccionados, puede crear una categoría de aplicación y usarla en la configuración del componente Control de aplicaciones.

Para crear una categoría de aplicación que incluya archivos ejecutables de dispositivos seleccionados:

1. En la lista desplegable **OPERACIONES → APLICACIONES DE TERCEROS**, seleccione **CATEGORÍAS DE APLICACIONES**.

   Se muestra la página con una lista de categorías de aplicaciones.

2. Haga clic en el botón **Añadir**.

   Se inicia el Asistente para crear nueva categoría. Avance por el Asistente utilizando el botón Siguiente.

3. En la página del Asistente **Seleccione el método de creación de la categoría**, especifique el nombre de la categoría y seleccione la opción **Categoría que incluye archivos ejecutables de dispositivos seleccionados. Estos archivos ejecutables se procesan automáticamente y sus métricas se agregan a la categoría**.

4. Haga clic en **Añadir**.

5. En la ventana que se abre, seleccione un dispositivo o los dispositivos cuyos archivos ejecutables se utilizarán para crear la categoría de aplicaciones.

6. Especifique los siguientes parámetros:

   - Algoritmo de cálculo del valor de hash

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores de hash calculados se almacena en la base de datos del Servidor de administración. El almacenamiento de valores de hash no aumenta significativamente el tamaño de la base de datos.

SHA-256 es una función hash criptográfica: no se ha encontrado ninguna vulnerabilidad en su algoritmo, y por lo que se la considera como la función criptográfica más fiable hoy en día. Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores admiten el cálculo de SHA-256. El cálculo de la función hash MD5 es compatible con todas las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center para archivos en la categoría:

- Si todas los instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, seleccione la casilla **Calcular SHA-256 para archivos en esta categoría (admitido por Kaspersky Endpoint Security 10 Service Pack 2 for Windows o posterior)**. No es aconsejable agregar categorías creadas según el criterio de hash SHA-256 de un archivo ejecutable para versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows. Esto puede causar fallos en el funcionamiento de la aplicación de seguridad. En ese caso, puede usar la función hash criptográfica MD5 para archivos de la categoría.

- Si alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows está instalada en su red, seleccione **Calcular MD5 para archivos de esta categoría (admitido por Kaspersky Endpoint Security, versiones anteriores a 10 Service Pack 2 para Windows)**. No puede agregar una categoría cuyo criterio de creación sea la suma de comprobación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. En ese caso, puede usar la función hash criptográfica SHA-256 para archivos de la categoría.

Si distintos dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, seleccione la casilla **Calcular SHA-256 para archivos en esta categoría** y la casilla **Calcular MD5 para archivos en esta categoría**.

La casilla **Calcular SHA-256 para archivos en esta categoría (admitido por Kaspersky Endpoint Security 10 Service Pack 2 para Windows o posterior)** está seleccionada de forma predeterminada.

La casilla **Calcular MD5 para archivos de esta categoría (admitido por versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** no aparecerá marcada de forma predeterminada.

- Sincronizar datos con el repositorio del Servidor de administración

Seleccione esta opción si desea que el Servidor de administración verifique periódicamente los cambios en la carpeta o las carpetas especificadas.

Esta opción está desactivada de forma predeterminada.

Si activa esta opción, especifique el periodo (en horas) para verificar los cambios en la carpeta (o las carpetas) especificada. De forma predeterminada, el intervalo de análisis es 24 horas.

- Tipo de archivo

En esta sección, puede especificar el tipo de archivo que se utiliza para crear la categoría de aplicaciones.

Todos los archivos. Se tienen en cuenta todos los archivos para crear la categoría. Esta opción está seleccionada de forma predeterminada.

Solo archivos fuera de las categorías de aplicaciones. Solo los archivos que se encuentran fuera de las categorías de aplicaciones se tienen en cuenta al crear la categoría.

- Carpetas

  En esta sección, puede especificar las carpetas del dispositivo o los dispositivos seleccionados que contienen archivos que se utilizan para crear la categoría de aplicaciones.

  Todas las carpetas. Todas las carpetas tienen en cuenta la categoría de creación. Esta opción está seleccionada de forma predeterminada.

  Carpeta especificada. Solo las carpetas especificadas tienen en cuenta la categoría de creación. Si selecciona esta opción, debe especificar la ruta a la carpeta.

Cuando finaliza el Asistente, se crea la categoría de aplicaciones. Se muestra en la lista de categorías de aplicaciones. Puede usar la categoría de aplicaciones creada cuando configura el Control de aplicaciones.

Crear una categoría de aplicación que incluya archivos ejecutables de la carpeta seleccionada

Puede utilizar archivos ejecutables de una carpeta seleccionada como un estándar de archivos ejecutables que desee permitir o bloquear en su organización. Según los archivos ejecutables de la carpeta seleccionada, puede crear una categoría de aplicaciones y utilizarla en la configuración del componente Control de aplicaciones.

Para crear una categoría de aplicaciones que incluya archivos ejecutables de la carpeta seleccionada, haga lo siguiente:

1. En la lista desplegable **OPERACIONES → APLICACIONES DE TERCEROS**, seleccione **CATEGORÍAS DE APLICACIONES**.

   Se muestra la página con una lista de categorías de aplicaciones.

2. Haga clic en el botón **Añadir**.

   Se inicia el Asistente para crear nueva categoría. Avance por el Asistente utilizando el botón Siguiente.

3. En la página del Asistente **Seleccione el método de creación de la categoría**, especifique el nombre de la categoría y seleccione la opción **Categoría que incluye archivos ejecutables de una carpeta específica. Los archivos ejecutables de las aplicaciones copiadas a la carpeta especificada se procesan automáticamente y sus métricas se agregan a la categoría**.

4. Especifique la carpeta cuyos archivos ejecutables se utilizarán para crear la categoría de la aplicación.

5. Defina los siguientes parámetros:

   - Incluir bibliotecas de vínculo dinámico (DLL) en esta categoría

La categoría de aplicaciones incluye bibliotecas de vínculo dinámico (archivos en el formato de DLL) y el componente Control de aplicaciones registra las acciones de esas bibliotecas que se ejecutan en el sistema. Si se incluyen archivos de DLL en la categoría, el rendimiento de Kaspersky Security Center puede verse afectado.

De forma predeterminada, esta casilla está en blanco.

- Incluir datos de script en esta categoría

  La categoría de aplicaciones incluye datos de scripts y la Protección frente a amenazas web no bloquea los scripts. Si se incluyen datos de script en la categoría, el rendimiento de Kaspersky Security Center puede verse afectado.

  De forma predeterminada, esta casilla está en blanco.

- Algoritmo de cálculo del valor de hash: **Calcular SHA-256 para archivos de esta categoría (compatible con Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores) / Calcular MD5 para archivos de esta categoría (compatible con versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)**

Según la versión de la aplicación de seguridad instalada en los dispositivos en su red, debe seleccionar un algoritmo para que Kaspersky Security Center calcule el valor de hash para archivos en esta categoría. La información sobre los valores de hash calculados se almacena en la base de datos del Servidor de administración. El almacenamiento de valores de hash no aumenta significativamente el tamaño de la base de datos.

SHA-256 es una función hash criptográfica: no se ha encontrado ninguna vulnerabilidad en su algoritmo, y por lo que se la considera como la función criptográfica más fiable hoy en día. Kaspersky Endpoint Security 10 Service Pack 2 para Windows y versiones posteriores admiten el cálculo de SHA-256. El cálculo de la función hash MD5 es compatible con todas las versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows.

Seleccione cualquiera de las opciones de cálculo del valor de hash de Kaspersky Security Center para archivos en la categoría:

- Si todas los instancias de aplicaciones de seguridad instaladas en su red son Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores, seleccione la casilla **Calcular SHA-256 para archivos en esta categoría (admitido por Kaspersky Endpoint Security 10 Service Pack 2 for Windows o posterior)**. No es aconsejable agregar categorías creadas según el criterio de hash SHA-256 de un archivo ejecutable para versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows. Esto puede causar fallos en el funcionamiento de la aplicación de seguridad. En ese caso, puede usar la función hash criptográfica MD5 para archivos de la categoría.

- Si alguna versión anterior a Kaspersky Endpoint Security 10 Service Pack 2 para Windows está instalada en su red, seleccione **Calcular MD5 para archivos de esta categoría (admitido por Kaspersky Endpoint Security, versiones anteriores a 10 Service Pack 2 para Windows)**. No puede agregar una categoría cuyo criterio de creación sea la suma de comprobación MD5 de un archivo ejecutable para Kaspersky Endpoint Security 10 Service Pack 2 para Windows o versiones posteriores. En ese caso, puede usar la función hash criptográfica SHA-256 para archivos de la categoría.

Si distintos dispositivos en su red usan versiones anteriores y posteriores de Kaspersky Endpoint Security 10, seleccione la casilla **Calcular SHA-256 para archivos en esta categoría** y la casilla **Calcular MD5 para archivos en esta categoría**.

La casilla **Calcular SHA-256 para archivos en esta categoría (admitido por Kaspersky Endpoint Security 10 Service Pack 2 para Windows o posterior)** está seleccionada de forma predeterminada.

La casilla **Calcular MD5 para archivos de esta categoría (admitido por versiones anteriores a Kaspersky Endpoint Security 10 Service Pack 2 para Windows)** no aparecerá marcada de forma predeterminada.

- Forzar el análisis de la carpeta en busca de cambios

Si esta opción está activada, la aplicación verifica periódicamente la carpeta de adición de contenido de categoría para ver si hay cambios. Puede especificar la frecuencia de comprobaciones (en horas) en el campo de entrada al lado de la casilla de verificación. De forma predeterminada, el intervalo de tiempo entre las comprobaciones forzadas es de 24 horas.

Si esta opción está desactivada, la aplicación no fuerza ninguna de las verificaciones de la carpeta. El servidor intenta acceder a los archivos si se han modificado, agregado o eliminado.

Esta opción está desactivada de forma predeterminada.

Cuando finaliza el Asistente, se crea la categoría de aplicaciones. Se muestra en la lista de categorías de aplicaciones. Puede usar la categoría de aplicación en la configuración de Control de aplicaciones.

Para obtener información detallada acerca de Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Ver la lista de categorías de aplicaciones

Puede ver la lista de categorías de aplicaciones configuradas y la configuración de cada categoría de aplicaciones.

Para ver la lista de categorías de aplicaciones,

En la pestaña **OPERACIONES**, en la lista desplegable **APLICACIONES DE TERCEROS**, seleccione **CATEGORÍAS DE APLICACIONES**.

Se muestra la página con una lista de categorías de aplicaciones.

Para ver las propiedades de una categoría de aplicaciones,

Haga clic en el nombre de la categoría de aplicaciones.

Se muestra la ventana de propiedades de la categoría de aplicaciones. Las propiedades se agrupan en varias pestañas.

Configuración del Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows

Después de crear las categorías del Control de aplicaciones, puede utilizarlas para configurar el Control de aplicaciones en las directivas de Kaspersky Endpoint Security para Windows.

Para configurar el Control de aplicaciones en la directiva de Kaspersky Endpoint Security para Windows:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.

   Se muestra la página con una lista de directivas.

2. Haga clic en la directiva **Kaspersky Endpoint Security para Windows**.

   Se abre la ventana de configuración de directivas.

3. Seleccione la pestaña **Configuración de la aplicación**, sección **Controles de seguridad**, subsección **Control de aplicaciones**.

   Se muestra la ventana **Control de aplicaciones** con la configuración de Control de aplicaciones.

4. Cambie el botón de alternancia para habilitar la opción **Control de aplicaciones**.

5. Si desea probar las reglas de Control de aplicaciones, cambie el botón de alternancia para habilitar la opción **Modo de prueba**.

   Si desea aplicar las reglas de Control de aplicaciones, cambie el botón de alternancia para desactivar la opción **Modo de prueba**.

6. Habilite la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows monitoree la carga de módulos DLL cuando los usuarios inician las aplicaciones.

   La información sobre el módulo y la aplicación que lo cargó se guardará en un informe.

Kaspersky Endpoint Security para Windows supervisa solo los módulos DLL y los controladores cargados después de seleccionarse la opción **Controlar la carga de módulos DLL**. Reinicie el equipo después de seleccionar la opción **Controlar la carga de módulos DLL** si desea que Kaspersky Endpoint Security para Windows supervise todos los módulos y controladores DLL, incluidos los cargados antes de que se inicie Kaspersky Endpoint Security para Windows.

7. (Opcional) En el bloque **Plantillas de mensajes**, cambie la plantilla del mensaje que se muestra cuando se bloquea el inicio de una aplicación y el mensaje de correo electrónico de la plantilla que se le envía.

8. En la configuración del bloque **Modo de control de aplicaciones**, seleccione el modo **Lista de rechazados** o **Lista de admitidos**.

   De forma predeterminada, el modo **Lista de rechazados** está seleccionado.

9. Haga clic en el enlace **Configuración de listas de reglas**.

   La ventana **Listas de admitidos y listas de rechazados** se abre para permitirle añadir una categoría de aplicación. De manera predeterminada, la pestaña **Lista de rechazados** se selecciona si se selecciona el modo **Lista de rechazados** o la pestaña **Lista de admitidos** si se selecciona el modo **Lista de permitidos**.

10. En la ventana **Listas de permitidos y lista de rechazados**, haga clic en el botón **Añadir**.

    Se abre la ventana **Regla de control de aplicaciones**.

11. Haga clic en el enlace **Por favor elija una categoría**.

    Se abre la ventana **Categoría de aplicación**.

12. Agregue la categoría o las categorías de aplicaciones que ya había creado.

    Puede editar la configuración de una categoría creada haciendo clic en el botón **Editar**.

    Puede crear una nueva categoría haciendo clic en el botón **Agregar**.

    Puede eliminar una categoría de la lista haciendo clic en el botón **Eliminar**.

13. Después de completar la lista de categorías de aplicaciones, haga clic en el botón **Aceptar**.

    Se cierra la ventana **Categoría de aplicaciones**.

14. En la ventana de la regla **Control de aplicaciones**, en el bloque **Temas y sus derechos**, cree la lista de usuarios y grupos de usuarios para aplicar la regla de Control de aplicaciones.

15. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana de la **regla de Control de aplicaciones**.

16. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana de **Lista de rechazados y Lista de permitidos**.

17. Haga clic en el botón **Aceptar** para guardar la configuración y cerrar la ventana **Control de aplicaciones**.

18. Haga clic en el botón **Cerrar** (⨯) para cerrar la ventana con la configuración de directiva de Kaspersky Endpoint Security para Windows.

Control de aplicaciones está configurado. Una vez que la directiva se propaga a los dispositivos cliente, se administra el inicio de los archivos ejecutables.

Para obtener información detallada acerca de Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Añadir archivos ejecutables relacionados con eventos a la categoría de aplicaciones

Después de configurar Control de aplicaciones en las directivas de Kaspersky Endpoint Security para Windows, en la lista de eventos se mostrarán los eventos siguientes:

- **Inicio de aplicación prohibido** (evento *crítico*). Este evento se muestra si ha configurado el Control de aplicaciones para aplicar reglas.
- **Inicio de la aplicación prohibido en el modo de prueba** (evento de *información*). Este evento se muestra si ha configurado el Control de aplicaciones para probar reglas.
- **Mensaje de bloqueo de inicio de aplicación al administrador** (evento de *advertencia*). Este evento se muestra si ha configurado el Control de aplicaciones para aplicar reglas y un usuario ha solicitado acceso a la aplicación cuyo inicio se ha bloqueado.

Se recomienda crear selecciones de eventos para ver eventos relacionados con la operación de Control de aplicaciones.

Puede agregar archivos ejecutables relacionados con los eventos de Control de aplicaciones a una categoría de aplicaciones existente o a una nueva categoría de aplicaciones. Puede agregar archivos ejecutables solo a una categoría de aplicaciones con contenido agregado manualmente.

Para agregar archivos ejecutables relacionados con eventos de Control de aplicaciones a una categoría de aplicaciones:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → SELECCIONES DE EVENTOS**.

   Se muestra la lista de selecciones de eventos.

2. Seleccione la selección de eventos para ver eventos relacionados con el Control de aplicaciones e inicie esta selección de eventos.

   Si no ha creado una selección de eventos relacionada con el Control de aplicaciones, puede seleccionar e iniciar una selección predefinida, por ejemplo, **Eventos recientes**.

   Se muestra la lista de eventos.

3. Seleccione los eventos cuyos archivos ejecutables asociados desea agregar a la categoría de aplicaciones y haga clic en el botón **Asignar a categoría**.

   Se inicia el Asistente para crear nueva categoría. Avance por el Asistente utilizando el botón **Siguiente**.

4. En la página del Asistente, especifique la configuración relevante:

   - En la sección **Acción en el archivo ejecutable relacionado con el evento**, seleccione una de las siguientes opciones:

     - **Añadir a una nueva categoría de aplicaciones**

       Seleccione esta opción si desea crear una nueva categoría de aplicación basada en archivos ejecutables relacionados con eventos.

       Esta opción está seleccionada de forma predeterminada.

       Si ha seleccionado esta opción, especifique un nuevo nombre de categoría.

- Añadir a una categoría de aplicaciones existente

  Seleccione esta opción si quiere agregar eventos relacionados con archivos ejecutables a una categoría de aplicaciones existente.

  Esta opción no está seleccionada de forma predeterminada.

  Si ha seleccionado esta opción, seleccione la categoría de aplicación con contenido agregado manualmente al que desea agregar archivos ejecutables.

- En la sección **Tipo de regla**, seleccione una de las siguientes opciones:
  - **Reglas para añadir inclusiones**
  - **Reglas para añadir exclusiones**
- En la sección **Parámetro utilizado como condición**, seleccione una de las siguientes opciones:
  - Detalles del certificado (o hashes SHA-256 para archivos sin certificado)

    Los archivos pueden estar firmados con un certificado. Se pueden firmar varios archivos con el mismo certificado. Por ejemplo, se pueden firmar diferentes versiones de la misma aplicación con el mismo certificado o se pueden firmar varias aplicaciones diferentes del mismo proveedor con el mismo certificado. Cuando selecciona un certificado, varias versiones de una aplicación o varias aplicaciones del mismo proveedor pueden terminar en la categoría.

    Cada archivo tiene su propia función hash SHA-256 exclusiva. Cuando selecciona una función hash SHA-256, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

    Seleccione esta opción si quiere agregar a las reglas de la categoría los detalles del certificado de un archivo ejecutable (o la función hash SHA-256 para archivos sin certificado).

    Esta opción está seleccionada de forma predeterminada.

  - Detalles del certificado (se omitirán los archivos sin certificado)

    Los archivos pueden estar firmados con un certificado. Se pueden firmar varios archivos con el mismo certificado. Por ejemplo, se pueden firmar diferentes versiones de la misma aplicación con el mismo certificado o se pueden firmar varias aplicaciones diferentes del mismo proveedor con el mismo certificado. Cuando selecciona un certificado, varias versiones de una aplicación o varias aplicaciones del mismo proveedor pueden terminar en la categoría.

    Seleccione esta opción si quiere agregar los detalles del certificado de un archivo ejecutable a las reglas de la categoría. Si el archivo ejecutable no tiene certificados, este archivo se omitirá. No se agregará ninguna información sobre este archivo a la categoría.

  - Solo SHA-256 (se omitirán los archivos sin hash)

    Cada archivo tiene su propia función hash SHA-256 exclusiva. Cuando selecciona una función hash SHA-256, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

    Seleccione esta opción si solo quiere agregar los detalles de la función hash SHA-256 del archivo ejecutable.

  - Solo MD5 (modo discontinuado, solo para Kaspersky Endpoint Security 10 Service Pack 1)

Cada archivo tiene su propia función hash MD5 exclusiva. Cuando selecciona una función hash MD5, solo el archivo correspondiente, por ejemplo, la versión de la aplicación que se ha definido, termina en la categoría.

Seleccione esta opción si solo quiere agregar los detalles de la función hash MD5 del archivo ejecutable. El cálculo de la función hash MD5 es compatible con Kaspersky Endpoint Security 10 Service Pack 1 for Windows y las versiones anteriores.

5. Haga clic en **Aceptar**.

Cuando finalice el Asistente, los archivos ejecutables relacionados con los eventos de Control de aplicaciones se añaden a la categoría de aplicaciones existente o a una nueva categoría de aplicaciones. Puede ver la configuración de la categoría de aplicaciones que ha modificado o creado.

Para obtener información detallada acerca de Control de aplicaciones, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows y Kaspersky Security for Virtualization Light Agent.

Crear un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

Kaspersky Security Center Web Console le permite realizar la instalación remota de aplicaciones de terceros mediante el uso de paquetes de instalación. Estas aplicaciones de terceros se incluyen en una base de datos dedicada de Kaspersky. La base de datos se crea automáticamente cuando ejecuta por primera vez la tarea*Descargar actualizaciones en el repositorio del Servidor de administración*.

Para crear un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky:

1. En el programa Kaspersky Security Center Web Console, abra **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**.
2. Haga clic en el botón **Añadir**.
3. En la página Asistente de nuevo paquete que se abre, seleccione la opción **Seleccionar una aplicación de la base de datos de Kaspersky para crear un paquete de instalación** y luego haga clic en **Siguiente**.
4. En la lista de aplicaciones que se abre, seleccione la aplicación correspondiente y luego haga clic en **Siguiente**.
5. Seleccione el idioma de localización apropiado en la lista desplegable y luego haga clic en **Siguiente**.

Este paso solo se muestra si la aplicación ofrece varias opciones de idioma.

6. Si se le solicita que acepte un Contrato de licencia para la instalación, en la página **Contrato de licencia de usuario final** que se abre haga clic en el enlace para leer el Contrato de licencia en el sitio web del proveedor y luego seleccione la casilla de verificación **Confirmo que he leído, comprendo y acepto en su totalidad los términos y condiciones de este Contrato de licencia de usuario final**.
7. En la página **Nombre del nuevo paquete de instalación** que se abre, en el campo **Nombre del paquete**, introduzca el nombre del paquete de instalación y luego haga clic en **Siguiente**.

Espere hasta que el paquete de instalación recién creado se cargue en el Servidor de administración. Cuando el Asistente de nuevo paquete muestre el mensaje que le informa que el proceso de creación del paquete se creó con éxito, haga clic en **Finalizar**.

El paquete de instalación recién creado aparece en la lista de paquetes de instalación. Puede seleccionar este paquete al crear o reconfigurar la tarea *Instalar aplicación de forma remota*.

Ver y modificar la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

Si previamente creó algún paquete de instalación de aplicaciones de terceros que figura en la base de datos de Kaspersky, puede ver y modificar posteriormente la configuración de estos paquetes.

La modificación de la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky solo está disponible bajo la licencia de Administración de vulnerabilidades y parches.

Para ver y modificar la configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky:

1. En el programa Kaspersky Security Center Web Console, abra **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → PAQUETES DE INSTALACIÓN**.
2. En la lista de paquetes de instalación que se abre, haga clic en el nombre del paquete relevante.
3. En la página de propiedades que se abre, modifique la configuración, si es necesario.
4. Haga clic en el botón **Guardar**.

La configuración que modificó se guarda.

Configuración de un paquete de instalación de una aplicación de terceros desde la base de datos de Kaspersky

La configuración de un paquete de instalación de una aplicación de terceros se agrupa en las siguientes pestañas:

Solo una parte de la configuración que figura a continuación se muestra de forma predeterminada, por lo que puede añadir las columnas correspondientes haciendo clic en el botón **Filtro** y seleccionando los nombres de columna relevantes de la lista.

- Pestaña **Control de aplicaciones**:
  - Campo de entrada que contiene el nombre del paquete de instalación que se puede editar manualmente
  - **Aplicación**

    El nombre de la aplicación de terceros para la que se crea el paquete de instalación.

- **Versión**

  El número de versión de la aplicación de terceros para la que se crea el paquete de instalación.

- **Tamaño**

  El tamaño del paquete de instalación de terceros (en kilobytes).

- **Creado**

  La fecha y la hora en que se creó el paquete de instalación de terceros.

- **Ruta**

  La ruta a la carpeta de la red donde se guarda el paquete de instalación de terceros.

- Pestaña **Proceso de instalación**:

  - **Instalar los componentes generales del sistema necesarios**

    Si esta opción está activada, antes de instalar una actualización, la aplicación instala automáticamente todos los componentes generales del sistema (requisitos previos) que se requieren para instalar la actualización. Por ejemplo, estos requisitos previos pueden ser actualizaciones del sistema operativo.

    Si esta opción está desactivada, es posible que tenga que instalar los requisitos previos de manera manual.

    Esta opción está desactivada de forma predeterminada.

  - Tabla que muestra las propiedades de actualización y que contiene las siguientes columnas:

    - **Nombre**

      El nombre de la clave.

    - **Descripción**

      La descripción de la actualización.

    - **Origen**

      El origen de la actualización, es decir, si fue lanzada por Microsoft o por un otro desarrollador externo.

    - **Tipo**

      El tipo de actualización, es decir, si está destinada a un controlador o una aplicación.

    - **Categoría**

La categoría de servicios de actualización de Windows Server (WSUS) que se muestra para las actualizaciones de Microsoft (actualizaciones críticas, actualizaciones de definiciones, controladores, paquetes de características, actualizaciones de seguridad, paquetes de servicios, herramientas, paquetes acumulativos de actualizaciones, actualizaciones o paso a nueva versión).

- **Nivel de importancia según MSRC**

  El nivel de importancia de la actualización definido por Microsoft Security Response Center (MSRC).

- **Nivel de importancia**

  El nivel de importancia de la actualización definido por Kaspersky.

- **Nivel de importancia del parche (para parches destinados a aplicaciones de Kaspersky)**

  El nivel de importancia del parche, si está destinado a una aplicación de Kaspersky.

- **Artículo**

  El identificador (id.) del artículo de la Base de conocimientos que describe la actualización.

- **Boletín**

  El id. del boletín de seguridad que describe la actualización.

- **No asignada para instalación (nueva versión)**

  Muestra si la actualización tiene el estado No asignado para instalación.

- **Para instalar**

  Muestra si la actualización tiene el estado Para instalar.

- **Instalando**

  Muestra si la actualización tiene el estado Instalando.

- **Instalada**

  Muestra si la actualización tiene el estado Instalada.

- **Error**

  Muestra si la actualización tiene el estado Fallo.

- **Se requiere reiniciar**

  Muestra si la actualización tiene el estado Se requiere reiniciar.

- **Registrada**

  Muestra la fecha y hora en que se registró la actualización.

- **Se ha instalado en modo interactivo**

  Muestra si la actualización requiere interactuar con el usuario durante la instalación.

- **Anulado**

  Muestra la fecha y hora en que se revocó la actualización.

- **Estado de aprobación de la actualización**

  Muestra si la actualización está aprobada para su instalación.

- **Revisión**

  Muestra el número de revisión actual de la actualización.

- **Id. de actualización**

  Muestra el id. de la actualización

- **Versión de la aplicación**

  Muestra el número de versión a la que se actualizará la aplicación.

- **Sustituido**

  Muestra otras actualizaciones que pueden reemplazar a la actualización.

- **Sustituyendo**

  Muestra otras actualizaciones que pueden ser reemplazadas por la actualización.

- **Debe aceptar las condiciones del Contrato de licencia**

  Muestra si la actualización requiere la aceptación de los términos de un Contrato de licencia de usuario final (EULA).

- **Dirección de URL de la descripción**

  Muestra el nombre del proveedor de actualizaciones.

- **Familia de la aplicación**

  Muestra el nombre de la familia de aplicaciones a la que pertenece la actualización.

- Aplicación

  Muestra el nombre de la aplicación a la que pertenece la actualización.

- Idioma de localización

  Muestra el idioma de la localización de la actualización.

- No asignada para instalación (nueva versión)

  Muestra si la actualización tiene el estado No asignado para instalación (nueva versión).

- Requiere la instalación de requisitos previos

  Muestra si la actualización tiene el estado de instalación Requiere la instalación de requisitos previos.

- Modo de descarga

  Muestra el modo de descarga de la actualización.

- Es un parche

  Muestra si la actualización es un parche.

- No instalado

  Muestra si la actualización tiene el estado No instalada.

- La pestaña **Configuración** que muestra la configuración del paquete de instalación (con sus nombres, descripciones y valores) que se utilizan como parámetros de la línea de comandos durante la instalación. Si el paquete no proporciona dicha configuración, se muestra el mensaje correspondiente. Puede modificar los valores de esta configuración.

- La pestaña **Historial de revisión** que muestra las revisiones del paquete de instalación y que contiene las siguientes columnas:

  - Revisión

    Muestra el número de revisión de los paquetes de instalación.

  - Hora

    Muestra la hora en que se creó la revisión.

  - Usuario

    Muestra el nombre de la cuenta de usuario con la que se creó la revisión.

  - Acción

Enumera las acciones realizadas en el paquete de instalación dentro de la revisión.

- **Descripción**

  Muestra la descripción de texto añadida para la revisión.

Etiquetas de aplicaciones

Esta sección describe las etiquetas de aplicaciones y proporciona instrucciones para crearlas y modificarlas, así como para etiquetar aplicaciones de terceros.

Acerca de las etiquetas de aplicación

Kaspersky Security Center le permite etiquetar aplicaciones de terceros (aplicaciones hechas por vendedores de software diferente a Kaspersky). Una etiqueta es la etiqueta de una aplicación que puede ser utilizada para agrupar o encontrar aplicaciones. Una etiqueta asignada a las aplicaciones puede servir como una condición en las selecciones de dispositivos.

Por ejemplo, puede crear la etiqueta `[Navegadores]` y asignar a todos los navegadores, como Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Creación de una etiqueta de aplicación

Creación de una categoría de aplicación:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → ETIQUETAS DE LA APLICACIÓN**.
2. Haga clic en **Añadir**.

   Una nueva ventana de etiqueta se abre.
3. Introduzca el nombre de la etiqueta.
4. Haga clic en **Aceptar** para guardar los cambios.

La nueva etiqueta aparece en la lista de etiquetas de aplicación.

Renombramiento de una etiqueta de aplicación

Para renombrar una etiqueta de aplicación:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → ETIQUETAS DE LA APLICACIÓN**.

2. Seleccione la casilla de verificación junto a la etiqueta que quiere renombrar y haga clic en **Editar**.

   Se abre la ventana de propiedades de la etiqueta.

3. Cambie el nombre de la etiqueta.

4. Haga clic en **Aceptar** para guardar los cambios.

La etiqueta actualizada aparece en la lista de etiquetas de aplicaciones.

Asignación de etiquetas a una aplicación

Para asignar una o varias etiquetas a una aplicación:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → REGISTRO DE APLICACIONES**.

2. Haga clic en el nombre de la aplicación a la que desea asignar etiquetas.

3. Seleccione la pestaña **Etiquetas**.

   La pestaña muestra todas las etiquetas de aplicación que existen en el Servidor de administración. Para etiquetas asignadas a la aplicación seleccionada, la casilla de verificación en la columna **Etiqueta asignada** está seleccionada.

4. Para etiquetas que quiera asignar, seleccione las casillas de verificación en la columna **Etiqueta asignada**.

5. Haga clic en **Guardar** para guardar los cambios.

Las etiquetas están asignadas a la aplicación.

Eliminación de etiquetas asignadas desde una aplicación

Para eliminar una o varias etiquetas de una aplicación:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → REGISTRO DE APLICACIONES**.

2. Haga clic en el nombre de la aplicación de la que desea eliminar etiquetas.

3. Seleccione la pestaña **Etiquetas**.

   La pestaña muestra todas las etiquetas de aplicación que existen en el Servidor de administración. Para etiquetas asignadas a la aplicación seleccionada, la casilla de verificación en la columna **Etiqueta asignada** está seleccionada.

4. Para etiquetas que quiera eliminar, quite la selección de las casillas de verificación en la columna **Etiqueta asignada**.

5. Haga clic en **Guardar** para guardar los cambios.

Las etiquetas se retiran de la aplicación.

Las etiquetas de aplicación retiradas no se eliminan. Si lo desea, puede eliminarlas manualmente.

Eliminación de una etiqueta de aplicación

Para eliminar una etiqueta de aplicación:

1. En el menú principal, vaya a **OPERACIONES → APLICACIONES DE TERCEROS → ETIQUETAS DE LA APLICACIÓN**.
2. En la lista, seleccione la etiqueta de la aplicación que quiere eliminar.
3. Haga clic en el botón **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina la etiqueta de la aplicación. La etiqueta eliminada se elimina automáticamente de todas las aplicaciones a las que fue asignada.

Supervisión e informes

Esta sección describe las capacidades de supervisión e informes de Kaspersky Security Center. Estas capacidades le brindan una descripción general de su infraestructura, estados de protección y estadísticas.

Después del despliegue de Kaspersky Security Center o durante la operación, puede configurar las funciones de supervisión e informes para que se adapten mejor a sus necesidades.

Escenario: seguimiento e informes

Esta sección proporciona un escenario para configurar la función Supervisión e informes en Kaspersky Security Center.

Requisitos previos

Después de desplegar Kaspersky Security Center en la red de una organización, puede comenzar a supervisarlo y generar informes sobre su funcionamiento.

El seguimiento y la elaboración de informes en la red de una organización se realizan en etapas:

1. **Configuración del cambio de estado de los dispositivos**

   Obtenga información sobre la configuración de los estados del dispositivo según las condiciones específicas. Al cambiar estas configuraciones, puede cambiar la cantidad de eventos con niveles de importancia *Crítica* o *Advertencia*. Al configurar la conmutación de estados de dispositivo, asegúrese de lo siguiente:

- Las nuevas configuraciones no entran en conflicto con las directivas de seguridad de la información de su organización.
- Usted tiene la capacidad de reaccionar a eventos de seguridad importantes en la red de su organización de manera oportuna.

2. **Configuración de notificaciones sobre eventos en dispositivos cliente**

   Instrucciones:

   Configure la notificación (por correo electrónico, SMS o ejecutando un archivo ejecutable) de eventos en dispositivos cliente

3. **Cambio de respuesta de su red de seguridad ante el Brote de virus evento**

   Puede modificar los umbrales específicos en las propiedades del Servidor de administración. También puede crear una directiva más estricta que se activará o crear una tarea que se ejecutará cuando ocurra este evento.

4. **Realizar acciones recomendadas para notificaciones críticas y de advertencia**

   Instrucciones:

   Acciones recomendadas a realizar para la red de su organización

5. **Revisión del estado de seguridad de la red de su organización**

   Instrucciones:

   - Revisión del widget Estado de la protección
   - Generación y revisión del Informe del estado de la protección
   - Generación y revisión del Informe de errores

6. **Ubicación de dispositivos cliente que no están protegidos**

   Instrucciones:

   - Revisión del widget Nuevos dispositivos
   - Generación y revisión del Informe del despliegue de la protección

7. **Comprobación de protección de dispositivos cliente**

   Instrucciones:

   - Generación y revisión de los informes desde las categorías Estado de la protección y Estadísticas de amenazas
   - Inicio y revisión de la selección de eventos Crítico

8. **La evaluación y la limitación del evento se cargan en la base de datos**

   Se transfiere la información sobre eventos que ocurren durante el funcionamiento de aplicaciones administradas de un dispositivo cliente y se registra en la base de datos del Servidor de administración. Para reducir la carga en el Servidor de administración, evalúe y limite el número máximo de eventos que se pueden almacenar en la base de datos.

   Instrucciones:

   - Cálculo del espacio de la base de datos
   - Limitar el número máximo de eventos

9. **Consultar la información de la licencia**

   Instrucciones:

   - Adición del widget Uso de claves de licencia al panel y revisión
   - Generación y revisión del Informe de uso de claves de licencia

Resultados

Al completar el escenario, estará informado sobre la protección de la red de su organización y, por lo tanto, podrá planificar acciones para una mayor protección.

Acerca de los tipos de supervisión e informes

La información sobre eventos de seguridad en la red de una organización se almacena en la base de datos del Servidor de administración. En función de los eventos, Kaspersky Security Center 14 Web Console proporciona los siguientes tipos de monitoreo e informes en la red de su organización:

- Panel
- Informes
- Selecciones de eventos
- Notificaciones

Panel

El panel de control le permite supervisar las tendencias de seguridad en la red de su organización al proporcionarle una visualización gráfica de la información

Informes

La característica de los informes le permiten obtener información numérica detallada sobre la seguridad de la red de su organización, guardar esta información en un archivo, enviarla por correo electrónico e imprimirla.

Selecciones de eventos

Las selecciones de eventos proporcionan una vista en pantalla de los conjuntos de eventos con nombre que se seleccionan desde la base de datos del Servidor de administración. Estos conjuntos de eventos se agrupan según las siguientes categorías:

- Por nivel de importancia: **Eventos críticos**, **Fallos operativos**, **Advertencias** y **Eventos de información**
- Por tiempo: **Eventos recientes**
- Por tipo: **Solicitudes de los usuarios** y **Eventos de auditoría**

Puede crear y ver selecciones de eventos definidos por el usuario según la configuración disponible en la interfaz de Kaspersky Security Center 14 Web Console para configurarlas.

Notificaciones

Las notificaciones le alertan sobre eventos y le ayudan a acelerar sus respuestas a estos eventos al realizar acciones recomendadas o acciones que usted considera apropiadas.

Panel de control y widgets

Esta sección contiene información sobre el panel y los widgets que este proporciona. La sección incluye instrucciones sobre cómo administrar y configurar los widgets.

Uso del tablero

El panel de control le permite supervisar las tendencias de seguridad en la red de su organización al proporcionarle una visualización gráfica de la información

El panel está disponible en Kaspersky Security Center 14 Web Console, en la sección **SUPERVISIÓN E INFORMES**, al hacer clic en **PANEL**.

El panel proporciona widgets que se pueden personalizar. Puede elegir una gran cantidad de widgets diferentes, presentados como gráficos circulares o en forma de anillo, tablas, gráficos, gráficos de barras y listas. La información mostrada en los widgets se actualiza automáticamente; el periodo de actualización es de uno a dos minutos. El intervalo entre actualizaciones varía para widgets diferentes. Puede actualizar los datos en un widget manualmente en cualquier momento a través del menú de configuración.

De forma predeterminada, los widgets incluyen información sobre todos los eventos almacenados en la base de datos del Servidor de administración.

Kaspersky Security Center 14 Web Console tiene un conjunto predeterminado de widgets de las siguientes categorías:

- **Estado de la protección**
- **Despliegue**
- **Actualizar**
- **Estadísticas de amenazas**
- **Otro**

Algunos widgets tienen información de texto con enlaces. Puede consultar la información detallada haciendo clic en un enlace.

Al configurar el panel, puede añadir widgets que necesite, esconder widgets que no necesite, cambiar el tamaño o el aspecto de widgets, mover widgets y cambiar su configuración.

Añadir widgets al panel de control

Para añadir widgets al panel de control:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **PANEL**.
2. Haga clic en el botón **Añadir o restaurar un widget web**.
3. En la lista de widgets disponibles, seleccione los artefactos que desea añadir al panel.

   Los widgets están agrupados por la categoría. Para ver la lista de widgets incluidos en una categoría, haga clic en el icono de flecha (>) junto al nombre de la categoría.
4. Haga clic en el botón **Añadir**.

Los widgets seleccionados se añaden al final del panel de control.

Ahora puede editar la representación y los parámetros de los artefactos añadidos.

Ocultar un widget desde el panel de control

Ocultar un widget mostrado desde el panel de control:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **PANEL**.
2. Haga clic en el icono de la **Configuración** (⚙) al lado del widget que desea ocultar.
3. Seleccionar **Ocultar el widget web**.
4. En la ventana **Advertencia** que se abre, haga clic en **Aceptar**.

El widget seleccionado se oculta. Más tarde, puede añadir este widget al panel de control nuevamente.

Mover un widget en el tablero

Mover un widget en el panel de control:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **PANEL**.
2. Haga clic en el icono de la **Configuración** (⚙) al lado del widget que desea mover.
3. Seleccionar **Mover**.
4. Haga clic en la localización a la que quiera mover el widget. Solo puede seleccionar otro widget.

Se intercambian los lugares de los widgets seleccionados.

Cambio del tamaño o aspecto del widget

Para los widgets que muestran un gráfico, puede cambiar su representación: un gráfico de barras o un gráfico de líneas. Para algunos widgets, puede cambiar su tamaño: compacto, medio o máximo.

Para cambiar la representación del widget:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **PANEL**.
2. Haga clic en el icono de la **Configuración** (⚙) al lado del widget que desea editar.
3. Realice una de las siguientes acciones:
   - Para mostrar el widget como un gráfico de barras, seleccione el **Tipo de gráfico: barras**.
   - Para mostrar el widget como un gráfico de líneas, seleccione el **Tipo de gráfico: líneas**.
   - Para cambiar el área ocupada por el widget, seleccione uno de los valores:
     - **Compacto**
     - **Compacto (solo barra)**
     - **Medio (gráfico de anillos)**
     - **Medio (gráfico de barras)**
     - **Máximo**

Se cambia la representación del widget seleccionado.

Cambiar configuración del widget

Cambiar configuración de un widget:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **PANEL**.
2. Haga clic en el icono de la **Configuración** (⚙) al lado del widget que desea cambiar.
3. Seleccionar **Mostrar configuración**.
4. En la ventana de configuración del widget que se abre, cambie la configuración del widget según sea necesario.
5. Haga clic en **Guardar** para guardar los cambios.

Se modifican los ajustes del widget seleccionado.

El conjunto de ajustes depende del widget específico. A continuación, se presentan algunos de los ajustes comunes:

- **Cobertura del widget web** (conjunto de objetos de los que muestra la información el widget): por ejemplo, un grupo de administración o de selección de dispositivos.
- **Elija una tarea** (la tarea de la que muestra la información el widget).
- **Intervalo de tiempo** (el intervalo de tiempo durante el cual se muestra la información en el widget): entre las dos fechas especificadas; desde la fecha especificada hasta el día actual; o desde el día actual menos el número especificado de días hasta el día actual.
- **Asignar estado Crítico si se especifica lo siguiente** y **Asignar estado Advertencia si se especifica lo siguiente** (las reglas que determinan el color de las luces del semáforo).

Acerca del modo Solo panel

Puede configurar el modo Solo panel para los empleados que no administran la red pero que desean ver las estadísticas de protección de la red en Kaspersky Security Center (por ejemplo, un alto directivo). Cuando un usuario tiene este modo activado, solo se le muestra un panel con un conjunto predefinido de widgets. Así, puede monitorear las estadísticas especificadas en los widgets, por ejemplo, el estado de protección de todos los dispositivos administrados, la cantidad de amenazas recién detectadas o la lista de las amenazas más frecuentes en la red.

Cuando un usuario trabaja en el modo Solo panel, se aplican las siguientes restricciones:

- El menú principal no se muestra al usuario, para que no pueda cambiar la configuración de protección de la red.
- El usuario no puede realizar ninguna acción con los widgets, por ejemplo, añadirlos u ocultarlos. Por lo tanto, debe colocar y configurar todos los widgets necesarios para el usuario en el panel, por ejemplo, establecer la regla de conteo de objetos o especificar el intervalo de tiempo.

No puede asignarse a sí mismo el modo de Solo panel. Si desea trabajar en este modo, comuníquese con un administrador del sistema, un proveedor de servicios administrados (MSP) o un usuario que tenga el derecho **Modificar ACL de objetos** el área funcional **Características generales: Permisos de usuario**.

Configuración del modo Solo panel

Antes de comenzar el Modo Solo panel, asegúrese de que se cumplan los siguientes requisitos previos:

- Tiene el derecho **Modificar ACL de objetos** en el área funcional **Funciones generales: Permisos de usuario**. Si no tiene este derecho, no verá la pestaña para configurar el modo.
- El usuario tiene el derecho de Lectura en el área funcional **Funciones generales**: **Funcionalidad básica**.

Si hay una jerarquía de Servidores de administración en su red, para configurar el modo Solo panel, vaya al servidor donde la cuenta de usuario está disponible en la sección **USUARIOS Y FUNCIONES → USUARIOS**. Puede ser un servidor primario o un servidor secundario físico. No es posible ajustar el modo en un servidor virtual.

Para configurar el modo Solo panel:

1. En el menú principal, vaya a **USUARIOS Y FUNCIONES → USUARIOS**.

2. Haga clic en el nombre de la cuenta de usuario cuyo panel con widgets desea ajustar.

3. En la ventana de configuración que se abre, seleccione la pestaña **Panel**.

   En la pestaña que se abre, se muestra el mismo Panel para usted que para el usuario.

4. Si está activada la opción **Mostrar la consola en modo de solo panel**, pulse el botón de alternancia para desactivarla.

   Cuando esta opción está activada, tampoco puede cambiar el panel. Después de desactivar la opción, puede administrar los widgets.

5. Configure la apariencia del panel. El conjunto de widgets preparados en la pestaña **Panel** está disponible para el usuario de la cuenta personalizable. Él o ella no puede cambiar ninguna configuración o tamaño de los widgets, ni añadir o eliminar widgets del panel. Por lo tanto, ajústelos para el usuario, para que pueda ver las estadísticas de protección de la red. Para tal efecto, en la pestaña **Panel** puede realizar las mismas acciones con los widgets que en la sección **SUPERVISIÓN E INFORMES → PANEL**:

   - Añadir nuevos widgets al panel de control.
   - Ocultar widgets que el usuario no necesita.
   - Mover widgets para ponerlos en un orden específico.
   - Cambiar el tamaño o la apariencia de los widgets.
   - Cambiar la configuración de los widgets.

6. Pulse el botón de alternancia para activar la opción **Mostrar la consola en modo de solo panel**.

   Después de eso, solo el panel está disponible para el usuario. Él o ella puede monitorear las estadísticas, pero no puede cambiar la configuración de protección de la red ni la apariencia del panel. Como se muestra el mismo panel para usted que para el usuario, tampoco usted puede cambiar el panel.

   Si mantiene la opción desactivada, se muestra el menú principal para el usuario, de modo que pueda realizar varias acciones en Kaspersky Security Center, entre ellas cambiar la configuración de seguridad y los widgets.

7. Haga clic en el botón **Guardar** cuando termine de configurar el modo Solo panel. Solo después de que lo haga, el panel preparado se mostrará al usuario.

8. Si el usuario desea ver las estadísticas de las aplicaciones compatibles de Kaspersky y necesita derechos de acceso para hacerlo, configure los derechos del usuario Después de eso, los datos de las aplicaciones de Kaspersky se muestran al usuario en los widgets de estas aplicaciones.

Ahora el usuario puede iniciar sesión en Kaspersky Security Center con la cuenta personalizada y monitorear las estadísticas de protección de la red en el modo Solo panel.

Informes

Esta sección describe cómo usar informes, administrar plantillas de informes personalizadas, usar plantillas de informes para generar nuevos informes y crear tareas de entrega de informes.

Utilización de informes

La característica de los informes le permiten obtener información numérica detallada sobre la seguridad de la red de su organización, guardar esta información en un archivo, enviarla por correo electrónico e imprimirla.

Los informes están disponibles en Kaspersky Security Center 14 Web Console, en la sección **SUPERVISIÓN E INFORMES**, al hacer clic en **INFORMES**.

De forma predeterminada, los informes incluyen información de los últimos 30 días.

Kaspersky Security Center tiene un conjunto predeterminado de informes de las siguientes categorías:

- **Estado de la protección**
- **Despliegue**
- **Actualización**
- **Estadísticas de amenazas**
- **Otros**

Puede crear plantillas de informe personalizadas, modificar plantillas de informe y eliminarlas.

Puede crear informes que se basan en plantillas existentes, exportar informes a archivos y crear tareas para la entrega del informe.

Crear una plantilla de informes

Para crear una plantilla de informes:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **INFORMES**.
2. Haga clic en **Añadir**.

   Se ejecutará el Asistente de nueva plantilla de informe. Avance a través del Asistente utilizando el botón **Siguiente**.
3. En la primera página del Asistente, introduzca el nombre del informe y seleccione el tipo de informe.
4. En la página del Asistente **Cobertura**, seleccione el conjunto de dispositivos cliente (grupo de administración, selección de dispositivos, dispositivos seleccionados o todos los dispositivos de red) cuyos datos se mostrarán en informes que se basen en esta plantilla de informe.
5. En la página del Asistente **Período del informe**, especifique el periodo del informe. Los valores disponibles son los siguientes:

   - Entre las dos fechas especificadas
   - Desde la fecha especificada hasta la fecha de creación del informe
   - Desde la fecha de creación del informe menos el número especificado de días hasta la fecha de creación del informe

   Esta página puede no aparecer para algunos informes.

6. Haga clic **Aceptar** para cerrar el Asistente.

7. Realice una de las siguientes acciones:

   - Haga clic en el botón **Guardar y ejecutar** para guardar la nueva plantilla de informes y ejecutar un informe basado esto.

     Se guarda la plantilla del informe. Se genera el informe.

   - Haga clic en el botón **Guardar** para guardar la nueva plantilla de informe.

     Se guarda la plantilla del informe.

Se puede utilizar esta nueva plantilla para generar y visualizar informes.

Ver y editar las propiedades de la plantilla de informe

Puede ver y editar las propiedades básicas de una plantilla de informe, por ejemplo, el nombre de la plantilla de informe o los campos que se muestran en el informe.

Para ver y editar las propiedades de una plantilla de informe:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **INFORMES**.

2. Seleccione la casilla de verificación junto a la plantilla de informe cuyas propiedades quiere ver y modificar.

   Como una alternativa, primero puede generar el informe y después hacer clic en el botón **Editar**.

3. Haga clic en el botón **Abrir propiedades de plantillas de informes**.

   Se abre la ventana **Editar informe <Nombre del informe>** con la pestaña **Control de aplicaciones** seleccionada.

4. Editar las propiedades de la plantilla del informe:

   - Pestaña **Control de aplicaciones**:

     - Nombre de la plantilla de informe

     - **Número máximo de entradas que mostrar**

Si esta opción está activada, el número de entradas que se muestran en la tabla con datos detallados del informe no excede el valor especificado.

Las entradas de informe se ordenan primero de acuerdo con las reglas especificadas en la sección **Campos → Campos detallados** de las propiedades de la plantilla de informe y luego solo se conserva la primera de las entradas resultantes. El encabezado de la tabla con datos detallados del informe muestra el número de entradas que se muestra y el número total de entradas disponibles que coinciden con otras configuraciones de la plantilla de informes.

Si esta opción está desactivada, la tabla con datos detallados del informe muestra todas las entradas disponibles. No le recomendamos que utilice esta opción. La limitación del número de entradas de informe visualizadas reduce la carga en el sistema de administración de bases de datos (DBMS) y reduce el tiempo requerido para generar y exportar el informe. Algunos de los informes contienen demasiadas entradas. Si este es el caso, puede resultarle difícil leerlos y analizarlos todos. Además, su dispositivo puede quedarse sin memoria mientras genera un informe de este tipo, y, por consiguiente, no podrá ver el informe.

Esta opción está activada de forma predeterminada. El valor predeterminado es 1000.

- **Grupo**

  Haga clic en el botón **Configuración** para cambiar el conjunto de dispositivos cliente para los que se crea el informe. Para algunos tipos de informes, el botón puede no estar disponible. La configuración real depende de la configuración especificada durante la creación de la plantilla de informe.

- **Intervalo de tiempo**

  Haga clic en el botón **Configuración** para modificar el periodo del informe. Para algunos tipos de informes, el botón puede no estar disponible. Los valores disponibles son los siguientes:

  - Entre las dos fechas especificadas
  - Desde la fecha especificada hasta la fecha de creación del informe
  - Desde la fecha de creación del informe menos el número especificado de días hasta la fecha de creación del informe

- Incluir datos de los Servidores de administración secundarios y virtuales

  Si esta opción está activada, el informe incluye la información de los Servidores de administración secundarios y virtuales que están subordinados al Servidor de administración para el cual se crea la plantilla de informe.

  Desactive esta opción si desea ver solo los datos del Servidor de administración actual.

  Esta opción está activada de forma predeterminada.

- Hasta el nivel de anidamiento

  El informe incluye datos de los Servidores de administración secundarios y virtuales que se encuentran bajo el Servidor de administración actual en un nivel de anidamiento menor o igual al valor especificado.

  El valor predeterminado es 1. Es posible que desee cambiar este valor si tiene que recuperar información de los Servidores de administración secundarios ubicados en los niveles más bajos del árbol.

- Intervalo de espera de datos (min)

Antes de generar el informe, el Servidor de administración para el que se crea la plantilla de informe espera los datos de los Servidores de administración secundarios durante la cantidad de minutos especificada. Si no se reciben datos de un Servidor de administración secundario al final de este periodo, el informe se ejecuta de todos modos. En lugar de los datos reales, el informe muestra los datos tomados del caché (si la opción **Copiar en caché datos de los Servidores de administración secundarios** está activada) o, por el contrario, **N/A** (no disponible).

El valor predeterminado es 5 (minutos).

- Copiar en caché datos de los Servidores de administración secundarios

  Los Servidores de administración secundarios transfieren regularmente datos al Servidor de administración para el que se crea la plantilla del informe. Allí, los datos transferidos se almacenan en el caché.

  Si el Servidor de administración actual no puede recibir datos de un Servidor de administración secundario mientras genera el informe, se muestran los datos tomados de la caché en él. También se muestra la fecha en que se transfirieron los datos al caché.

  Habilitar esta opción le permite ver la información de los Servidores de administración secundarios, incluso si no se pueden recuperar los datos actualizados. Sin embargo, los datos mostrados pueden ser obsoletos.

  Esta opción está desactivada de forma predeterminada.

- Frecuencia de actualización de la caché (h)

  Los Servidores de administración secundarios transfieren a intervalos regulares datos al Servidor de administración para el que se crea la plantilla del informe. Puede especificar este periodo en horas. Si especifica 0 horas, los datos se transfieren solo cuando se termina de generar el informe.

  El valor predeterminado es 0.

- Transferir información detallada desde los Servidores de administración secundarios

  En el informe generado, la tabla con datos detallados del informe incluye datos de los Servidores de administración secundarios del Servidor de administración para los cuales se crea la plantilla del informe.

  Habilitar esta opción ralentiza la generación de informes y aumenta el tráfico entre los Servidores de administración. Sin embargo, puede ver todos los datos en un informe.

  En lugar de activar esta opción, es posible que desee analizar datos de informes detallados para detectar un Servidor de administración secundario defectuoso y luego generar el mismo informe solo para ese Servidor de administración defectuoso.

  Esta opción está desactivada de forma predeterminada.

- Pestaña **Campos**

  Seleccione los campos que se mostrarán en el informe y utilice el botón **Subir** y el botón **Bajar** para cambiar el pedido de estos campos. Use el botón **Añadir** o **Editar** para especificar si la información en el informe debe ser ordenada y filtrada por cada uno de los campos.

  En la sección **Filtros de los campos de detalles**, también puede hacer clic en el botón **Convertir filtros** para comenzar a usar el formato de filtrado extendido. Este formato le permite combinar las condiciones de filtrado especificadas en varios campos, utilizando la operación lógica OR. Después de hacer clic en el botón, a la derecha se abre el panel **Convertir filtros**. Haga clic en el botón **Convertir filtros** para confirmar la revocación. Ahora puede definir un filtro convertido con condiciones de la sección **Campos detallados** que se aplican mediante la operación lógica OR.

La conversión de un informe al formato que admite condiciones de filtrado complejas hará que el informe sea incompatible con las versiones anteriores de Kaspersky Security Center (11 y anteriores). Además, el informe convertido no contendrá ningún dato de los Servidores de administración secundarios que ejecuten versiones incompatibles.

5. Haga clic en **Guardar** para guardar los cambios.
6. Haga clic en el botón de **Cerrar** (⨯) para cerrar la ventana **Edición del informe <Nombre del informe>**.

La plantilla de informe actualizada aparece en la lista de plantillas de informe.

Exportación de un informe a un archivo

Puede exportar un informe a un archivo XML, HTML o PDF.

Para exportar un informe a un archivo:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. Seleccione la casilla de verificación junto al informe que desea exportar a un archivo.
3. Haga clic en el botón **Exportar informe**.
4. En la ventana que se abre, cambie el nombre del archivo del informe en el campo **Nombre**. De forma predeterminada, el nombre de archivo coincide con el nombre de la plantilla de informe seleccionada.
5. Seleccione el tipo de archivo del informe: XML, HTML o PDF.
6. Haga clic en el botón **Exportar informe**.

   El informe en el formato seleccionado se descargará a su dispositivo, a la carpeta predeterminada de su dispositivo, o se abrirá una ventana estándar **Guardar como** en su navegador para permitirle guardar el archivo donde desee.

El informe se guarda al archivo.

Generación y visualización de un informe

Para crear y visualizar un informe:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → INFORMES**.
2. Haga clic en el nombre de la planilla de informe que desea usar para crear un informe.

Se genera y se muestra un informe utilizando la plantilla seleccionada.

El informe muestra los siguientes datos:

- En la pestaña **Resumen**:

- El nombre y tipo de informe, una descripción breve del mismo y el periodo cubierto, así como información sobre el grupo de dispositivos para el que se generará el informe.
- Gráfico que muestra los datos más representativos del informe.
- Tabla consolidada con indicadores de informe calculados.

- Sobre la pestaña **Detalles** se muestra una tabla con los datos detallados del informe.

Crear una tarea de entrega de informes

Puede crear una tarea que entregará informes seleccionados.

Para crear una tarea de entrega de informes:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **INFORMES**.
2. [Opcional] Seleccione la casilla junto a la plantilla de informe para la que desea crear una tarea de generación de informe.
3. Haga clic en el botón **Nueva tarea de entrega de informes**.
4. Se inicia el Asistente para añadir tareas. Avance a través del Asistente utilizando el botón **Siguiente**.
5. En la primera página del Asistente, introduzca el nombre de la tarea. El nombre predeterminado es **Entregar informes (<N>)**, donde <N> es el número de la secuencia de la tarea.
6. En la página de configuración de tareas del Asistente, especifique la siguiente configuración:
   a. Plantillas de informes a ser entregados por la tarea. Si los seleccionó en el paso 2, omita este paso.
   b. El formato del informe: HTML, XLS, o PDF.
   c. Si los informes se enviarán por correo electrónico, junto con la configuración de las notificaciones de correo electrónico.
   d. Si los informes se guardarán en una carpeta, si los informes guardados anteriormente en esta carpeta se sobrescribirán y si una cuenta específica se usará para acceder a la carpeta (para una carpeta compartida).
7. Si desea modificar otras configuraciones de tarea después de crear la tarea, en la página **Finalizar la creación de tareas** del Asistente, active la opción **Abrir los detalles de la tarea cuando se complete la creación**.
8. Haga clic en el botón **Crear** para crear la tarea y cerrar el Asistente.

   Se crea la tarea de entrega de informes. Si activó la opción **Abrir los detalles de la tarea cuando se complete la creación**, se abre la ventana de configuración de tareas.

Eliminación de las plantillas del informe

Eliminar una o varias plantillas de informe:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **INFORMES**.

2. Seleccione la casilla de verificación al lado de las plantillas de informe que desee eliminar.

3. Haga clic en el botón **Eliminar**.

4. En la ventana que se abre, haga clic en **Aceptar** para confirmar su selección.

Se eliminan las plantillas de informe seleccionadas. Si estas plantillas de informes se incluyeron en las tareas de entrega de informes, también se eliminan de las tareas.

Eventos y selecciones de eventos

Esta sección proporciona información sobre eventos y selecciones de eventos, sobre los tipos de eventos que ocurren en los componentes de Kaspersky Security Center y sobre cómo administrar el bloqueo de eventos frecuentes.

Utilización de selecciones de eventos

Las selecciones de eventos proporcionan una vista en pantalla de los conjuntos de eventos con nombre que se seleccionan desde la base de datos del Servidor de administración. Estos conjuntos de eventos se agrupan según las siguientes categorías:

- Por nivel de importancia: **Eventos críticos**, **Fallos operativos**, **Advertencias** y **Eventos de información**
- Por tiempo: **Eventos recientes**
- Por tipo: **Solicitudes de los usuarios** y **Eventos de auditoría**

Puede crear y ver selecciones de eventos definidos por el usuario según la configuración disponible en la interfaz de Kaspersky Security Center 14 Web Console para configurarlas.

Las selecciones de eventos están disponibles en Kaspersky Security Center 14 Web Console, en la sección **SUPERVISIÓN E INFORMES**, al hacer clic en **SELECCIONES DE EVENTOS**.

De forma predeterminada, las selecciones de eventos incluyen información de los últimos 7 días.

Kaspersky Security Center tiene un conjunto predeterminado de las selecciones (predefinidas) del evento:

- Eventos con niveles de importancia diferentes:
  - **Eventos críticos**
  - **Fallos operativos**
  - **Advertencias**
  - **Mensajes de información**
- **Solicitudes de usuario** (eventos de aplicaciones administradas)
- **Eventos recientes** (durante la semana anterior)

- **Eventos de auditoría**.

También puede crear y configurar selecciones adicionales definidas por el usuario. En las selecciones definidas por el usuario, puede filtrar eventos por las propiedades de los dispositivos de los que se originaron (nombres de dispositivos, rangos de IP y grupos de administración), por tipos de evento y niveles de gravedad, por nombre de aplicación y componente, y por intervalo de tiempo. También es posible incluir resultados de tareas en el ámbito de búsqueda. También puede usar un campo de búsqueda simple donde se puede escribir una palabra o varias palabras. Se muestran todos los eventos que contienen cualquiera de las palabras escritas en cualquier lugar de sus atributos (como el nombre del evento, la descripción y el nombre del componente).

Tanto para selecciones predefinidas como definidas por el usuario, puede limitar el número de eventos mostrados o el número de registros para buscar. Ambas opciones afectan al tiempo que tarda Kaspersky Security Center en mostrar los eventos. Cuanto más grande es la base de datos, más lento puede ser el proceso.

Puede hacer lo siguiente:

- Editar propiedades de las selecciones de eventos
- Generar selecciones de eventos
- Ver detalles de las selecciones de eventos
- Eliminar selecciones de eventos
- Eliminar eventos de la base de datos del Servidor de administración

Creación de una selección de eventos

Para crear una selección de eventos:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → SELECCIONES DE EVENTOS**.
2. Haga clic en **Añadir**.
3. En la ventana **Nueva selección de eventos** que se abre, especifique la configuración de la nueva selección de eventos. Haga esto en una o varias de las secciones en la ventana.
4. Haga clic en **Guardar** para guardar los cambios.

   Se abre la ventana de confirmación.
5. Para ver el resultado de la selección de eventos, mantenga seleccionada la casilla **Ir al resultado de la selección**.
6. Haga clic en **Guardar** para confirmar la creación de selección de eventos.

Para ver el resultado de la selección de eventos, mantenga activada la casilla **Ir al resultado de la selección**. De otro modo, la nueva selección de eventos aparece en la lista de selecciones de eventos.

Editar una selección de eventos

Editar una selección de eventos:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → SELECCIONES DE EVENTOS**.
2. Seleccione la casilla de verificación junto a la selección de eventos que quiera editar.
3. Haga clic en el botón **Propiedades**.
   Se abrirá una ventana de configuración de selección de eventos.
4. Editar las propiedades de la selección de eventos.

   > Para selecciones de eventos predefinidas, solo puede editar las propiedades en las siguientes pestañas: **Control de aplicaciones** (excepto el nombre de selección), **Hora** y **Derechos de acceso**.

   Para las selecciones definidas por el usuario, puede editar todas las propiedades.
5. Haga clic en **Guardar** para guardar los cambios.

La selección de eventos editado se muestra en la lista.

Visualización de una lista de una selección de eventos

Para ver una selección de eventos:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → SELECCIONES DE EVENTOS**.
2. Seleccione la casilla de verificación al lado de la selección de eventos que quiera iniciar.
3. Realice una de las siguientes acciones:
   - Si desea configurar la clasificación en el resultado de selección de eventos, haga lo siguiente:
     a. Haga clic en el botón **Reconfigurar la clasificación y comenzar**.
     b. En la ventana que se muestra **Reconfigurar la clasificación para la selección de eventos**, especifique la configuración de clasificación.
     c. Haga clic en el nombre de la selección.
   - De lo contrario, si desea ver la lista de eventos tal como están ordenados en el Servidor de administración, haga clic en el nombre de la selección.

Se muestra el resultado de selección de eventos.

Ver detalles de un evento

Para ver detalles de un evento:

1. Iniciar una selección de eventos.
2. Haga clic en la hora del evento requerido.
   Se abre la ventana **Propiedades del evento**.
3. En la ventana mostrada, puede hacer lo siguiente:
   - Consultar la información sobre el evento seleccionado
   - Ir al siguiente evento y al evento anterior en el resultado de selección de eventos
   - Ir al dispositivo en el que ocurrió el evento
   - Ir al grupo de administración que incluye el dispositivo en el que ocurrió el evento
   - Para un evento relacionado con una tarea, vaya a las propiedades de la tarea

Exportar eventos a un archivo

Exportar eventos a un archivo:

1. Iniciar una selección de eventos.
2. Seleccione la casilla de verificación junto al evento requerido.
3. Haga clic en el botón **Exportar a archivo**.

El evento seleccionado se exporta a un archivo.

Visualización de un historial de objeto desde un evento

Desde un evento de creación o modificación de un objeto que admite la administración de la revisión, puede cambiar al historial de la revisión del objeto.

Para visualizar un historial de objeto desde un evento:

1. Iniciar una selección de eventos.
2. Seleccione la casilla de verificación junto al evento requerido.
3. Haga clic en el botón **Historial de revisión**.

El historial de la revisión del objeto se abre.

Eliminar eventos

Para eliminar uno o varios eventos:

1. Iniciar una selección de eventos.
2. Seleccione las casillas de verificación junto a los eventos requeridos.
3. Haga clic en el botón **Eliminar**.

Los eventos seleccionados se eliminan y no se pueden restaurar.

Eliminación de selecciones de eventos

Puede eliminar solo las selecciones de eventos definidas por el usuario. Las selecciones de eventos predefinidas no se pueden eliminar.

Para eliminar una o varias selecciones de eventos:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → SELECCIONES DE EVENTOS**.
2. Seleccione las casillas de verificación junto a las selecciones de eventos que desea eliminar.
3. Haga clic en **Eliminar**.
4. En la ventana que se abre, haga clic en **Aceptar**.

Se elimina la selección de eventos.

Configuración del plazo de almacenamiento para un evento

Kaspersky Security Center le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre eventos se guarda en la base de datos del Servidor de administración. Es posible que deba almacenar algunos eventos durante un período de tiempo más largo o más corto que el especificado por los valores predeterminados. Puede cambiar la configuración predeterminada del término de almacenamiento para un evento.

Si no está interesado en almacenar algunos eventos en la base de datos del Servidor de administración, puede desactivar la configuración adecuada en la directiva del Servidor de administración y la directiva de aplicación de Kaspersky, o en las propiedades del Servidor de administración (solo para eventos del Servidor de administración). Esto reducirá el número de tipos de evento en la base de datos.

Cuanto más largo sea el término de almacenamiento para un evento, más rápidamente alcanzará su capacidad máxima la base de datos. Sin embargo, un término de almacenamiento más largo para un evento le permite realizar tareas de supervisión e informes durante un período de tiempo más largo.

Para establecer el término de almacenamiento para un evento en la base de datos del Servidor de administración:

1. Seleccione **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Realice una de las siguientes acciones:

- Para configurar el término de almacenamiento de los eventos del Agente de red o de una aplicación Kaspersky administrada, haga clic en el nombre de la directiva correspondiente.

  Se abre la ventana de propiedades de la directiva.

- Para configurar los eventos del Servidor de administración, en la parte superior de la pantalla, haga clic en el icono de la **Configuración** ( ) al lado del nombre del Servidor de administración requerido.

  Si tiene una directiva para el Servidor de administración, puede hacer clic en el nombre de esta directiva.

  Se abre la página de propiedades del Servidor de administración (o la página de propiedades de la directiva del Servidor de administración).

3. Seleccione la pestaña **Configuración de eventos**.

   Se muestra una lista de los tipos de evento relacionados con la sección **Crítico**.

4. Seleccione la sección de **Fallo operativo**, **Advertencia** o **Información**.

5. En la lista de tipos de evento en el panel derecho, haga clic en el enlace del evento cuyo término de almacenamiento desea cambiar.

   En la sección **Registro de eventos** de la ventana que se abre, la opción **Almacenar en la base de datos del Servidor de administración durante (días)** está activada.

6. En el cuadro de edición debajo de este botón de alternancia, introduzca la cantidad de días para almacenar el evento.

7. Si no desea almacenar un evento en la base de datos del Servidor de administración, desactive la opción **Almacenar en la base de datos del Servidor de administración durante (días)**.

   Si configura los eventos del Servidor de administración en la ventana de propiedades del Servidor de administración y si la configuración del evento está bloqueada en la directiva del Servidor de administración de Kaspersky Security Center, no puede redefinir el valor del término de almacenamiento para un evento.

8. Haga clic en **Aceptar**.

   Se cierra la ventana de propiedades de la directiva.

A partir de ahora, cuando el Servidor de Administración reciba y almacene los eventos del tipo seleccionado, estos tendrán el plazo de almacenamiento modificado. El Servidor de administración no cambia el plazo de almacenamiento de los eventos recibidos anteriormente.

Tipos de evento

Cada componente de Kaspersky Security Center tiene su propio conjunto de tipos de evento. Esta sección enumera los tipos de eventos que ocurren en el Servidor de administración de Kaspersky Security Center, Agente de red, Servidor de MDM para iOS y Servidor de dispositivos móviles de Exchange. Los tipos de eventos que ocurren en las aplicaciones de Kaspersky no se enumeran en esta sección.

Estructura de datos de descripción de tipo de evento

Para cada tipo de evento, se proporcionan su nombre para mostrar, el identificador (Id.), el código alfabético, la descripción y el plazo de almacenamiento predeterminado.

- **Nombre de visualización del tipo de evento**. Este texto se muestra en Kaspersky Security Center cuando configura los eventos y cuando ocurren.
- **ID del tipo de evento**. Este código numérico se usa cuando procesa eventos utilizando herramientas de terceros para el análisis de eventos.
- **Tipo de evento** (código alfabético). Este código se usa cuando navega y procesa eventos utilizando vistas públicas que se proporcionan en la base de datos de Kaspersky Security Center y cuando los eventos se exportan a un sistema SIEM.
- **Descripción**. Este texto contiene las situaciones en las que ocurre un evento y lo que puede hacer en tal caso.
- **Plazo de almacenamiento predeterminado**. Este es el número de días durante los cuales el evento se almacena en la base de datos del Servidor de administración y se muestra en la lista de eventos en el Servidor de administración. Transcurrido este periodo, se elimina el evento. Si el valor del plazo de almacenamiento de eventos es 0, dichos eventos se detectan pero no se muestran en la lista de eventos en el Servidor de administración. Si se configuró para guardar dichos eventos en el registro de eventos del sistema operativo, puede encontrarlos allí.

  Puede cambiar el plazo de almacenamiento para eventos:

  - Consola de administración: Configuración del plazo de almacenamiento para un evento
  - Kaspersky Security Center 14 Web Console: Configuración del plazo de almacenamiento para un evento

Otros datos pueden incluir los siguientes campos:

- **event_id**: número único del evento en la base de datos, generado y asignado automáticamente. No se debe confundir con el **ID del tipo de evento**.
- **task_id**: el ID de la tarea que causó el evento (si lo hay).
- **gravedad**: uno de los siguientes niveles de gravedad (en orden ascendente de gravedad):

  0) Nivel de gravedad no válido

  1) Info.

  2) Advertencia

  3) Error

  4) Crítico

Eventos del Servidor de administración

Esta sección contiene información sobre los eventos relacionados con el Servidor de administración.

Eventos críticos del Servidor de administración

La siguiente tabla muestra los tipos de eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Crítico**.

Eventos críticos del Servidor de administración

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plaz almacer predete
Se ha superado el límite de	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Una vez al día, Kaspersky Security	180 días

licencias			Center comprueba si se excede una restricción de licencia. Los eventos de este tipo ocurren cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en dispositivos cliente exceden algunos límites de licencia y si el número de unidades de licencia utilizadas actualmente y cubiertas por una sola licencia supera el 110 % del número total de unidades cubiertas por la licencia. Incluso cuando se produce este evento, los dispositivos cliente están protegidos. Puede responder al evento de las siguientes formas: • Mire la lista de dispositivos administrados. Elimine dispositivos que no están en uso. • Proporcione una licencia para más dispositivos (añada un código de activación o un archivo clave válidos al Servidor de administración). Kaspersky Security Center determina las reglas para generar eventos cuando se excede una restricción de licencia.	
Brote de virus	26 (para	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este	180 días

	Protección frente a amenazas en archivos)		tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto periodo de tiempo. Puede responder al evento de las siguientes formas: • Puede configurar el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se activará o cree una tarea que se ejecutará cuando ocurra este evento.	
Brote de virus	27 (para Protección frente a amenazas en el correo)	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto periodo de tiempo. Puede responder al evento de las siguientes formas: • Puede configurar el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se activará o cree una tarea que se ejecutará cuando ocurra este evento.	180 días
Brote de virus	28 (para	GNRL_EV_VIRUS_OUTBREAK	Los eventos de este	180 días

	firewall)		tipo ocurren cuando el número de objetos maliciosos detectados en varios dispositivos administrados supera el umbral en un corto periodo de tiempo. Puede responder al evento de las siguientes formas: • Puede configurar el umbral en las propiedades del Servidor de administración. • Cree una directiva más estricta que se activará o cree una tarea que se ejecutará cuando ocurra este evento.	
Se ha perdido la conexión con el dispositivo	4111	KLSRV_HOST_OUT_CONTROL	Los eventos de este tipo ocurren si un dispositivo administrado es visible en la red pero no se ha conectado al Servidor de administración durante un cierto periodo de tiempo. Averigüe lo que impide el buen funcionamiento del Agente de red en el dispositivo. Las causas posibles incluyen problemas de red y la eliminación de Agente de red del dispositivo.	180 días
El estado del dispositivo es Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Los eventos de este tipo ocurren cuando se le asigna el estado *Crítico* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del	180 días

			dispositivo se cambia a *Crítico*.	
El archivo clave se ha añadido a la lista de rechazados	4124	KLSRV_LICENSE_BLACKLISTED	Los eventos de este tipo ocurren cuando Kaspersky ha añadido a la lista de rechazados el código de activación o el archivo clave que usa en la lista de prohibidos. Póngase en contacto con el Servicio de soporte técnico para obtener más detalles.	180 días
Modo de funcionalidad limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Los eventos de este tipo ocurren cuando Kaspersky Security Center empieza a funcionar con funcionalidad básica, sin la Administración de vulnerabilidades y parches y sin la función Administración de dispositivos móviles. A continuación, se presentan las causas y las respuestas adecuadas al evento: • El periodo de vigencia de la licencia ha caducado. Proporcione una licencia para utilizar el modo de funcionalidad completa de Kaspersky Security Center (añada un código de activación válido o un archivo clave al Servidor de administración). • El Servidor de administración gestiona más dispositivos de los que especifica el límite de licencia.	180 días

			Mueva los dispositivos de los grupos de administración de un Servidor de administración a los de otro Servidor de administración (si el límite de licencia del otro Servidor de administración lo permite).	
La licencia caduca pronto	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Ocurren eventos de este tipo cuando se acerca la fecha de caducidad de la licencia comercial. Una vez al día, Kaspersky Security Center comprueba si se acerca la fecha de caducidad de la licencia. Los eventos de este tipo se publican 30 días, 15 días, cinco días y un día antes de la fecha de caducidad de la licencia. No puede cambiar el número de días. Si el Servidor de administración se apaga el día especificado antes de la fecha de caducidad de la licencia, el evento no se publicará hasta el día siguiente. Cuando caduca la licencia comercial, Kaspersky Security Center presta solo la funcionalidad básica. Puede responder al evento de las siguientes formas: • Asegúrese de añadir una clave de licencia de reserva al Servidor de administración.	180 días

			• Si usa una suscripción, asegúrese de renovarla. Una suscripción ilimitada se renueva automáticamente si se ha pagado previamente al proveedor de servicios en el plazo de vencimiento.	
El certificado ha caducado	4132	KLSRV_CERTIFICATE_EXPIRED	Los eventos de este tipo ocurren cuando caduca el certificado del Servidor de administración para la Administración de dispositivos móviles. Debe actualizar el certificado caducado. Puede configurar actualizaciones automáticas de certificados seleccionando la casilla de verificación **Reemitir el certificado automáticamente siempre que sea posible** en la configuración de emisión del certificado.	180 días
Se han anulado las actualizaciones para los módulos del software Kaspersky	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Los eventos de este tipo ocurren si los especialistas técnicos de Kaspersky han revocado las actualizaciones sin problemas (El estado *revocado* se muestra para estas actualizaciones), por ejemplo, se deben actualizar a una versión más reciente. El evento afecta a los parches de Kaspersky Security Center pero no a los módulos de las	180 días

			aplicaciones de Kaspersky administradas. El evento proporciona el motivo por el que no se instalan las actualizaciones sin problemas.	

Servidor de administración eventos de fallos operativos

La siguiente tabla muestra los tipos de eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Fallo operativo**.

Servidor de administración eventos de fallos operativos

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamie predetermin
Error en tiempo de ejecución	4125	KLSRV_RUNTIME_ERROR	Los eventos de este tipo ocurren debido a problemas desconocidos. La mayoría de las veces, se trata de problemas de DBMS, problemas de red y otros problemas de software y hardware. Los detalles del evento se pueden encontrar en la descripción del evento.	180 días
Se ha superado el límite de instalaciones para uno de los grupos de aplicaciones con licencia	4126	KLSRV_INVLICPROD_EXCEDED	El Servidor de administración genera eventos de este tipo de manera periódica (cada hora). Los eventos de este tipo ocurren si administra claves de licencia de aplicaciones de terceros en Kaspersky Security Center y si el número de instalaciones ha superado el límite establecido por la clave de licencia de la aplicación de terceros. Puede responder al evento de las siguientes formas:	180 días

			• Mire la lista de dispositivos administrados. Elimine la aplicación de terceros de los dispositivos en los cuales la aplicación no está en uso. • Utilice una licencia de terceros para más dispositivos. Puede administrar claves de licencia de terceros utilizando la funcionalidad de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia incluye las aplicaciones de terceros que cumplen los criterios establecidos por usted.	
No se ha podido sondear el segmento de la nube	4143	KLSRV_KLCLOUD_SCAN_ERROR	Los eventos de este tipo ocurren cuando el Servidor de administración no puede sondear un segmento de red en un entorno de nube. Lea los detalles en la descripción del evento y actúe en consecuencia.	No almacena
Error al copiar las actualizaciones en la carpeta especificada	4123	KLSRV_UPD_REPL_FAIL	Los eventos de este tipo ocurren cuando las actualizaciones de software se copian a (una) carpeta(s) compartida(s) adicional(es). Puede responder al evento de las siguientes formas: • Compruebe si la cuenta de usuario que se emplea para obtener acceso a la(s) carpeta(s) tiene	180 días

			permiso de escritura. • Compruebe si cambió un nombre de usuario y / o una contraseña de la carpeta(s). • Compruebe la conexión a Internet, ya que podría ser la causa del evento. Siga las instrucciones para actualizar las bases de datos y los módulos de software.	
No queda espacio libre en el disco	4107	KLSRV_DISK_FULL	Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración se queda sin espacio libre. Liberar espacio en disco en el dispositivo.	180 días
La carpeta compartida no está disponible	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Los eventos de este tipo ocurren si la carpeta compartida del Servidor de administración no está disponible. Puede responder al evento de las siguientes formas: • Compruebe si el Servidor de administración (donde se encuentra la carpeta compartida) está encendido y disponible. • Compruebe si se cambió/cambiaron un nombre de usuario y / o una contraseña de la carpeta.	180 días

			• Compruebe la conexión de red.	
La base de datos de información del Servidor de administración no está disponible	4109	KLSRV_DATABASE_UNAVAILABLE	Los eventos de este tipo ocurren si la base de datos del Servidor de administración no está disponible. Puede responder al evento de las siguientes formas: • Compruebe si está disponible el servidor remoto que instala SQL Server. • Vea los registros de DBMS para descubrir el motivo de la falta de disponibilidad de la base de datos del Servidor de administración. Por ejemplo, un servidor remoto que tiene instalado SQL Server podría no estar disponible debido al mantenimiento preventivo.	180 días
No hay espacio libre en la base de datos del Servidor de administración	4110	KLSRV_DATABASE_FULL	Los eventos de este tipo ocurren cuando no hay espacio libre en la base de datos del Servidor de administración. El Servidor de administración no funciona cuando su base de datos ha alcanzado su capacidad y cuando no es posible seguir guardando en la base de datos.	180 días

					A continuación se describen las causas de este evento, según el DBMS que utiliza, y las respuestas adecuadas al evento: • Usted utiliza el DBMS de SQL Server Express Edition: En la documentación de SQL Server Express, revise el límite del tamaño de la base de datos de la versión que utiliza. Probablemente, la base de datos de su Servidor de administración ha superado el límite del tamaño de la base de datos. Limite el número de eventos para almacenar en la base de datos del Servidor de administración. En la base de datos del Servidor de administración hay demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de la directiva de Kaspersky Endpoint Security para Windows relacionada con el almacenamiento de eventos del Control de aplicaciones en la base de datos del Servidor de administración. • Usted utiliza un DBMS distinto de

			SQL Server Express Edition: No limite el número de eventos para almacenar en la base de datos del Servidor de administración. Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración. Revise la información sobre la selección de DBMS.	

Eventos de advertencia del Servidor de administración

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Advertencia**.

Eventos de advertencia del Servidor de administración

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo almacenar predeterm
Se ha superado el límite de licencias	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una vez al día, Kaspersky Security Center comprueba si se excede una restricción de licencia. Los eventos de este tipo ocurren cuando el Servidor de administración detecta que las aplicaciones de Kaspersky instaladas en los dispositivos cliente exceden algunos límites de licencia y si el número de unidades de licencia utilizadas actualmente y cubiertas por una sola licencia constituye del 100 % al 110 % del número total de unidades cubiertas por la licencia.	90 días

			Incluso cuando se produce este evento, los dispositivos cliente están protegidos. Puede responder al evento de las siguientes formas: • Mire la lista de dispositivos administrados. Elimine dispositivos que no están en uso. • Proporcione una licencia para más dispositivos (añada un código de activación o un archivo clave válidos al Servidor de administración). Kaspersky Security Center determina las reglas para generar eventos cuando se excede una restricción de licencia.	
El dispositivo ha permanecido inactivo en la red durante mucho tiempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Los eventos de este tipo ocurren cuando un dispositivo administrado muestra inactividad durante algún tiempo. La mayoría de las veces, esto sucede cuando se da de baja un dispositivo administrado. Puede responder al evento de las siguientes formas: • Elimine manualmente el dispositivo de la lista de dispositivos administrados. • Especifique el intervalo de tiempo después del cual se crea el	90 días

			evento **El dispositivo ha permanecido inactivo en la red durante mucho tiempo** mediante el uso de la Consola de administración o Kaspersky Security Center 14 Web Console. • Especifique el intervalo de tiempo después del cual el dispositivo se eliminará automáticamente del grupo mediante el uso de la Consola de administración o Kaspersky Security Center 14 Web Console.	
Conflicto de nombres de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Los eventos de este tipo ocurren cuando el Servidor de administración considera que dos o más dispositivos administrados distintos son un solo dispositivo. La mayoría de las veces, esto sucede cuando se ha utilizado un disco duro clonado para el despliegue de software en los dispositivos administrados y sin haber cambiado el Agente de red al modo de clonación de discos específico en un dispositivo de referencia.	90 días

			Para evitar este problema, cambie el Agente de red al modo de clonación de discos en un dispositivo de referencia antes de clonar el disco duro de este dispositivo.	
El estado del dispositivo es Advertencia	4114	KLSRV_HOST_STATUS_WARNING	Los eventos de este tipo ocurren cuando se le asigna el estado de *Advertencia* a un dispositivo administrado. Puede configurar las condiciones en las cuales el estado del dispositivo se cambia a *Advertencia*.	90 días
Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia	4127	KLSRV_INVLICPROD_FILLED	Los eventos de este tipo ocurren cuando la cantidad de instalaciones de aplicaciones de terceros incluidas en un grupo de aplicaciones con licencia alcanza el 90 % del valor máximo permitido que se especifica en las propiedades de la clave de licencia. Puede responder al evento de las siguientes formas: • Si la aplicación de terceros no está en uso en algunos de los dispositivos administrados, elimínela de estos dispositivos. • Si cree que la cantidad de instalaciones de la aplicación de terceros excederá pronto el máximo permitido, le recomendamos que adquiera con anticipación una licencia de terceros para una	90 días

			mayor cantidad de dispositivos. Puede administrar claves de licencia de terceros utilizando la funcionalidad de grupos de aplicaciones con licencia.	
Se ha solicitado el certificado	4133	KLSRV_CERTIFICATE_REQUESTED	Los eventos de este tipo ocurren cuando no se puede volver a emitir automáticamente un certificado para Administración de dispositivos móviles. A continuación se mencionan las probables causas del evento y las respuestas adecuadas a este: • Se ha iniciado la nueva emisión automática de un certificado para el que la opción **Reemitir el certificado automáticamente siempre que sea posible** está desactivada. Esto puede deberse a un error ocurrido durante la creación del certificado. Es posible que se deba volver a emitir el certificado de forma manual. • Si utiliza una integración con una infraestructura de clave pública, la causa podría ser la falta del atributo SAM-Account-Name de la cuenta utilizada para la integración con PKI y para la	90 días

			emisión del certificado. Revise las propiedades de la cuenta.	
El certificado se ha eliminado	4134	KLSRV_CERTIFICATE_REMOVED	Los eventos de este tipo ocurren cuando un administrador elimina algún tipo de certificado (General, Correo, VPN) para Administración de dispositivos móviles. Después de eliminar un certificado, los dispositivos móviles que estén conectados a través de este certificado no podrán conectarse al Servidor de administración. Este evento puede resultar útil a la hora de investigar errores asociados con la administración de dispositivos móviles.	90 días
El certificado de APNs ha caducado	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Los eventos de este tipo ocurren cuando caduca un certificado de APNs. Debe renovar el certificado de APNs manualmente e instalarlo en un servidor de MDM para iOS.	No almace
El certificado de APNs caducará pronto	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Los eventos de este tipo ocurren cuando quedan menos de 14 días para que caduque el certificado de APNs. Cuando el certificado de APNs caduca, debe renovarlo manualmente e instalarlo en un servidor de MDM para iOS.	No almace

			Le recomendamos que programe la renovación del certificado de APNs antes de la fecha de caducidad.	
No se ha podido enviar el mensaje FCM al dispositivo móvil	4138	KLSRV_GCM_DEVICE_ERROR	Los eventos de este tipo ocurren cuando Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectarse a dispositivos móviles administrados con sistema operativo Android y cuando el servidor de FCM no puede manejar algunas de las solicitudes que recibe del Servidor de administración. Significa que algunos de los dispositivos móviles administrados no recibirán una notificación push. Lea el código HTTP en los detalles de la descripción del evento y actúe en consecuencia. Para obtener más información sobre los códigos HTTP que se reciben del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (consulte el capítulo "Códigos de respuesta de errores de mensajes descendentes").	90 días
Se produjo un error de HTTP al enviar el mensaje FCM al servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	Los eventos de este tipo ocurren cuando Administración de dispositivos móviles está configurada para usar Google Firebase Cloud Messaging (FCM) para conectar	90 días

			dispositivos móviles administrados con sistema operativo Android y cuando el servidor de FCM devuelve un código HTTP distinto de 200 (OK) a la solicitud del Servidor de administración. A continuación se mencionan las probables causas del evento y las respuestas adecuadas a este: • Problemas en el lado del servidor de FCM. Lea el código HTTP en los detalles de la descripción del evento y actúe en consecuencia. Para obtener más información sobre los códigos HTTP que se reciben del servidor de FCM y los errores relacionados, consulte la documentación del servicio Google Firebase (consulte el capítulo "Códigos de respuesta de errores de mensajes descendentes"). • Problemas del servidor proxy (si usa un servidor proxy). Lea el código HTTP en los detalles del evento y actúe en consecuencia.	
No se ha podido enviar el mensaje FCM al servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	Los eventos de este tipo ocurren debido a errores inesperados en el Servidor de administración cuando se trabaja con el protocolo	90 días

			HTTP de Google Firebase Cloud Messaging. Lea los detalles en la descripción del evento y actúe en consecuencia. Si no puede encontrar la solución para un problema por su cuenta, le recomendamos que se comunique con el Servicio de soporte técnico de Kaspersky.	
Poco espacio libre en el disco duro	4105	KLSRV_NO_SPACE_ON_VOLUMES	Los eventos de este tipo ocurren cuando el disco duro del dispositivo donde está instalado el Servidor de administración casi se queda sin espacio libre. Liberar espacio en disco en el dispositivo.	90 días
Poco espacio libre en la base de datos del Servidor de administración	4106	KLSRV_NO_SPACE_IN_DATABASE	Los eventos de este tipo ocurren si el espacio en la base de datos del Servidor de administración es demasiado reducido. Si no soluciona la situación, la base de datos del Servidor de administración pronto alcanzará su capacidad y el Servidor de administración no funcionará. A continuación se describen las causas de este evento, según el DBMS que utiliza, y las respuestas adecuadas al evento. Usted utiliza el DBMS de SQL Server Express Edition: • En la documentación de SQL Server Express, revise el	90 días

			límite del tamaño de la base de datos de la versión que utiliza. Probablemente la base de datos de su Servidor de administración esté por alcanzar el límite del tamaño de la base de datos. • Limite el número de eventos para almacenar en la base de datos del Servidor de administración. • En la base de datos del Servidor de administración hay demasiados eventos enviados por el componente Control de aplicaciones. Puede cambiar la configuración de la directiva de Kaspersky Endpoint Security para Windows relacionada con el almacenamiento de eventos del Control de aplicaciones en la base de datos del Servidor de administración. Usted utiliza un DBMS distinto de SQL Server Express Edition: • No limite el número de eventos para almacenar en la base de datos del Servidor de administración. • Reduzca la lista de eventos para almacenar en la

			base de datos del Servidor de administración. Revise la información sobre la selección de DBMS.	
Se ha interrumpido la conexión con el Servidor de administración secundario	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Los eventos de este tipo ocurren cuando se interrumpe una conexión con el Servidor de administración secundario. Lea el Registro de eventos de Kaspersky del dispositivo donde está instalado el Servidor de administración secundario y responda en consecuencia.	90 días
Se ha interrumpido la conexión con el Servidor de administración principal	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Los eventos de este tipo ocurren cuando se interrumpe una conexión con el Servidor de administración principal. Lea el Registro de eventos de Kaspersky del dispositivo donde está instalado el Servidor de administración principal y responda en consecuencia.	90 días
Se han registrado las nuevas actualizaciones para los módulos del software Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Los eventos de este tipo ocurren cuando el Servidor de administración registra actualizaciones nuevas para el software de Kaspersky instalado en los dispositivos administrados que usted debe aprobar para su instalación.	90 días

			Apruebe o rechace las actualizaciones con la Consola de administración o con Kaspersky Security Center Web Console.	
Se ha superado el límite del número de eventos en la base de datos, se ha iniciado la eliminación de eventos	4145	KLSRV_EVP_DB_TRUNCATING	Los eventos de este tipo ocurren cuando ha comenzado la eliminación de eventos antiguos de la base de datos del Servidor de administración después de que se alcanzó la capacidad de la base de datos del Servidor de administración. Puede responder al evento de las siguientes formas: • Cambie el número de eventos almacenados en la base de datos del Servidor de administración. • Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración.	No almace
Se ha superado el límite del número de eventos en la base de datos, los eventos se han eliminado	4146	KLSRV_EVP_DB_TRUNCATED	Los eventos de este tipo ocurren cuando se han eliminado los eventos antiguos de la base de datos del Servidor de administración después de que se alcanzó la capacidad de la base de datos del Servidor de administración. Puede responder al evento de las siguientes formas: • Cambie el número máximo permitido de eventos que se almacenarán en la base de datos del	No almace

			Servidor de administración. • Reduzca la lista de eventos para almacenar en la base de datos del Servidor de administración.	

Eventos informativos del Servidor de administración

La siguiente tabla muestra los eventos del Servidor de administración de Kaspersky Security Center que tienen el nivel de importancia **Información**.

Eventos informativos del Servidor de administración

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha consumido más del 90 % de la clave de licencia	4097	KLSRV_EV_LICENSE_CHECK_90	30 días
Se ha detectado un nuevo dispositivo	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 días
El dispositivo se ha agregado automáticamente al grupo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 días
El dispositivo se ha eliminado del grupo: inactivo en la red durante mucho tiempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 días
Pronto se superará el límite de instalaciones de uno de los grupos de aplicaciones con licencia (ya se ha usado más del 95 %)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 días
Se han encontrado archivos para enviar a Kaspersky para su análisis	4131	KLSRV_APS_FILE_APPEARED	30 días
El ID de instancia de FCM ha cambiado en este dispositivo móvil	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 días
Las actualizaciones se han copiado correctamente en la carpeta especificada	4122	KLSRV_UPD_REPL_OK	30 días
La conexión con el Servidor de administración secundario está establecida	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 días
La conexión con el Servidor de administración principal está establecida	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 días
Las bases de datos se han actualizado	4144	KLSRV_UPD_BASES_UPDATED	30 días

Auditoría: Se ha establecido la conexión con el Servidor de administración	4147	KLAUD_EV_SERVERCONNECT	30 días
Auditoría: Se ha modificado el objeto	4148	KLAUD_EV_OBJECTMODIFY	30 días
Auditoría: El estado del objeto ha cambiado	4150	KLAUD_EV_TASK_STATE_CHANGED	30 días
Comprobar: Parámetros de grupo modificados	4149	KLAUD_EV_ADMGROUP_CHANGED	30 días
Auditoría: Se ha finalizado la conexión al Servidor de administración	4151	KLAUD_EV_SERVERDISCONNECT	30 días
Auditoría: Se han modificado las propiedades del objeto	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 días
Auditoría: Se han modificado los permisos de usuario	4153	KLAUD_EV_OBJECTACLMODIFIED	30 días

Eventos del Agente de red

Esta sección contiene información sobre los eventos relacionados con el Agente de red.

Eventos de fallos operativos del Agente de red

La siguiente tabla muestra los tipos de eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Fallo operativo**.

Eventos de fallos operativos del Agente de red

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Descripción	Plazo de almacenamiento predeterminado
Error al instalar la actualización	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Los eventos de este tipo ocurren si la actualización automática y los parches para los componentes de Kaspersky Security Center no tuvieron éxito. El evento no concierne actualizaciones de las aplicaciones de Kaspersky administradas.	30 días

			Lea la descripción del evento. Un problema de Windows en un Servidor de administración puede ser una razón para este evento. Si la descripción menciona algún problema de la configuración de Windows, resuelva este problema.	
Error al instalar la actualización de software de terceros	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Los eventos de este tipo ocurren si las funciones de la Administración de vulnerabilidades y parches y la Administración de dispositivos móviles están en el uso, y si la instalación de actualizaciones de software de terceros no tuvo éxito. Compruebe si el enlace al software de terceros es válido. Lea la descripción del evento.	30 días
Error al instalar las actualizaciones de Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Los eventos de este tipo ocurren si las actualizaciones de Windows no tuvieron éxito. Configurar las actualizaciones de Windows en una directiva del Agente de red.	30 días

			Lea la descripción del evento. Busque el error en Microsoft Knowledge Base. Póngase en contacto con el servicio de soporte técnico de Microsoft si no puede resolver el problema usted mismo.	

Eventos de advertencia del Agente de red

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Advertencia**.

Eventos de advertencia del Agente de red

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha devuelto una advertencia durante la instalación de la actualización del módulo de software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 días
La instalación de la actualización de software de terceros ha finalizado con una advertencia	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 días
Se ha pospuesto la instalación de la actualización de software de terceros	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 días
Se ha producido un incidente	549	GNRL_EV_APP_INCIDENT_OCCURED	30 días
Se ha iniciado el proxy de KSN. Error en la comprobación de la disponibilidad de KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 días

Eventos informativos de advertencia del Agente de red

La siguiente tabla muestra los eventos del Agente de red de Kaspersky Security Center que tienen el nivel de gravedad **Información**.

Eventos informativos de advertencia del Agente de red

Nombre de visualización del tipo de evento	Id. del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
La actualización de módulos del	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 días

software se ha instalado correctamente			
Se ha iniciado la instalación de la actualización del módulo de software	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 días
La aplicación se ha instalado	7703	KLNAG_EV_INV_APP_INSTALLED	30 días
La aplicación se ha desinstalado	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 días
La aplicación supervisada se ha instalado	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 días
La aplicación supervisada se ha desinstalado	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 días
La aplicación de terceros se ha instalado	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 días
Se ha agregado un nuevo dispositivo	7708	KLNAG_EV_DEVICE_ARRIVAL	30 días
El dispositivo se ha eliminado	7709	KLNAG_EV_DEVICE_REMOVE	30 días
Se ha detectado un nuevo dispositivo	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 días
El dispositivo se ha autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 días
Uso compartido del escritorio de Windows: se ha leído el archivo	7712	KLUSRLOG_EV_FILE_READ	30 días
Uso compartido del escritorio de Windows: se ha modificado el archivo	7713	KLUSRLOG_EV_FILE_MODIFIED	30 días
Uso compartido del escritorio de Windows: se ha iniciado la aplicación	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 días
Uso compartido del escritorio de Windows: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 días
Uso compartido del escritorio de Windows: detenido	7716	KLUSRLOG_EV_WDS_END	30 días
La actualización de software de	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 días

terceros se ha instalado correctamente			
Se ha iniciado la instalación de la actualización de software de terceros	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 días
El proxy de KSN se ha iniciado. La comprobación de disponibilidad de KSN se ha completado correctamente	7719	KSNPROXY_STARTED_CON_CHK_OK	30 días
El proxy de KSN se ha detenido	7720	KSNPROXY_STOPPED	30 días

Eventos del Servidor de MDM para iOS

Esta sección contiene información sobre los eventos relacionados con el Servidor de MDM para iOS.

Eventos de fallos operativos del Servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Fallo operativo**.

Eventos de fallos operativos del Servidor de MDM para iOS

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Error al solicitar la lista de perfiles	PROFILELIST_COMMAND_FAILED	30 días
Error al instalar el perfil	INSTALLPROFILE_COMMAND_FAILED	30 días
Error al eliminar el perfil	REMOVEPROFILE_COMMAND_FAILED	30 días
Error al solicitar la lista de perfiles de aprovisionamiento	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 días
Error al instalar perfil de aprovisionamiento	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 días
Error al quitar el perfil de aprovisionamiento	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 días
Error al solicitar la lista de certificados digitales	CERTIFICATELIST_COMMAND_FAILED	30 días
Error al solicitar la lista de aplicaciones instaladas	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 días
Error al solicitar información general sobre el dispositivo móvil	DEVICEINFORMATION_COMMAND_FAILED	30 días

Error al solicitar información sobre la seguridad	SECURITYINFO_COMMAND_FAILED	30 días
Error al bloquear el dispositivo móvil	DEVICELOCK_COMMAND_FAILED	30 días
Error al restablecer la contraseña	CLEARPASSCODE_COMMAND_FAILED	30 días
Error al borrar los datos del dispositivo móvil	ERASEDEVICE_COMMAND_FAILED	30 días
Error al instalar la app	INSTALLAPPLICATION_COMMAND_FAILED	30 días
Error al establecer el código de recuperación de la aplicación	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 días
Error al solicitar la lista de apps administradas	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 días
Error al eliminar la app administrada	REMOVEAPPLICATION_COMMAND_FAILED	30 días
La configuración de itinerancia se ha rechazado	SETROAMINGSETTINGS_COMMAND_FAILED	30 días
Se ha producido un error en el funcionamiento de la aplicación	PRODUCT_FAILURE	30 días
El resultado del comando contiene datos no válidos	MALFORMED_COMMAND	30 días
Error al enviar la notificación de inserción	SEND_PUSH_NOTIFICATION_FAILED	30 días
No se puede enviar el comando	SEND_COMMAND_FAILED	30 días
Dispositivo no encontrado	DEVICE_NOT_FOUND	30 días

Eventos de advertencia del Servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Advertencia**.

Eventos de advertencia del Servidor de MDM para iOS

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha detectado un intento de conectar el dispositivo móvil bloqueado	INACTICE_DEVICE_TRY_CONNECTED	30 días
El perfil se ha eliminado	MDM_PROFILE_WAS_REMOVED	30 días
Se ha detectado un intento de reutilización de un certificado de cliente	CLIENT_CERT_ALREADY_IN_USE	30 días
Se ha detectado un dispositivo inactivo	FOUND_INACTIVE_DEVICE	30 días
Se requiere un código de recuperación	NEED_REDEMPTION_CODE	30 días
El perfil se ha incluido en una directiva	UMDM_PROFILE_WAS_REMOVED	30 días

eliminada del dispositivo		

Eventos informativos del Servidor de MDM para iOS

La siguiente tabla muestra los eventos del servidor de MDM para iOS de Kaspersky Security Center que tienen el nivel de gravedad **Información**.

Eventos informativos del Servidor de MDM para iOS

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha conectado el nuevo dispositivo móvil	NEW_DEVICE_CONNECTED	30 días
La lista de perfiles se ha solicitado correctamente	PROFILELIST_COMMAND_SUCCESSFULL	30 días
El perfil se ha instalado correctamente	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 días
El perfil se ha eliminado correctamente	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 días
La lista de perfiles de aprovisionamiento se ha solicitado correctamente	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 días
El perfil de aprovisionamiento se ha instalado correctamente	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 días
El perfil de aprovisionamiento se ha eliminado correctamente	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 días
La lista de certificados digitales se ha solicitado correctamente	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 días
La lista de aplicaciones instaladas se ha solicitado correctamente	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 días
Se ha solicitado correctamente la información general sobre el dispositivo móvil	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 días
La información sobre seguridad se ha	SECURITYINFO_COMMAND_SUCCESSFULL	30 días

solicitado correctamente		
Se ha bloqueado correctamente el dispositivo móvil	DEVICELOCK_COMMAND_SUCCESSFULL	30 días
La contraseña se ha restablecido correctamente	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 días
Los datos se han eliminado del dispositivo móvil	ERASEDEVICE_COMMAND_SUCCESSFULL	30 días
La aplicación se ha instalado correctamente	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 días
El código de recuperación de la aplicación se ha establecido correctamente	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 días
Lista de aplicaciones administradas solicitada correctamente	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 días
La aplicación administrada se ha eliminado correctamente	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 días
La configuración de itinerancia se ha aplicado correctamente	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 días

Eventos del Servidor de dispositivos móviles de Exchange

Esta sección contiene información sobre los eventos relacionados con Servidor de dispositivos móviles de Exchange.

Eventos de fallos operativos del servidor de dispositivos móviles de Exchange

La siguiente tabla muestra los eventos del Servidor de dispositivos móviles de Kaspersky Security Center Exchange que tienen el nivel de gravedad **Fallo operativo**.

Eventos de fallos operativos del servidor de dispositivos móviles de Exchange

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Error al borrar los datos del dispositivo móvil	WIPE_FAILED	30 días
No se puede eliminar la información sobre la conexión del dispositivo móvil al buzón	DEVICE_REMOVE_FAILED	30 días

No se puede aplicar la directiva de ActiveSync al buzón de correo	POLICY_APPLY_FAILED	30 días
Error de funcionamiento de la aplicación	PRODUCT_FAILURE	30 días
Error al modificar el estado de la función ActiveSync	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 días

Eventos informativos del Servidor de dispositivos móviles de Exchange

La siguiente tabla muestra los eventos del Servidor de dispositivos móviles de Kaspersky Security Center Exchange que tienen el nivel de gravedad **Información**.

Eventos informativos del Servidor de dispositivos móviles de Exchange

Nombre de visualización del tipo de evento	Tipo de evento	Plazo de almacenamiento predeterminado
Se ha conectado el nuevo dispositivo móvil	NEW_DEVICE_CONNECTED	30 días
Los datos se han eliminado del dispositivo móvil	WIPE_SUCCESSFULL	30 días

Bloqueo de eventos frecuentes

En esta sección se proporciona información sobre cómo administrar el bloqueo de eventos frecuentes y sobre cómo eliminar el bloqueo de eventos frecuentes.

Acerca del bloqueo de eventos frecuentes

Una aplicación administrada, por ejemplo, Kaspersky Endpoint Security para Windows, instalada en uno o varios dispositivos administrados, puede enviar muchos eventos del mismo tipo al Servidor de administración. La recepción de eventos frecuentes puede sobrecargar la base de datos del Servidor de administración y sobrescribir otros eventos. El Servidor de administración comienza a bloquear los eventos más frecuentes cuando el total de eventos recibidos excede el límite especificado para la base de datos.

El Servidor de administración bloquea la recepción automática de eventos frecuentes. No puede bloquear los eventos frecuentes usted, mismo ni elegir qué eventos bloquear.

Si desea saber si un evento está bloqueado, puede ver la lista de notificaciones o comprobar si está presente en la sección **Bloqueo de eventos frecuentes** de las propiedades del Servidor de administración. Si el evento está bloqueado, puede hacer lo siguiente:

- Si desea impedir que se sobrescriba la base de datos, puede continuar bloqueando la recepción de este tipo de eventos.
- Si desea, por ejemplo, encontrar el motivo del envío de los eventos frecuentes al Servidor de administración puede desbloquear los eventos frecuentes y seguir recibiendo los eventos de este tipo de todos modos.
- Si desea seguir recibiendo los eventos frecuentes hasta que se los vuelva a bloquear, puede eliminar el bloqueo de eventos frecuentes.

Gestión del bloqueo de eventos frecuentes

El Servidor de administración bloquea la recepción de eventos frecuentes, pero usted puede desbloquearla y continuar recibiendo eventos frecuentes. También puede bloquear la recepción de eventos frecuentes que desbloqueó antes.

Para gestionar el bloqueo de eventos frecuentes:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Bloqueo de eventos frecuentes**.

3. En la sección **Bloqueo de eventos frecuentes**:

   - Si desea desbloquear la recepción de eventos frecuentes:

     a. Seleccione los eventos frecuentes que desea desbloquear y haga clic en el botón **Excluir**.

     b. Haga clic en el botón **Guardar**.

   - Si desea bloquear eventos frecuentes, haga lo siguiente:

     a. Seleccione los eventos frecuentes que desea bloquear y haga clic en el botón **Bloquear**.

     b. Haga clic en el botón **Guardar**.

El Servidor de administración recibe los eventos frecuentes desbloqueados y no recibe los bloqueados.

Eliminación del bloqueo de eventos frecuentes

Puede eliminar el bloqueo de los eventos frecuentes y comenzar a recibirlos hasta que el Servidor de administración los vuelva a bloquear.

Para eliminar el bloqueo de eventos frecuentes, haga lo siguiente:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Bloqueo de eventos frecuentes**.

3. En la sección **Bloqueo de eventos frecuentes**, seleccione la fila del evento frecuente cuyo bloqueo desea eliminar.

4. Haga clic en el botón **Quitar del bloqueo**.

El evento frecuente se elimina de la lista de eventos frecuentes. El Servidor de administración recibirá eventos de este tipo.

Recepción de eventos de Kaspersky Security para servidores de Microsoft Exchange

La información sobre los eventos durante el funcionamiento de las aplicaciones administradas, como Kaspersky Endpoint Security para Windows, se transfiere desde los dispositivos administrados y se registra en la base de datos del Servidor de administración. De forma predeterminada, los eventos de Kaspersky Security para servidores Microsoft Exchange no se registran en la base de datos del Servidor de administración. Si Kaspersky Security para servidores Microsoft Exchange está instalado en los dispositivos administrados de su organización y desea recibir eventos de esta aplicación, active el registro de eventos de dicha aplicación mediante la utilidad klscflag.

Para activar el registro de eventos de Kaspersky Security para servidores Microsoft Exchange:

1. En el dispositivo del Servidor de administración, ejecute el símbolo del sistema de Windows con una cuenta con derechos de administrador.
2. Cambie su directorio actual a la carpeta de instalación de Kaspersky Security Center (generalmente, C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).
3. Ejecute el siguiente comando:

   ```
   klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
   ```

   El registro de eventos de Kaspersky Security para servidores Microsoft Exchange está activado.

Para Kaspersky Security para servidores Microsoft Exchange, no puede establecer el plazo de almacenamiento de los eventos ni seleccionar qué eventos deben guardarse en el repositorio del Servidor de administración. Puede establecer el número máximo de eventos que se pueden guardar en el repositorio. Esta configuración se aplica a los eventos recibidos de todas las aplicaciones de Kaspersky.

Notificaciones y estados del dispositivo

Esta sección contiene información sobre cómo ver notificaciones, configurar la entrega de notificaciones, usar los estados de los dispositivos y habilitar el cambio de estado de los dispositivos.

Uso de notificaciones

Las notificaciones le alertan sobre eventos y le ayudan a acelerar sus respuestas a estos eventos al realizar acciones recomendadas o acciones que usted considera apropiadas.

Según el método de la notificación elegido, están disponibles los siguientes tipos de notificaciones:

- Notificaciones en pantalla
- Notificaciones por SMS
- Notificaciones por correo electrónico

- Notificaciones por archivo ejecutable o script

Notificaciones en pantalla

Las notificaciones en pantalla le alertan sobre eventos agrupados por niveles de importancia (*Crítico*, *Advertencia* e *Informativo*).

La notificación en pantalla puede tener uno de estos dos estados:

- *Revisado*. Significa que ha realizado la acción recomendada para la notificación o ha asignado este estado para la notificación manualmente.
- *No revisado*. Significa que no ha realizado la acción recomendada para la notificación o ha asignado este estado para la notificación manualmente.

De forma predeterminada, la lista de notificaciones incluye notificaciones en el estado *No revisado*.

Puede supervisar la red de su organización, ver las notificaciones en pantalla y responder a ellas en tiempo real.

Notificaciones por correo electrónico, por SMS y por archivo ejecutable o script

Kaspersky Security Center ofrece la capacidad de supervisar la red de su organización enviando notificaciones sobre cualquier evento que considere importante. Para cualquier evento, puede configurar notificaciones por correo electrónico, SMS o ejecutando un archivo ejecutable o un script.

Al recibir notificaciones por correo electrónico o SMS, puede decidir su respuesta a un evento. La respuesta debe ser la más apropiada para la red de su organización. Al ejecutar un archivo ejecutable o una secuencia de comandos, predefinirá una respuesta a un evento. También puede considerar ejecutar un archivo ejecutable o una secuencia de comandos como respuesta principal a un evento. Después de que se ejecute el archivo ejecutable, puede seguir otros pasos para responder al evento.

Visualización de notificaciones en pantalla

Puede ver las notificaciones en pantalla de tres formas:

- En la sección **SUPERVISIÓN E INFORMES** → **NOTIFICACIONES**. Aquí puede ver las notificaciones relacionadas con las categorías predefinidas.
- En una ventana separada que se puede abrir sin importar qué sección esté usando en ese momento. En este caso puede marcar las notificaciones como revisadas.
- En el widget **Notificaciones por nivel de gravedad seleccionado** en la sección **SUPERVISIÓN E INFORMES PANEL**. En el widget, puede ver solo notificaciones de eventos que se encuentran en los niveles de importancia *Crítico* y *Advertencia*.

Puede realizar acciones: por ejemplo, puede responder a un evento.

Para ver las notificaciones desde las categorías predefinidas:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES** → **NOTIFICACIONES**.

   La categoría **Todas las notificaciones** se selecciona en el panel izquierdo y en el panel derecho se muestran todas las notificaciones.

2. En el panel izquierdo, seleccione una de las categorías:

   - **Despliegue**
   - **Dispositivos**
   - **Protección**
   - **Actualizaciones** (esto incluye notificaciones sobre las aplicaciones de Kaspersky disponibles para descargar y notificaciones sobre actualizaciones de bases de datos antivirus que se han descargado)
   - **Prevención de exploits**
   - **Servidor de administración** (esto incluye eventos que conciernen únicamente al Servidor de administración)
   - **Enlaces útiles** (esto incluye enlaces a recursos de Kaspersky, por ejemplo, Servicio de soporte técnico de Kaspersky, foro de Kaspersky, página de renovación de licencia o Enciclopedia de TI de Kaspersky)
   - **Noticias de Kaspersky** (esto incluye información sobre lanzamientos de aplicaciones de Kaspersky)

   Se muestra una lista de notificaciones de la categoría seleccionada. La lista contiene lo siguientes:

- Icono relacionado con el tema de la notificación: despliegue (), protección (), actualizaciones (), Administrador de dispositivos (), prevención de exploits (), Servidor de administración ().
- Nivel de importancia de la notificación. Se muestran notificaciones de los siguientes niveles de importancia: **Notificaciones críticas** (), **Notificaciones de advertencia** (), **Notificaciones informativas**. Las notificaciones de la lista se agrupan por niveles de importancia.
- **Notificación**. Esto contiene una descripción de la notificación.
- **Acción**. Esto contiene un enlace a una acción rápida que le recomendamos que realice. Por ejemplo, al hacer clic en este enlace, puede ir al repositorio e instalar aplicaciones de seguridad en los dispositivos, o ver una lista de dispositivos o una lista de eventos. Después de realizar la acción recomendada para la notificación, a esta notificación se le asigna el estado *Revisado*.
- **Estado registrado**. Esto contiene la cantidad de días u horas que han pasado desde el momento en que se registró la notificación en el Servidor de administración.

Para ver las notificaciones en pantalla en una ventana separada por nivel de importancia:

1. En la esquina superior derecha de Kaspersky Security Center 14 Web Console, haga clic en el icono del **Banderín** ().

   Si el icono del **Banderín** tiene un punto rojo, hay notificaciones que no se han revisado.

   Se abrirá una ventana con la lista de notificaciones. De forma predeterminada, la pestaña **Todas las notificaciones** se selecciona y las notificaciones son agrupadas por nivel de importancia: *Crítico*, *Advertencia* e *Información*.

2. Seleccione la pestaña **Sistema**.

   Se muestra la lista de notificaciones de niveles de importancia *Crítico* () y *Advertencia* (). La lista de notificaciones incluye lo siguiente:

- Marcador de color. Las notificaciones críticas están marcadas en rojo. Las notificaciones de advertencia están marcadas en amarillo.
- Icono que indica el tema de la notificación: despliegue, protección, actualizaciones, administración de dispositivos, prevención de exploits y Servidor de administración.
- Descripción de la notificación.
- Icono del **Banderín**. El icono de **banderín** está en gris si a las notificaciones se les ha asignado el estado *No revisado*. Cuando selecciona el icono de **banderín** gris y asigna el estado *Revisado* a una notificación, el icono cambia al color blanco.
- Enlace a la acción recomendada. Cuando realiza la acción recomendada después de hacer clic en el enlace, la notificación recibe el estado de *Revisado*.
- Número de días que han pasado desde la fecha en que se registró la notificación en el Servidor de administración.

3. Seleccione la pestaña **Más**.

   Se muestra la lista de notificaciones de nivel de importancia de *información*.

   La organización de la lista es la misma que para la lista en la pestaña **Sistema** (consulte la descripción anterior). La única diferencia es la ausencia de un marcador de color.

Puede filtrar las notificaciones por el intervalo de fecha en que se registraron en el Servidor de administración. Use la casilla de verificación **Mostrar filtro** para administrar el filtro.

Ver notificaciones en pantalla en el widget:

1. En la sección **PANEL**, seleccione **Añadir o restaurar un widget web**.
2. En la ventana que se abre, haga clic en la categoría **Otro**, seleccione el widget **Notificaciones por nivel de gravedad seleccionado** y haga clic en Agregar.

   El widget aparece ahora en la pestaña **PANEL**. De forma predeterminada, las notificaciones del nivel de importancia *Crítico* se muestran en el widget.

   Puede hacer clic en el botón **Configuración** en el widget y cambiar la configuración del widget para ver las notificaciones del nivel de importancia de *Advertencia*. O puede añadir otro widget: **Notificaciones por nivel de importancia seleccionado**, con una *Advertencia* de nivel de importancia.

   La lista de notificaciones en el widget está limitada por su tamaño e incluye dos notificaciones. Estas dos notificaciones se refieren a los últimos eventos.

La lista de notificaciones en el widget incluye lo siguiente:

- Icono relacionado con el tema de la notificación: despliegue, protección, actualizaciones, Administrador de dispositivos, prevención de exploits, Servidor de administración.
- Descripción de la notificación con un enlace a la acción recomendada. Cuando realiza una acción recomendada después de hacer clic en el enlace, la notificación recibe el estado de *Revisado*.
- Número de días o número de horas que han pasado desde la fecha en que se registró la notificación en el Servidor de administración.
- Enlace a otras notificaciones. Al hacer clic en este enlace, se le transfiere a la vista de notificaciones en la sección **NOTIFICACIONES** de la sección **SUPERVISIÓN E INFORMES**.

Acerca de los estados de los dispositivos

Kaspersky Security Center asigna un estado a cada dispositivo administrado. El estado particular depende de si se cumplen las condiciones definidas por el usuario. En algunos casos, al asignar un estado a un dispositivo, Kaspersky Security Center tiene en cuenta el indicador de visibilidad del dispositivo en la red (consulte la tabla a continuación). Si Kaspersky Security Center no encuentra un dispositivo en la red en un plazo de dos horas, el indicador de visibilidad del dispositivo se establece en *No visible*.

Los estados son los siguientes:

- *Crítico* o *Crítico/Visible*
- *Advertencia* o *Advertencia/Visible*
- *Correcto* o *Correcto/Visible*

La tabla a continuación enumera las condiciones predeterminadas que se deben cumplir para asignar el estado *Crítico* o *Advertencia* a un dispositivo, con todos los valores posibles.

Condiciones para asignar un estado a un dispositivo

Condición	Descripción de la condición	Valores disponibles
La aplicación de seguridad no está instalada	El Agente de red está instalado en el dispositivo, pero una aplicación de seguridad no está instalada.	• El botón está activado. • El botón está desactivado.
Demasiados virus detectados	Una tarea de detección de virus (por ejemplo, la tarea *Análisis antivirus*) ha detectado algunos virus en el dispositivo y el número de virus encontrados supera el valor especificado.	Más de 0.
El nivel de protección en tiempo real es distinto del establecido por el administrador	El dispositivo es visible en la red, pero el nivel de la protección en tiempo real se diferencia del nivel configurado (en la condición) por el administrador para el estado del dispositivo.	• Detenido. • En pausa. • En ejecución.
No se ha realizado ningún análisis antivirus desde hace mucho tiempo	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero la tarea *Análisis antivirus* no se ha ejecutado durante el intervalo de tiempo especificado. La condición se aplica solo a los dispositivos que se agregaron a la base de datos del Servidor de administración hace siete días o antes.	Más de 1 día.
Las bases de datos están desactualizadas	El dispositivo es visible en la red y una aplicación de seguridad está instalada en el dispositivo, pero las bases de datos antivirus no se han actualizado en este dispositivo durante el intervalo de tiempo especificado. La condición se aplica solo a los dispositivos que se agregaron a la base de datos del Servidor de administración hace un día o antes.	Más de 1 día.
No conectado durante mucho	El Agente de red está instalado en el dispositivo, pero el dispositivo no se ha conectado a un Servidor de administración durante el	Más de 1 día.

tiempo	intervalo de tiempo especificado porque el dispositivo se desactivó.	
Se han detectado amenazas activas	El número de objetos no procesados en la carpeta **AMENAZAS ACTIVAS** supera el valor especificado.	Más de 0 elementos.
Se requiere reiniciar	El dispositivo es visible en la red, pero una aplicación requiere que el dispositivo se reinicie por más tiempo que el intervalo de tiempo especificado y por una de las razones seleccionadas.	Más de 0 minutos.
Hay aplicaciones incompatibles instaladas	El dispositivo es visible en la red, pero el inventario del software realizado a través del Agente de red ha detectado aplicaciones incompatibles instaladas en el dispositivo.	• El botón está desactivado. • El botón está activado.
Se han detectado vulnerabilidades de software	El dispositivo es visible en la red y el Agente de red está instalado en el dispositivo, pero la tarea *Buscar vulnerabilidades y actualizaciones requeridas* ha detectado vulnerabilidades con el nivel de gravedad especificado en aplicaciones instaladas en el dispositivo.	• Crítico. • Alta. • Media. • Ignorar si no se puede reparar la vulnerabilidad. • Ignorar si se asigna una actualización para su instalación.
La licencia comercial ha caducado	El dispositivo es visible en la red, pero la licencia ha caducado.	• El botón está desactivado. • El botón está activado.
la licencia caduca pronto	El dispositivo es visible en la red, pero la licencia caduca en el dispositivo en menos días que el número especificado de días.	Más de 0 días.
Hace mucho tiempo que no se comprueba si hay actualizaciones de Windows Update	El dispositivo es visible en la red, pero la tarea *Sincronizar Windows Update* no se ha ejecutado durante el intervalo de tiempo especificado.	Más de 1 día.
Estado de cifrado no válido	El Agente de red está instalado en el dispositivo, pero el resultado del cifrado del dispositivo es igual al valor especificado.	• No cumple con la directiva debido a la respuesta del usuario (para

		dispositivos externos solamente). • No cumple con la directiva debido a un error. • Se requiere reiniciar al aplicar la directiva. • No se indica ninguna directiva de cifrado. • No admitido. • Al aplicar la directiva.
La configuración del dispositivo móvil no cumple la directiva	La configuración del dispositivo móvil es diferente de la configuración que se especificó en la directiva de Kaspersky Endpoint Security for Android para dispositivos móviles durante la comprobación de las reglas de cumplimiento.	• El botón está desactivado. • El botón está activado.
Incidentes sin procesar detectados	Se han detectado algunos incidentes no procesados en el dispositivo. Los incidentes se pueden crear automáticamente, mediante las aplicaciones administradas por Kaspersky que están instaladas en el dispositivo cliente, o el administrador las puede crear de forma manual.	• El botón está desactivado. • El botón está activado.
Estado del dispositivo definido por la aplicación	El estado del dispositivo se define por la aplicación administrada.	• El botón está desactivado. • El botón está activado.
El dispositivo no tiene espacio disponible en el disco	El espacio libre en disco en el dispositivo es menor que el valor especificado o el dispositivo no se pudo sincronizar con el Servidor de administración. El estado *Crítico* o *Advertencia* pasa al estado *Correcto* cuando el dispositivo se sincroniza correctamente con el Servidor de administración y el espacio libre en el dispositivo es mayor o igual al valor especificado.	Más de 0 MB.
Se ha perdido la conexión con el dispositivo	Durante la detección de dispositivos, el dispositivo se reconoció como visible en la red, pero más de tres intentos de sincronizar con el Servidor de administración fallaron.	• El botón está desactivado.

		• El botón está activado.
La protección está desactivada	El dispositivo es visible en la red, pero la aplicación de seguridad en el dispositivo se ha desactivado durante más tiempo que el intervalo de tiempo especificado.	Más de 0 minutos.
La aplicación de seguridad no se está ejecutando	El dispositivo es visible en la red y hay una aplicación de seguridad instalada en el dispositivo pero no se está ejecutando.	• El botón está desactivado. • El botón está activado.

Kaspersky Security Center le permite configurar el cambio automático del estado de un dispositivo en un grupo de administración cuando las condiciones especificadas se cumplen. Cuando las condiciones especificadas se cumplen, se asigna al dispositivo cliente uno de los estados siguientes: *Crítico* o *Advertencia*. Cuando no se cumplen las condiciones especificadas, al dispositivo cliente se le asigna el estado *Correcto*.

Distintos estados pueden corresponder a distintos valores de una condición. Por ejemplo, de manera predeterminada, si la condición **Las bases de datos están desactualizadas** tiene el valor **Más de 3 días**, se asigna el estado *Advertencia* al dispositivo cliente; si el valor fuera **Más de 7 días**, se le asignaría el estado *Crítico*.

Si actualiza Kaspersky Security Center desde la versión anterior, los valores de la condición **Las bases de datos están desactualizadas** para asignar el estado a *Crítico* o *Advertencia* no cambian.

Cuando Kaspersky Security Center asigna un estado a un dispositivo, para algunas condiciones (consulte la columna Descripción de la condición) se tiene en cuenta el indicador de visibilidad. Por ejemplo, si a un dispositivo administrado se le ha asignado el estado *Crítico* porque se cumplió la condición Las bases de datos están desactualizadas, y luego se configuró el indicador de visibilidad para el dispositivo, entonces al dispositivo se le asigna el estado *Correcto*.

Configuración del cambio de estado de los dispositivos

Puede cambiar las condiciones para asignar el estado *Crítico* o *Advertencia* a un dispositivo.

Para activar el cambio del estado del dispositivo a Crítico:

1. En el menú principal, vaya a **DISPOSITIVOS → JERARQUÍA DE GRUPOS**.
2. En la lista de grupos que se abre, haga clic en el enlace con el nombre de un grupo para el que desea cambiar los estados de los dispositivos.
3. En la ventana de propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Crítico**.
5. En el panel derecho, en la sección **Se establece en Crítico si se especifican**, active la condición para cambiar un dispositivo al estado *Crítico*.

Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.

6. Seleccione el botón de selección junto a la condición en la lista.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor requerido para la condición seleccionada.

   Los valores no pueden configurarse para cada condición.
9. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Crítico*.

Para activar el cambio del estado del dispositivo a Advertencia:

1. En el menú principal, vaya a **DISPOSITIVOS → JERARQUÍA DE GRUPOS**.
2. En la lista de grupos que se abre, haga clic en el enlace con el nombre de un grupo para el que desea cambiar los estados de los dispositivos.
3. En la ventana de propiedades que se abre, seleccione la pestaña **Estado del dispositivo**.
4. En el panel izquierdo, seleccione **Advertencia**.
5. En el panel derecho, en la sección **Se establece en Advertencia si se especifican**, active la condición para cambiar un dispositivo al estado *Advertencia*.

   Solo puede cambiar la configuración que no esté bloqueada en la directiva primaria.
6. Seleccione el botón de selección junto a la condición en la lista.
7. En la esquina superior izquierda de la lista, haga clic en el botón **Editar**.
8. Configure el valor requerido para la condición seleccionada.

   Los valores no pueden configurarse para cada condición.
9. Haga clic en **Aceptar**.

Cuando se cumplen las condiciones especificadas, al dispositivo administrado se le asigna el estado *Advertencia*.

Configurar entrega de notificaciones

Puede configurar notificaciones sobre eventos que ocurren en Kaspersky Security Center. Según el método de la notificación elegido, están disponibles los siguientes tipos de notificaciones:

- Correo electrónico: Cuando se produce un evento, Kaspersky Security Center envía una notificación a las direcciones de correo electrónico especificadas.
- SMS: Cuando se produce un evento, Kaspersky Security Center envía una notificación a los números de teléfono móvil especificados.

- Archivo ejecutable: cuando ocurre un evento, el archivo ejecutable se ejecuta en el Servidor de administración.

Para configurar la entrega de notificaciones de eventos que ocurren en Kaspersky Security Center:

1. En la parte superior de la pantalla, haga clic en el icono de la **Configuración** ( ) al lado del nombre del Servidor de administración requerido.

   La ventana de propiedades del Servidor de administración se abre con la pestaña **Control de aplicaciones** seleccionada.

2. Haga clic en la sección **Notificación**, y en el panel derecho seleccione la pestaña para el método de notificación que desee:

   - Correo electrónico

La pestaña **Correo electrónico** le permite configurar la notificación de eventos por correo electrónico.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las cuales la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolos con punto y coma. Puede usar los siguientes valores:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

Si activa la opción **Buscar registros MX por DNS**, puede utilizar varios registros MX de las direcciones IP para el mismo nombre DNS del servidor SMTP. El mismo nombre DNS puede tener varios registros MX con diferentes valores de prioridad de recepción de mensajes de correo electrónico. El Servidor de administración intenta enviar notificaciones del correo electrónico al servidor SMTP en orden ascendente de prioridad de registros MX.

Si activa la opción **Buscar registros MX por DNS** y no activa el uso de la configuración de TLS, le recomendamos que use la configuración de DNSSEC en el dispositivo de su servidor como medida adicional de protección para el envío de notificaciones del correo electrónico.

Si habilita la opción **Utilizar autenticación ESMTP**, puede especificar la configuración de autenticación ESMTP en los campos **Nombre de usuario** y **Contraseña**. De forma predeterminada, la opción está deshabilitada y la configuración de autenticación ESMTP no está disponible.

Puede especificar la configuración de TLS para la conexión con un servidor SMTP:

- **No usar TLS**

Puede seleccionar esta opción si desea desactivar el cifrado de mensajes de correo electrónico.

- **Utilizar TLS si es compatible con el servidor SMTP**

Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.

- **Usar siempre TLS, comprobar la validez del certificado del servidor**

Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse con el servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si selecciona el valor **Usar siempre TLS, comprobar la validez del certificado del servidor**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

Puede especificar certificados para una conexión TLS al hacer clic en el enlace **Especificar certificados**:

- Busque un archivo de certificado para el servidor SMTP:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo en el Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

- Busque un archivo de certificado para el cliente:

Puede utilizar un certificado que haya recibido de cualquier fuente, por ejemplo, de cualquier autoridad de certificación confiable. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

- Certificado X-509:

Debe especificar un archivo con el certificado y un archivo con la clave privada. Ambos archivos no dependen el uno del otro y, por ende, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

- Contenedor pkcs12:

Debe cargar un solo archivo que contenga el certificado y su clave privada. Cuando se cargue el archivo, deberá especificar la contraseña para decodificar la clave privada. La contraseña puede tener un valor vacío si la clave privada no está codificada.

En el campo **Asunto**, especifique el asunto del correo electrónico. Puede dejar este campo vacío.

En la lista desplegable **Plantilla de asunto**, seleccione la plantilla para su asunto. Una variable determinada por la plantilla seleccionada se coloca automáticamente en el campo **Asunto**. Puede crear un asunto de correo electrónico seleccionando varias plantillas de asunto.

En el campo **Correo electrónico del remitente: si este valor no está definido, se usará la dirección del destinatario. Advertencia: Le recomendamos que no utilice una dirección de correo electrónico ficticia**, especifique la dirección de correo electrónico del remitente. Si deja este campo vacío, de forma predeterminada, se utiliza la dirección del destinatario. Se recomienda no utilizar direcciones de correo electrónico falsas.

El campo **Mensaje de notificación** contiene el texto estándar con información sobre el evento que la aplicación envía cuando un evento ocurre. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio. Puede editar el texto del mensaje agregando otros parámetros sustitutos con detalles más relevantes del evento.

Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que escribir dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

Al hacer clic en el enlace **Configurar límite numérico de notificaciones**, puede especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Al hacer clic en el botón **Enviar mensaje de prueba**, puede verificar si ha configurado las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que ha especificado.

- SMS

La pestaña **SMS** le permite configurar la transmisión de notificaciones por SMS de varios eventos a un teléfono celular. Los mensajes SMS se envían a través de una puerta de enlace de correo electrónico.

En el campo **Servidores SMTP**, especifique las direcciones del servidor de correo, separándolos con punto y coma. Puede usar los siguientes valores:

- Dirección IPv4 o IPv6
- Nombre de la red de Windows (nombre NetBIOS) del dispositivo
- Nombre DNS del servidor SMTP

En el campo **Puerto del servidor SMTP**, especifique el número de un puerto de comunicación del servidor SMTP. El número de puerto predeterminado es el 25.

Si la opción **Utilizar autenticación ESMTP** está activada, puede especificar la configuración de autenticación ESMTP en los campos **Nombre de usuario** y **Contraseña**. De forma predeterminada, la opción está deshabilitada y la configuración de autenticación ESMTP no está disponible.

Puede especificar la configuración de TLS para la conexión con un servidor SMTP:

- **No usar TLS**

Puede seleccionar esta opción si desea desactivar el cifrado de mensajes de correo electrónico.

- **Utilizar TLS si es compatible con el servidor SMTP**

Puede seleccionar esta opción si desea usar una conexión TLS con un servidor SMTP. Si el servidor SMTP no es compatible con TLS, el Servidor de administración se conecta con el servidor SMTP sin usar TLS.

- **Usar siempre TLS, comprobar la validez del certificado del servidor**

Puede seleccionar esta opción si desea usar la configuración de autenticación de TLS. Si el servidor SMTP no es compatible con TLS, el Servidor de administración no puede conectarse con el servidor SMTP.

Le recomendamos que use esta opción para una mejor protección de la conexión con un servidor SMTP. Si selecciona esta opción, puede establecer la configuración de autenticación para una conexión TLS.

Si selecciona el valor **Usar siempre TLS, comprobar la validez del certificado del servidor**, puede especificar un certificado para la autenticación del servidor SMTP y elegir si desea activar la comunicación mediante cualquier versión de TLS o solo a través de TLS 1.2 o versiones posteriores. Además, puede especificar un certificado para la autenticación del cliente en el servidor SMTP.

Puede especificar un archivo de certificado del servidor SMTP al hacer clic en el enlace **Especificar certificados**:

Puede recibir un archivo con la lista de certificados de una autoridad de certificación confiable y cargar el archivo en el Servidor de administración. Kaspersky Security Center verifica si el certificado de un servidor SMTP también está firmado por una autoridad de certificación confiable. Si el certificado de un servidor SMTP no se recibe de una autoridad de certificación confiable, Kaspersky Security Center no podrá conectarse al servidor SMTP.

En el campo **Destinatarios (direcciones de correo electrónico)**, especifique las direcciones de correo electrónico a las cuales la aplicación enviará notificaciones. Puede especificar varias direcciones en este campo, separándolas con punto y coma. Las notificaciones se transmitirán a los números de teléfono asociados con las direcciones de correo electrónico especificadas.

En el campo **Asunto**, especifique el asunto del correo electrónico.

En la lista desplegable **Plantilla de asunto**, seleccione la plantilla para su asunto. Una variable de acuerdo con la plantilla seleccionada se coloca en el campo **Asunto**. Puede crear un asunto de correo electrónico seleccionando varias plantillas de asunto.

En el campo **Dirección de correo electrónico del remitente: Si este valor no está definido, se usará la dirección del destinatario. Advertencia: No recomendamos usar una dirección de correo electrónico ficticia**, especifique la dirección de correo electrónico del remitente. Si deja este campo vacío, de forma predeterminada, se utiliza la dirección del destinatario. Se recomienda no utilizar direcciones de correo electrónico falsas.

En el campo **Números de teléfono de destinatarios de mensajes SMS**, especifique los números de teléfono celular de los destinatarios de la notificación por SMS.

En el campo **Mensaje de notificación** se especifica un con información sobre el evento que la aplicación envía cuando un evento ocurre. Este texto incluye parámetros sustitutos, como el nombre del evento, el nombre del dispositivo y el nombre del dominio.

Si el texto de la notificación contiene un símbolo porcentual (%), lo tiene que escribir dos veces seguidas para permitir el envío del mensaje. Por ejemplo, "La carga de la CPU es del 100%%".

Haga clic en el enlace **Configurar límite numérico de notificaciones**, para especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

Haga clic en **Enviar mensaje de prueba** para verificar si ha configurado las notificaciones correctamente: la aplicación envía una notificación de prueba al destinatario que ha especificado.

- Archivo ejecutable para lanzar

Si se selecciona este método de notificación, en el campo de entrada puede especificar la aplicación que se iniciará cuando ocurra un evento.

En el campo **Archivo ejecutable que se ejecutará en el Servidor de administración cuando ocurra un evento**, especifique la carpeta y el nombre del archivo que se ejecutará. Antes de especificar el archivo, prepare el archivo y especifique los marcadores que definen los detalles del evento que se enviarán en el mensaje de notificación. La carpeta y el archivo que especifique deben estar ubicados en el Servidor de administración.

Al hacer clic en el enlace **Configurar límite numérico de notificaciones**, puede especificar el número máximo de notificaciones que la aplicación puede enviar durante el intervalo de tiempo especificado.

3. En la pestaña, defina la configuración de la notificación.

4. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

La configuración de entrega de notificaciones guardada se aplica a todos los eventos que ocurren en Kaspersky Security Center.

Puede anular la configuración de entrega de notificación para ciertos eventos en la sección **Configuración de eventos** de la Configuración del Servidor de administración, de una configuración de directiva o de una configuración de aplicación.

Notificaciones de eventos mostradas mediante archivos ejecutables

Kaspersky Security Center puede informar al administrador sobre los eventos de los dispositivos cliente mediante la ejecución de un archivo ejecutable. El archivo ejecutable debe contener otro archivo ejecutable con los marcadores de posición del evento que se transferirá al administrador.

Marcadores de posición para describir un evento

Marcador de posición	Descripción del marcador de posición
%SEVERITY%	Nivel de importancia del evento
%COMPUTER%	Nombre del dispositivo en el que ocurrió el evento
%DOMAIN%	Dominio
%EVENT%	Evento
%DESCR%	Descripción de eventos
%RISE_TIME%	Hora de creación
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nombre de la tarea
%KL_PRODUCT%	Agente de red de Kaspersky Security Center
%KL_VERSION%	Número de versión del Agente de red
%HOST_IP%	Dirección IP
%HOST_CONN_IP%	Dirección IP de conexión

Ejemplo:
Las notificaciones de eventos se envían por medio de un archivo ejecutable (como script1.bat), dentro del cual se inicia otro archivo ejecutable (como script2.bat) con el marcador de posición %COMPUTER%. Cuando ocurre un evento, el archivo script1.bat se abre en el dispositivo del administrador, que a su vez abre el archivo script2.bat con el marcador de posición %COMPUTER%. El administrador recibe el nombre del dispositivo en el que ha ocurrido el evento.

Avisos de Kaspersky

Esta sección describe cómo usar, configurar y desactivar los anuncios de Kaspersky.

Acerca de los anuncios de Kaspersky

La sección Anuncios de Kaspersky (**SUPERVISIÓN E INFORMES** → **Anuncios de Kaspersky**) le mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas que están instaladas en los dispositivos administrados. Kaspersky Security Center actualiza periódicamente la información de la sección, eliminando anuncios desactualizados y añadiendo nueva información.

Kaspersky Security Center muestra solo los anuncios de Kaspersky relacionados con el Servidor de administración conectado y las aplicaciones de Kaspersky instaladas en los dispositivos administrados de este Servidor de administración. Los anuncios se muestran individualmente para cualquier tipo de Servidor de administración: principal, secundario o virtual.

El Servidor de administración debe tener una conexión a Internet para recibir anuncios de Kaspersky.

Los anuncios incluyen información de los siguientes tipos:

- Anuncios relacionados con seguridad

Los anuncios relacionados con seguridad están destinados a mantener las aplicaciones de Kaspersky instaladas en su red actualizadas y completamente funcionales. Los anuncios pueden incluir información sobre actualizaciones críticas para las aplicaciones de Kaspersky, correcciones para las vulnerabilidades encontradas y formas de solucionar otros problemas en las aplicaciones de Kaspersky. Los anuncios relacionados con seguridad están habilitados de forma predeterminada. Si no desea recibir los anuncios, puede desactivar esta función.

Para mostrarle la información que corresponde a la configuración de la protección de su red, Kaspersky Security Center envía datos a los servidores en la nube de Kaspersky y recibe solo aquellos anuncios relacionados con las aplicaciones de Kaspersky instaladas en su red. El conjunto de datos que se puede enviar a los servidores se describe en el Contrato de licencia de usuario final que acepta cuando instala el Servidor de administración de Kaspersky Security Center.

- Anuncios de marketing

  Los anuncios de marketing incluyen información sobre ofertas especiales para sus aplicaciones de Kaspersky, publicidad y noticias de Kaspersky. Los anuncios de marketing están deshabilitados de forma predeterminada. Recibe este tipo de anuncios solo si habilitó Kaspersky Security Network (KSN). Puede desactivar los anuncios de marketing al desactivar KSN.

  Para mostrarle solo información relevante que podría ser útil para proteger sus dispositivos de red y en sus tareas diarias, Kaspersky Security Center envía datos a los servidores en la nube de Kaspersky y recibe los anuncios correspondientes. El grupo de datos que se puede enviar a los servidores se describe en la sección Datos procesados de la Declaración de KSN.

La información nueva se divide en las siguientes categorías según su importancia:

1. Información crítica
2. Novedades importantes
3. Advertencia
4. Información

Cuando aparece información nueva en la sección Anuncios de Kaspersky, Kaspersky Security Center 14 Web Console muestra una etiqueta de notificación que corresponde al nivel de importancia del anuncio. Puede hacer clic en la etiqueta para ver este anuncio en la sección Anuncios de Kaspersky.

Puede especificar la configuración de Anuncios de Kaspersky, incluidas las categorías de anuncios que desea ver y dónde mostrar la etiqueta de notificación.

Especificación de la configuración de anuncios de Kaspersky

En la sección Anuncios de Kaspersky, puede especificar la configuración de los anuncios de Kaspersky, incluidas las categorías de los anuncios que desea ver y dónde mostrar la etiqueta de notificación.

Para configurar los anuncios de Kaspersky:

1. En el menú principal, vaya a **SUPERVISIÓN E INFORMES → ANUNCIOS DE KASPERSKY**.
2. Haga clic en el enlace **Configuración**.

   Se abre la ventana de configuración de Anuncios de Kaspersky.
3. Especifique los siguientes parámetros:

- Seleccione el nivel de importancia de los anuncios que desea ver. No se mostrarán los anuncios de otras categorías.
- Seleccione dónde desea ver la etiqueta de notificaciones. La etiqueta se puede mostrar en todas las secciones de la consola o en la sección **SUPERVISIÓN E INFORMES** y sus subsecciones.

4. Haga clic en el botón **Aceptar**.

   La configuración de Anuncios de Kaspersky está establecida.

Desactivación de anuncios de Kaspersky

La sección Anuncios de Kaspersky (**SUPERVISIÓN E INFORMES** → **Anuncios de Kaspersky**) le mantiene informado al brindarle información relacionada con su versión de Kaspersky Security Center y las aplicaciones administradas que están instaladas en los dispositivos administrados. Si no desea recibir anuncios de Kaspersky, puede desactivar esta función.

Los anuncios de Kaspersky incluyen dos tipos de información: anuncios relacionados con seguridad y anuncios de marketing. Puede desactivar los anuncios de cada tipo por separado.

Para desactivar los anuncios relacionados con seguridad:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Anuncios de Kaspersky**.

3. Ponga el botón de alternancia en la posición **Anuncios relacionados con la seguridad DESACTIVADOS**.

4. Haga clic en el botón **Guardar**.

   Los anuncios de Kaspersky están desactivados.

Los anuncios de marketing están deshabilitados de forma predeterminada. Solo recibirá anuncios de marketing si habilitó Kaspersky Security Network (KSN). Puede desactivar KSN para desactivar este tipo de anuncios.

Para desactivar los anuncios de marketing:

1. En la ventana principal de la aplicación, haga clic en el icono de **Configuración** ( ) junto al nombre del Servidor de administración requerido.

   Se abre la ventana Propiedades del Servidor de administración.

2. En la pestaña **Control de aplicaciones**, seleccione la sección **Configuración de KSN**.

3. Desactive la opción **Cuando esta opción está activada, Kaspersky Security Center envía sus propias estadísticas a KSN para que los analistas de Kaspersky las analicen**.

4. Haga clic en el botón **Guardar**.

   Los anuncios de marketing están desactivados.

Visualización de información sobre la detección de amenazas

Puede activar o desactivar la visualización de información sobre alertas.

*Para activar o desactivar la visualización de la sección **Alertas** en el menú principal:*

1. En el menú principal, vaya a la configuración de su cuenta y elija **Opciones de interfaz.**
2. En la ventana **Opciones de interfaz** que se abre, active o desactive la opción **Mostrar las alertas de EDR**.
3. Hacer clic en **Guardar**.

La consola muestra la subsección **ALERTAS** en la sección **SUPERVISIÓN E INFORMES** del menú principal. En la subsección **ALERTAS**, puede ver información sobre la detección de amenazas en los dispositivos de endpoint. Si se añade una clave de licencia para EDR Optimum, luego Kaspersky Security Center 14 Web Console muestra automáticamente la subsección **ALERTAS** en la sección **SUPERVISIÓN E INFORMES** del menú principal. También se puede añadir un widget que muestre información sobre alertas. Además, si instaló el complemento EDR Optimum, puede ver información detallada sobre las amenazas detectadas al hacer clic en el enlace **más detalles**.

Registro de actividad de Kaspersky Security Center 14 Web Console

El registro de actividad de Kaspersky Security Center 14 Web Console puede ayudar a investigar las causas de un mal funcionamiento del software. Cuando se ponga en contacto con el Servicio de soporte técnico de Kaspersky por un mal funcionamiento de Kaspersky Security Center 14 Web Console, los especialistas del Servicio de soporte técnico de Kaspersky pueden solicitarle los archivos de registro de Kaspersky Security Center 14 Web Console. Los archivos de registro de Kaspersky Security Center 14 Web Console se almacenan en la <Carpeta de instalación de la Kaspersky Security Center 14 Web Console>/registros durante todo el tiempo que use la aplicación. Los archivos de registro no se envían a los especialistas del Servicio de soporte técnico de Kaspersky automáticamente.

Para activar el registro de actividad de Kaspersky Security Center 14 Web Console,

Seleccione la casilla **Activar el registro de actividades de Kaspersky Security Center 14 Web Console** en la ventana **Configuración de la conexión de Kaspersky Security Center 14 Web Console** del Asistente de instalación de Kaspersky Security Center 14 Web Console.

Los archivos de registro están en formato de texto.

Los nombres de los archivos de registro tienen el formato logs- <nombre del componente>.<nombre del dispositivo>-<número de revisión del archivo> .AAAA-MM-DD, donde:

- <nombre del componente> es el nombre del componente Kaspersky Security Center o es el nombre del complemento de administración de Kaspersky Security Center 14 Web Console.
- <nombre de dispositivo> es el nombre del dispositivo en el que se está ejecutando el <nombre de componente>.
- <número de revisión del archivo> es el número del archivo de registro creado para el <nombre del componente> que está en operación en el <nombre del dispositivo>. En un día, se pueden crear varios archivos de registro para el mismo <nombre de componente> y <nombre de dispositivo>. El tamaño máximo de un archivo de registro es de 50 megabytes (MB). Cuando se alcanza el tamaño máximo de archivo, se crea un archivo de registro nuevo. Un archivo de registro nuevo <número de revisión de archivo> se incrementa en 1.
- AAAA, MM y DD son el año, mes y día en que se creó el registro por primera vez. Cuando comienza un día nuevo, se crea un nuevo archivo de registro.

Integración entre Kaspersky Security Center y otras soluciones

Esta sección describe cómo configurar el acceso desde Kaspersky Security Center Web Console a otra aplicación de Kaspersky, como Kaspersky Endpoint Detection and Response y Kaspersky Managed Detection and Response; además, esta sección describe cómo configurar la exportación a sistemas SIEM.

Configuración del acceso a KATA / KEDR Web Console

Kaspersky Anti Targeted Attack (KATA) y Kaspersky Endpoint Detection and Response (KEDR) son dos bloques funcionales de Kaspersky Anti Targeted Attack Platform. Puede administrar estos bloques funcionales a través de Web Console para Kaspersky Anti Targeted Attack Platform (KATA / KEDR Web Console). Si utiliza tanto Kaspersky Security Center 14 Web Console como KATA / KEDR Web Console, puede configurar el acceso a KATA / KEDR Web Console directamente desde la interfaz de Kaspersky Security Center 14 Web Console.

Para configurar el acceso a KATA / KEDR Web Console:

1. En la lista desplegable **Configuración de la consola**, seleccione **Integración**.

   Se abre la ventana **Configuración de la consola**.

2. Seleccione la pestaña **Integración**.

3. En la pestaña **Integración**, seleccione la sección **Data**.

4. Ingrese la URL de KATA/KEDR Web Console en el campo **URL a KATA/KEDR Web Console**.

5. Haga clic en el botón **Guardar**.

Se añade la lista desplegable de **Administración avanzada** en la parte superior de la ventana principal de la aplicación. Puede utilizar este menú para abrir KATA / KEDR Web Console. Después de hacer clic en **Seguridad cibernética avanzada**, se abre una nueva pestaña en su navegador con el URL que ha especificado.

Establecimiento de una conexión en segundo plano

Para permitir que Kaspersky Security Center 14 Web Console realice sus tareas en segundo plano, debe establecer una conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. Puede establecer esta conexión solo si su cuenta tiene el derecho **Modificar LCA de objetos** el área funcional **Funciones generales: Permisos de usuario**.

Si instala el complemento de Kaspersky Endpoint Security para Windows 11.9.0, o si actualiza el complemento de Kaspersky Endpoint Security para Windows desde la versión anterior a la 11.7 y todavía no se ha establecido una conexión en segundo plano, se muestra una notificación de que se debe establecer una conexión en segundo plano. Además, tendrá que conceder a la cuenta de servicio los derechos de las **Características generales**: área funcional de **Operaciones en el Servidor de administración**.

Para establecer una conexión en segundo plano:

1. En la lista desplegable **Configuración de la consola**, seleccione **Integración**.

   Se abre la ventana **Configuración de la consola**.

2. Seleccione la pestaña **Integración**.

3. En la pestaña **Integración**, seleccione la sección **Integración**.

4. Para establecer una conexión en segundo plano, desplace el botón de alternancia a la posición: **Establecer una conexión en segundo plano para la integración ACTIVADO**.

5. En la sección **El servicio que establece una conexión en segundo plano se iniciará en el servidor de Kaspersky Security Center Web Console** abierta, haga clic en el botón **Aceptar**.

Se establece la conexión en segundo plano entre Kaspersky Security Center Web Console y el Servidor de administración. El Servidor de administración crea una cuenta para la conexión en segundo plano y esta cuenta se utiliza como una cuenta de servicio para mantener la interacción entre Kaspersky Security Center y otra aplicación o solución de Kaspersky. El nombre de esta cuenta de servicio contiene el prefijo NWCSvcUser.

El Servidor de administración cambia automáticamente la contraseña de la cuenta de servicio una vez cada 30 días, por razones de seguridad. No puede eliminar este servicio manualmente. El Servidor de administración elimina esta cuenta automáticamente cuando desactiva una conexión entre servicios. El Servidor de administración crea una cuenta de servicio única para cada Consola de administración y asigna todas las cuentas de servicio al grupo de seguridad con el nombre ServiceNwcGroup. El Servidor de administración crea este grupo de seguridad automáticamente durante el proceso de instalación de Kaspersky Security Center. No puede eliminar este grupo de seguridad manualmente.

Exportación de eventos a sistemas SIEM

Esta sección describe cómo configurar la exportación de eventos a los sistemas SIEM.

Configuración de la exportación de eventos a sistemas SIEM

Kaspersky Security Center permite la configuración mediante uno de los siguientes métodos: exportar a cualquier sistema SIEM que utilice formato Syslog, exportar a QRadar, Splunk, ArcSight sistemas SIEM que utilizan formatos LEEF y CEF o exportar eventos a sistemas SIEM directamente desde la base de datos de Kaspersky Security Center. Cuando completa este escenario, el Servidor de administración envía automáticamente eventos al sistema SIEM.

Requisitos previos

Antes de iniciar la exportación de la configuración de eventos en Kaspersky Security Center:

- Obtenga más información sobre los métodos de exportación de eventos.
- Asegúrese de contar con los valores de la configuración del sistema.

Puede realizar los pasos de este escenario en cualquier orden.

El proceso de exportación de eventos al sistema SIEM consta de las siguientes etapas:

- **Configuración del sistema SIEM para recibir eventos de Kaspersky Security Center**

Instrucciones prácticas: Configurar la exportación de eventos en un sistema SIEM

- **Seleccionar eventos que desea exportar al sistema SIEM:**

  Instrucciones:

  - Consola de administración: Marcar eventos de una aplicación de Kaspersky para exportar en formato Syslog, Marcar eventos generales para exportar en formato Syslog
  - Kaspersky Security Center 14 Web Console: Marcado de eventos de una aplicación de Kaspersky para exportar en formato Syslog, Marcado de eventos generales para exportar en formato Syslog

- **Configuración de la exportación de eventos al sistema SIEM utilizando uno de los siguientes métodos:**

  - Utilizando los protocolos TCP/IP, UDP o TLS sobre TCP.

    Instrucciones:

    - Consola de administración: Configurar la exportación de eventos a sistemas SIEM
    - Kaspersky Security Center 14 Web Console: Configuración de la exportación de eventos a sistemas SIEM

  - Usando la exportación de eventos directamente desde la base de datos de Kaspersky Security Center (Se proporciona un conjunto de vistas públicas en la base de datos de Kaspersky Security Center; puede encontrar la descripción de estas vistas públicas en el documento klakdb.chm).

Resultados

Después de configurar la exportación de eventos al sistema SIEM, puede ver los resultados de la exportación si seleccionó los eventos que desea exportar.

Antes de empezar

Al configurar la exportación automática de eventos en Kaspersky Security Center, debe especificar ciertos parámetros de la configuración del sistema SIEM. Se recomienda que compruebe esta configuración de antemano a fin de prepararse para configurar Kaspersky Security Center.

Para configurar correctamente el envío automático de eventos a un sistema SIEM, debe conocer los siguientes ajustes:

- **Dirección del servidor del sistema SIEM**

  La dirección IP del servidor en el que está instalado el sistema SIEM actualmente en uso. Compruebe este valor en su configuración del sistema SIEM.

- **Puerto del servidor del sistema SIEM**

  El número de puerto usado para establecer una conexión entre Kaspersky Security Center y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del receptor de su sistema SIEM.

- **Protocolo**

Protocolo usado para transferir mensajes desde Kaspersky Security Center a su sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del receptor de su sistema SIEM.

Acerca de los eventos en Kaspersky Security Center

Kaspersky Security Center le permite recibir información sobre los eventos de funcionamiento del Servidor de administración y aplicaciones de Kaspersky instaladas en dispositivos administrados. La información sobre eventos se guarda en la base de datos del Servidor de administración. Puede exportar esta información a sistemas SIEM externos. La exportación de la información de eventos a sistemas SIEM externos permite a los administradores de sistemas SIEM responder lo antes posible a eventos del sistema de seguridad que ocurren en dispositivos administrados o grupos de dispositivos.

En Kaspersky Security Center existen los siguientes tipos de eventos:

- Eventos generales. Estos eventos ocurren en todas las aplicaciones de Kaspersky administradas. Por ejemplo, FBrote de virus es un evento general. Los eventos generales tienen una sintaxis y semántica definidas estrictamente. Los eventos generales se utilizan, por ejemplo, en informes y paneles.

- Eventos específicos de aplicaciones de Kaspersky administradas. Cada aplicación de Kaspersky administrada tiene su propio conjunto de eventos.

Cada evento tiene su propio nivel de importancia. Según las condiciones en que se produzca, un evento se puede asignar varios niveles de importancia. Existen cuatro niveles de importancia de eventos:

- Un *evento crítico* es un evento que indica que se ha producido un problema crítico que puede llevar a la pérdida de datos, un funcionamiento defectuoso o un error crítico.

- Un *fallo operativo* es un evento que indica que se ha producido un grave problema, un error o un funcionamiento defectuoso que ocurrió durante el funcionamiento de la aplicación o al realizar un procedimiento.

- Una *advertencia* es un evento que no es necesariamente grave, pero también indica un problema posible en el futuro. La mayor parte de los eventos se designan como advertencias si la aplicación se puede restaurar sin la pérdida de datos o capacidades funcionales después de que tales eventos ocurran.

- Un evento *de información* es un evento que se produce para informar sobre la finalización correcta de una operación, el correcto funcionamiento de la aplicación o la finalización de un procedimiento.

Cada evento tiene un plazo de almacenamiento definido, durante el cual puede verlo o modificarlo en Kaspersky Security Center. Algunos eventos no se guardan en la base de datos del Servidor de administración de forma predeterminada porque su plazo de almacenamiento definido es el cero. Solo los eventos que se almacenarán en la base de datos del Servidor de administración durante al menos un día se pueden exportar a sistemas externos.

Sobre exportación de eventos

Puede utilizar la exportación de eventos en sistemas centralizados que tratan con problemas de seguridad a un nivel organizativo y técnico, proporcionan servicios de supervisión de la seguridad y unifican la información de soluciones diferentes. Estos son sistemas de SIEM, que proporcionan análisis en tiempo real de alertas de seguridad y eventos generados por el hardware de la red y las aplicaciones o Centros operativos de seguridad (SOCs).

Estos sistemas reciben datos desde muchas fuentes, redes incluidas, seguridad, servidores, bases de datos y aplicaciones. Los sistemas SIEM también proporcionan funcionalidad para consolidar datos supervisados a fin de ayudarle a evitar omitir eventos críticos. Además, los sistemas realizan análisis automatizados de eventos correlacionados y alertas a fin de notificar a los administradores sobre problemas de seguridad inmediatos. La generación de alertas se puede implementar a través de un panel o se puede enviar a través de canales de terceros, como el correo electrónico.

El proceso de exportar eventos desde Kaspersky Security Center a sistemas SIEM externos involucra a dos partes: un remitente del evento, Kaspersky Security Center, y un destinatario del evento, un sistema SIEM. Para exportar eventos correctamente, debe configurar estos parámetros en su sistema de SIEM y en la Consola de administración de Kaspersky Security Center. No importa qué componente configura primero. Puede configurar la transmisión de eventos desde Kaspersky Security Center y, a continuación, configurar la recepción de eventos por parte del sistema SIEM o viceversa.

Métodos para enviar eventos desde Kaspersky Security Center

Hay tres métodos para enviar eventos desde Kaspersky Security Center a sistemas externos:

- El envío de eventos con el protocolo de Syslog a cualquier sistema SIEM

  Usando el protocolo de Syslog, puede transmitir cualquier evento que ocurra en el Servidor de administración de Kaspersky Security Center y las aplicaciones de Kaspersky instaladas en dispositivos administrados. El protocolo Syslog es un protocolo de registros de mensajes estándar. Puede utilizarlo para exportar eventos a cualquier sistema SIEM.

  Para ello, debe marcar los eventos que desea transmitir al sistema SIEM. Puede marcar los eventos en la Consola de administración o en Kaspersky Security Center 14 Web Console. Solo los eventos marcados se transmitirán al sistema SIEM. Si no marcó nada, no se retransmitirá ningún evento.

- Enviando eventos sobre protocolos CEF y LEEF a sistemas QRadar, Splunk y ArcSight

  Puede utilizar los protocolos CEF y LEEF para exportar eventos generales. Al exportar eventos en protocolos CEF y LEEF, no tiene la capacidad de seleccionar eventos específicos que exportar. En cambio, todos los eventos generales se exportan. A diferencia del protocolo Syslog, los protocolos CEF y LEEF no son universales. CEF y LEEF están diseñados para los sistemas SIEM apropiados (QRadar, Splunk y ArcSight). Por lo tanto, cuando elige exportar eventos sobre uno de estos protocolos, usa el analizador requerido en el sistema SIEM.

  > Para exportar eventos a través de los protocolos CEF y LEEF, la función Integración con los sistemas SIEM debe activarse en el Servidor de administración utilizando una clave de licencia activa o un código de activación válido.

- Directamente desde la base de datos de Kaspersky Security Center a cualquier sistema SIEM.

  Este método de exportar eventos puede utilizarse para recibir eventos directamente de vistas públicas de la base de datos mediante consultas de SQL. Los resultados de una consulta se guardan a un archivo XML que se puede utilizar como datos de entrada para un sistema externo. Solo los eventos disponibles en vistas públicas se pueden exportar directamente desde la base de datos.

Recepción de eventos por el sistema SIEM

El sistema SIEM debe recibir y analizar correctamente los eventos recibidos desde Kaspersky Security Center. Con estos objetivos, debe configurar correctamente el sistema SIEM. La configuración depende del sistema SIEM específico utilizado. No obstante, hay varios pasos generales en la configuración de todos los sistemas SIEM, por ejemplo, configurando el receptor y el analizador.

Acerca de la configuración de la exportación de eventos en un sistema SIEM

El proceso de exportar eventos desde Kaspersky Security Center a sistemas SIEM externos involucra a dos partes: un remitente del evento – Kaspersky Security Center y un destinatario del evento – sistema SIEM. Debe configurar la exportación de eventos en su sistema SIEM y en Kaspersky Security Center.

La configuración que especifica en el sistema SIEM dependerá del sistema que usted esté usando. Generalmente, para todos los sistemas SIEM debe configurar un receptor y, opcionalmente, un analizador sintáctico del mensaje para analizar los eventos recibidos.

Configuración del receptor

Para poder recibir los eventos enviados por Kaspersky Security Center, debe configurar el receptor en su sistema SIEM. En general, la configuración siguiente se debe especificar en el sistema SIEM:

- **Protocolo de exportación o tipo de entrada**

  Es el protocolo de transferencia del mensaje, TCP/IP o UDP. Este protocolo debe ser el mismo que el protocolo que especificó en Kaspersky Security Center.

- **Puerto**

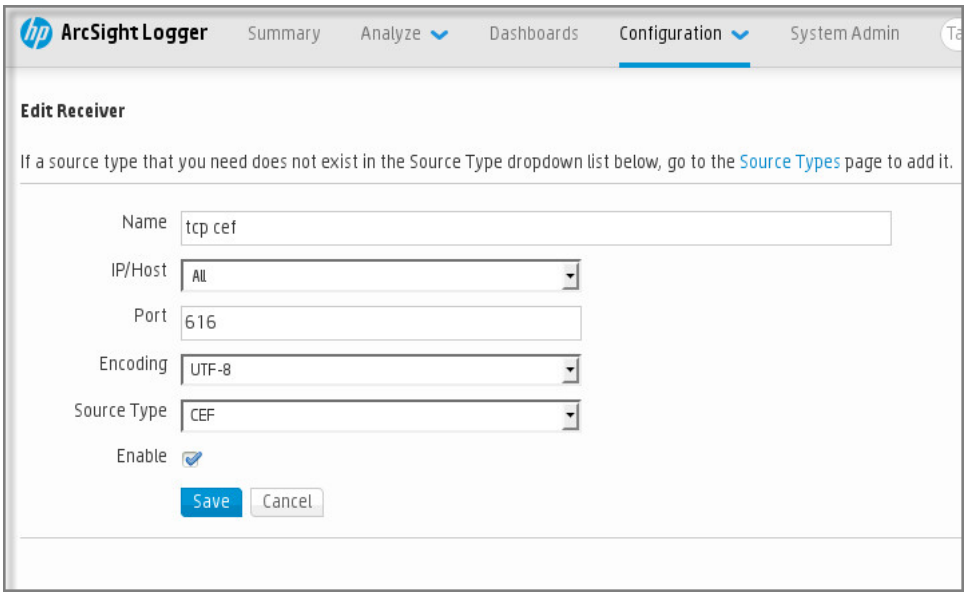
  Número de puerto para conectar con Kaspersky Security Center. Este puerto debe ser igual que el puerto que especificó en Kaspersky Security Center.

- **Protocolo del mensaje o tipo de la fuente**

  El protocolo utilizado para exportar eventos al sistema SIEM. Puede ser uno de los protocolos estándar: Syslog, CEF o LEEF. El sistema SIEM selecciona el analizador sintáctico del mensaje según el protocolo que especifica.

Según el sistema SIEM que utilice, es posible que deba especificar la configuración del receptor adicional.

La cifra siguiente muestra la pantalla de instalación del receptor en ArcSight.



Instalación del receptor en ArcSight

Analizador sintáctico del mensaje

Los eventos de Exportar se transfieren a sistemas SIEM como mensajes. Estos mensajes se deben analizar correctamente de modo que la información sobre los eventos se pueda utilizar por el sistema SIEM. Los analizadores sintácticos de los mensajes son una parte del sistema SIEM; se utilizan para dividir los contenidos del mensaje en los campos relevantes, como ID del evento, gravedad, descripción, parámetros, etc. Esto permite al sistema SIEM procesar eventos recibidos de Kaspersky Security Center de modo que se puedan almacenar en la base de datos del sistema SIEM.

Cada sistema SIEM tiene un conjunto de analizadores de mensajes estándar. Kaspersky también proporciona analizadores de mensajes para algunos sistemas SIEM, por ejemplo, para QRadar y ArcSight. Puede descargar estos analizadores de mensajes de los sitios web de los sistemas SIEM correspondientes. Al configurar el receptor, puede seleccionar utilizar uno de los analizadores de mensajes estándar o un analizador de mensajes de Kaspersky.

Marcado de eventos para exportar a sistemas SIEM en formato Syslog

Esta sección describe cómo marcar eventos para su posterior exportación a sistemas SIEM en formato Syslog.

Acerca del marcado de eventos para exportar al sistema SIEM en formato Syslog

Después de activar la exportación automática de eventos, debe seleccionar qué eventos se exportarán al sistema SIEM externo.

Puede configurar la exportación de eventos en formato Syslog a un sistema externo según una de las condiciones siguientes:

- Marcado de eventos generales. Si marca los eventos para exportar en una directiva, en la configuración de un evento, o en la configuración del Servidor de administración, el sistema SIEM recibirá los eventos marcados que se produjeron en todas las aplicaciones administradas por la directiva específica. Si los eventos exportados se seleccionaran en la directiva, no podrá redefinirlos para una aplicación particular administrada por esta directiva.

- Marcado de eventos para una aplicación administrada. Si marca eventos para exportar para una aplicación administrada instalada en un dispositivo administrado, el sistema SIEM solo recibirá los eventos que hayan ocurrido en esta aplicación.

Marcar eventos de una aplicación de Kaspersky para exportar en formato Syslog

Si desea exportar los eventos ocurridos en una aplicación administrada específica instalada en los dispositivos administrados, marque los eventos para su exportación en la directiva de aplicaciones. En este caso, los eventos marcados se exportan desde todos los dispositivos incluidos en la cobertura de la directiva.

Para marcar eventos que desea exportar para una aplicación administrada específica:

1. En el menú principal, vaya a **DISPOSITIVOS → DIRECTIVAS Y PERFILES**.
2. Haga clic en la directiva de la aplicación para la que desea marcar los eventos.

   Se abre la ventana de configuración de directivas.
3. Vaya a la sección **Configuración de eventos**.
4. Seleccione las casillas junto a los eventos que desea exportar a un sistema SIEM.
5. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   También puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de eventos**, que se abre al hacer clic en el enlace del evento.
6. Una marca de verificación (✓) aparece en la columna **Syslog** del evento o los eventos que haya marcado para exportar al sistema SIEM.
7. Haga clic en el botón **Guardar**.

Los eventos marcados desde la aplicación administrada están listos para ser exportados a un sistema SIEM.

Puede marcar los eventos que desea exportar a un sistema SIEM para un dispositivo administrado específico. Si se marcaron eventos previamente exportados en una directiva de aplicación, no podrá redefinir los eventos marcados para un dispositivo administrado.

Para marcar los eventos para la exportación de un dispositivo administrado, haga lo siguiente:

1. En el menú principal, vaya a **DISPOSITIVOS → DISPOSITIVOS ADMINISTRADOS**.

   Se muestra la lista de dispositivos administrados.
2. Haga clic en el enlace con el nombre del dispositivo requerido en la lista de dispositivos administrados.

   Se muestra la ventana de propiedades del dispositivo seleccionado.
3. Vaya a la sección **Aplicaciones**.
4. Haga clic en el enlace con el nombre de la aplicación pertinente en la lista de aplicaciones.
5. Vaya a la sección **Configuración de eventos**.

6. Seleccione las casillas de verificación junto a los eventos que desea exportar a SIEM.
7. Haga clic en el botón **Marcar para exportar al sistema SIEM mediante Syslog**.

   Además, puede marcar un evento para exportarlo a un sistema SIEM en la sección **Registro de eventos**, que se abre al hacer clic en el enlace del evento.

8. Una marca de verificación (✓) aparece en la columna **Syslog** del evento o los eventos que haya marcado para exportar al sistema SIEM.

A partir de ahora, el Servidor de administración envía los eventos marcados al sistema SIEM si la exportación al sistema SIEM está configurada.

Marcar eventos generales para exportar en formato Syslog

Puede utilizar el formato Syslog para marcar eventos generales que el Servidor de administración exportará a sistemas SIEM.

Para marcar eventos generales para exportar a un sistema SIEM:

1. Realice una de las siguientes acciones:
   - Haga clic en el icono de **Configuración** (⚙) junto al nombre del Servidor de administración requerido.
   - En el menú principal, vaya a **DISPOSITIVOS** → **DIRECTIVAS Y PERFILES** y, luego, haga clic en el enlace de una directiva.
2. En la ventana que se abre, diríjase a la pestaña **Configuración de eventos**.
3. Haga clic en **Marcar para exportar al sistema SIEM mediante Syslog**.

   Además, puede marcar un evento para exportarlo al sistema SIEM en la sección **Registro de eventos**, que se abre al hacer clic en el enlace del evento.

4. Una marca de verificación (✓) aparece en la columna **Syslog** del evento o los eventos que haya marcado para exportar al sistema SIEM.

A partir de ahora, el Servidor de administración envía los eventos marcados al sistema SIEM si la exportación al sistema SIEM está configurada.

Acerca de la exportación de mediante los protocolos CEF y LEEF

Puede utilizar los formatos CEF y LEEF para exportar eventos generales a los sistemas SIEM, como así también eventos que las aplicaciones de Kaspersky transfieren al Servidor de administración. El conjunto de eventos de exportación está predefinido, y no puede seleccionar los eventos que exportarse.

Para exportar eventos a través de los protocolos CEF y LEEF, la función Integración con los sistemas SIEM debe activarse en el Servidor de administración utilizando una clave de licencia activa o un código de activación válido.

Seleccione el formato de exportación que corresponda al sistema SIEM utilizado. La tabla a continuación muestra sistemas SIEM y los formatos de exportación correspondientes.

Formatos de exportación de eventos a un sistema SIEM

Sistema SIEM	Formato de exportación
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - es un formato de evento personalizado para IBM Security QRadar SIEM. QRadar puede integrar, identificar y procesar eventos LEEF. Los eventos LEEF deben usar la codificación de caracteres UTF-8. Puede encontrar información detallada sobre el protocolo LEEF en IBM Knowledge Center.

- CEF (Common Event Format): un estándar de administración de registros abierto que mejora el interoperabilidad de la información relacionada con la seguridad desde dispositivos y aplicaciones de seguridad y red diferentes. CEF le permite usar un formato de registros de eventos común de modo que los datos se puedan integrar y añadir fácilmente para que un sistema de administración de la empresa los analice.

La exportación automática significa que Kaspersky Security Center envía eventos generales al sistema SIEM. La exportación automática de eventos comienza inmediatamente después de que se activa. Esta sección explica detalladamente cómo activar la exportación automática de eventos.

Acerca de la exportación de eventos mediante el formato Syslog

Puede utilizar el formato Syslog para exportar a sistemas SIEM los eventos que se producen en el Servidor de administración y otras aplicaciones de Kaspersky instaladas en dispositivos administrados.

Syslog es un estándar para el protocolo de registro de mensajes. Permite la separación del software que genera mensajes, el sistema que los almacena y el software que los notifica y los analiza. Cada mensaje se etiqueta mediante un código, indicando el tipo del software que genera el mensaje y se le asigna un nivel de gravedad.

El formato Syslog se define por los documentos Request for Comments (RFC) publicados por el Internet Engineering Task Force (estándares de Internet). El estándar RFC 5424 se utiliza para exportar los eventos desde Kaspersky Security Center a sistemas externos.

En Kaspersky Security Center, puede usar el protocolo de Syslog para configurar la exportación de los eventos a sistemas externos.

El proceso de exportación consiste en dos pasos:

1. La activación de la exportación de evento automática. En este paso, Kaspersky Security Center se configura de modo que envíe eventos al sistema SIEM. Kaspersky Security Center empieza a enviar eventos inmediatamente después de que usted active la exportación automática.

2. La selección de los eventos que exportar al sistema externo. En este paso, usted selecciona qué evento exportar al sistema SIEM.

Configuración de Kaspersky Security Center para la exportación de eventos a un sistema SIEM

Este artículo describe cómo configurar la exportación de eventos a sistemas SIEM.

Para configurar la exportación a sistemas SIEM en Kaspersky Security Center 14 Web Console:

1. En la lista desplegable **Configuración de la consola**, seleccione **Integración**.

   Se abre la ventana **Configuración de la consola**.

2. Seleccione la pestaña **Integración**.

3. En la pestaña **Integración**, seleccione la sección **SIEM**.

4. Haga clic en el enlace **Configuración**.

   Se abre la sección **Exportar configuración**.

5. Ajuste la configuración en la sección **Exportar configuración**:

   - **Dirección del servidor del sistema SIEM**

     La dirección IP del servidor en el que está instalado el sistema SIEM actualmente en uso. Compruebe este valor en su configuración del sistema SIEM.

   - **Puerto del sistema SIEM**

     El número de puerto usado para establecer una conexión entre Kaspersky Security Center y su servidor del sistema SIEM. Especifica este valor en la configuración de Kaspersky Security Center y en la configuración del receptor de su sistema SIEM.

   - **Protocolo**

Seleccione el protocolo para transferir mensajes al sistema SIEM. Puede seleccionar el protocolo TCP/IP, UDP o TLS sobre TCP.

Puede ajustar la configuración de TLS si selecciona TLS sobre el protocolo TCP:

- **Autenticación del servidor**

  En el campo **Autenticación del servidor**, puede seleccionar los valores **Certificados de confianza** o **Huellas digitales SHA**:

  - **Certificados de confianza**. Puede recibir un archivo con la lista de certificados de una autoridad de certificados (CA) de confianza y cargar el archivo en Kaspersky Security Center. Kaspersky Security Center verifica si el certificado del servidor del sistema SIEM también está firmado por una CA de confianza o no.

    Para agregar un certificado de confianza, haga clic en el botón **Busque archivo de certificados de CA** y, a continuación, cargue el certificado.

  - **Huellas digitales SHA**. Puede especificar huellas digitales SHA-1 de certificados del sistema SIEM en Kaspersky Security Center. Para agregar una huella digital SHA-1, introdúzcala en el campo **Huellas digitales** y, a continuación, haga clic en el botón **Añadir**.

  Al usar el ajuste **Añadir autenticación del cliente**, puede generar un certificado para autenticar Kaspersky Security Center. Por lo tanto, utilizará un certificado autofirmado emitido por Kaspersky Security Center. En este caso, puede usar un certificado de confianza y una huella digital SHA para autenticar el servidor del sistema SIEM.

- **Añadir Nombre del sujeto/Nombre alternativo del sujeto**

  El nombre del sujeto es un nombre de dominio para el que se recibe el certificado. Kaspersky Security Center no puede conectarse al servidor del sistema SIEM si el nombre de dominio del servidor del sistema SIEM no coincide con el nombre del sujeto del certificado del servidor del sistema SIEM. Sin embargo, el servidor del sistema SIEM puede cambiar su nombre de dominio si el nombre ha cambiado en el certificado. En este caso, se pueden especificar los nombres de sujeto en el campo **Añadir Nombre del sujeto/Nombre alternativo del sujeto**. Si alguno de los nombres de sujeto especificados coincide con el nombre de sujeto del certificado del sistema SIEM, Kaspersky Security Center validará el certificado del servidor del sistema SIEM.

- **Añadir autenticación del cliente**

  Para la autenticación del cliente, puede insertar su certificado o generarlo en Kaspersky Security Center.

  - **Ingresar certificado**. Puede utilizar un certificado que haya recibido de cualquier fuente; por ejemplo, de cualquier CA de confianza. Debe especificar el certificado y su clave privada mediante uno de los siguientes tipos de certificado:

    - **PEM certificado X.509**. Cargue un archivo con un certificado en el campo **Archivo con certificado** y un archivo con una clave privada en el campo **Archivo con clave**. Ninguno de estos archivos dependen el uno del otro y, por tanto, no importa el orden en el que se carguen. Cuando se carguen ambos archivos, especifique la contraseña para descodificar la clave privada en el campo **Verificación de certificado o contraseña**. La contraseña puede tener un valor vacío si la clave privada no está codificada.

    - **PKCS12 certificado X.509**. Cargue un único archivo que contenga un certificado y su clave privada en el campo **Archivo con certificado**. Cuando se cargue el archivo, especifique la contraseña para descodificar la clave privada en el campo **Verificación de certificado o contraseña**. La contraseña puede tener un valor vacío si la clave privada no está codificada.

- **Generar clave**. Puede generar un certificado autofirmado en Kaspersky Security Center. Como resultado, Kaspersky Security Center almacena el certificado autofirmado generado y puede pasar la parte pública del certificado o huella digital SHA1 al sistema SIEM.

- Formato de los datos

  Puede seleccionar los formatos Syslog, CEF o LEEF, según lo requiera el sistema SIEM.

Si selecciona el formato Syslog, debe especificar:

- Tamaño máximo del mensaje de evento en bytes

  Especifique el tamaño máximo (en bytes) de un mensaje transmitido al sistema SIEM. Cada evento se transmite en un mensaje. Si la longitud real de un mensaje supera el valor especificado, el mensaje se trunca y los datos se pueden perder. El tamaño predeterminado es 2048 bytes. Este campo solo está disponible si seleccionó el formato de Syslog en el campo **Protocolo**.

6. Cambie la opción a la posición **Exportación automática de eventos a la base de datos del sistema SIEM ACTIVADA**.

7. Haga clic en el botón **Guardar**.

La exportación al sistema SIEM queda configurada.

Exportar eventos directamente desde la base de datos

Puede recuperar eventos directamente desde la base de datos de Kaspersky Security Center sin necesidad de usar la interfaz de Kaspersky Security Center. Puede consultar las vistas públicas directamente y recuperar los datos del evento o crear sus propias vistas sobre la base de las vistas públicas existentes y dirigirse a ellas para conseguir los datos que necesita.

Vistas públicas

Para su comodidad, se proporciona un conjunto de vistas públicas en la base de datos de Kaspersky Security Center. Puede encontrar la descripción de estas vistas públicas en el documento klakdb.chm.

La vista pública v_akpub_ev_event contiene un conjunto de campos que representan los parámetros del evento en la base de datos. En el documento klakdb.chm también puede encontrar información sobre vistas públicas correspondiente a otras entidades de Kaspersky Security Center, por ejemplo, dispositivos, aplicaciones o usuarios. Puede usar esta información en sus consultas.

Esta sección contiene instrucciones para crear una consulta SQL mediante la utilidad klsql2 y un ejemplo de consulta.

Para crear consultas SQL o vistas de bases de datos, también puede utilizar cualquier otro programa para trabajar con bases de datos. En la sección correspondiente, se proporciona información sobre cómo ver los parámetros para conectar a la base de datos de Kaspersky Security Center, como el nombre de la instancia y nombre de la base de datos.

Creación de una consulta SQL usando la herramienta klsql2

Esta sección describe cómo descargar y usar la utilidad klsql2, y cómo crear una consulta SQL usando esta utilidad. Cuando crea una consulta SQL por medio de la utilidad klsql2, no tiene que proporcionar el nombre de la base de datos ni parámetros de acceso, porque la consulta aborda las vistas públicas de Kaspersky Security Center directamente.

Para descargar y usar la utilidad klsql2:

1. Descargar la utilidad klsql2 desde el sitio web de Kaspersky.
2. Copie y extraiga el archivo klsql2.zip descargado en cualquier carpeta en el dispositivo con el Servidor de administración de Kaspersky Security Center instalado.

   El paquete klsql2.zip incluye los archivos siguientes:

   - klsql2.exe
   - src.sql
   - start.cmd
3. Abra el archivo src.sql en cualquier editor de texto.
4. En el archivo src.sql, escriba la consulta SQL que desee y guarde el archivo.
5. En el dispositivo con el Servidor de administración de Kaspersky Security Center instalado, en la línea de comandos, escriba el comando siguiente para ejecutar la consulta SQL desde el archivo src.sql y guarde los resultados en el archivo result.xml:
   ```
   klsql2 -i src.sql -o result.xml
   ```
6. Abra el archivo result.xml recién creado para ver los resultados de la consulta.

Puede modificar el archivo src.sql y crear cualquier consulta en las vistas públicas. A continuación, desde la línea de comandos, ejecute su pregunta y guarde los resultados en un archivo.

Ejemplo de una consulta SQL en la utilidad klsql2

Esta sección muestra un ejemplo de una consulta SQL, creada por medio de la utilidad klsql2.

El ejemplo siguiente ilustra la recuperación de los eventos que ocurrieron en dispositivos durante los últimos siete días, y muestra los eventos solicitados cuando ocurren; los eventos más recientes se muestran primero.

Ejemplo:

```
SELECT
e.nId, /* identificador de eventos */
e.tmRiseTime, /* hora, cuando se produjo el evento */
e.strEventType, /* nombre interno del tipo de evento */
e.wstrEventTypeDisplayName, /* nombre del evento mostrado */
e.wstrDescription, /* descripción del evento mostrada */
e.wstrGroupName, /* nombre del grupo, donde se encuentra el dispositivo */
h.wstrDisplayName, /* nombre del dispositivo mostrado, en el que se produjo el
evento */
```

```
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 /* IP-address del dispositivo, donde se
produjo el evento */
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
```

La visualización del nombre de la base de datos de Kaspersky Security Center

Si desea acceder a la base de datos de Kaspersky Security Center por medio de las herramientas de administración de bases de datos SQL Server, MySQL o MariaDB, debe conocer el nombre de la base de datos a fin de conectarse desde su editor de scripts de SQL.

Ver el nombre de la base de datos de Kaspersky Security Center:

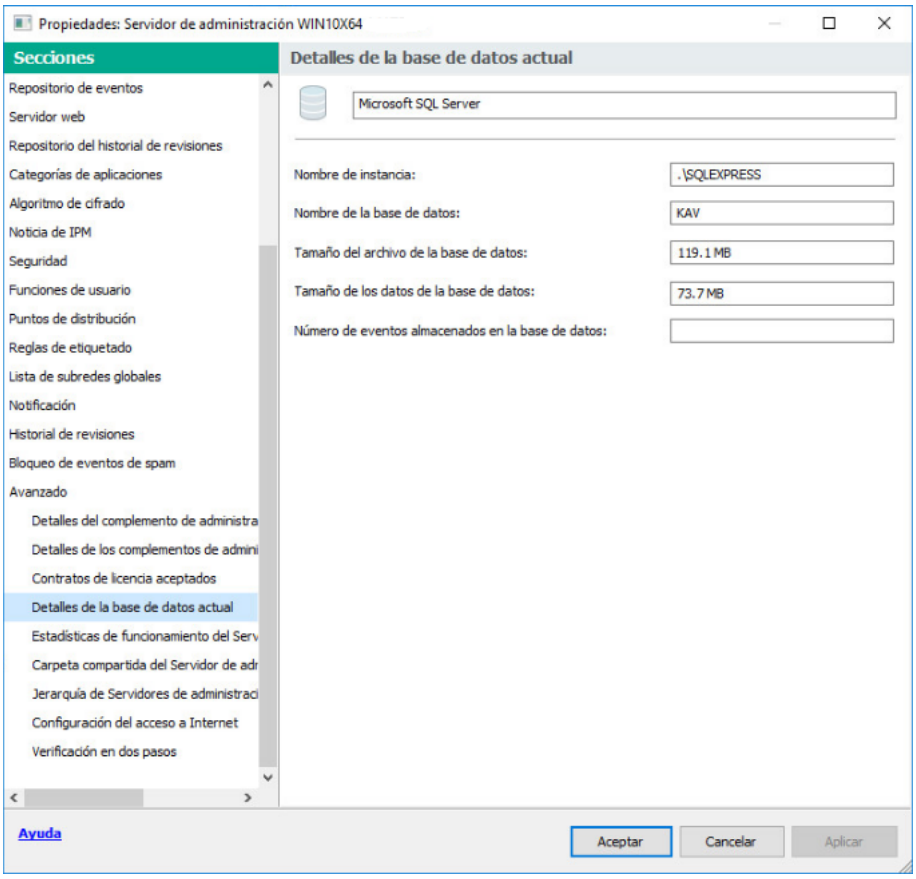
1. En el árbol de consola de Kaspersky Security Center, abra el menú contextual de la carpeta **Servidor de administración** y seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración, en el panel **Avanzado**, seleccione **Detalles de la base de datos actual**.
3. En la sección **Detalles de la base de datos actual**, tenga en cuenta las propiedades de la base de datos siguientes (consulte la siguiente figura):

   - **Nombre de instancia**

     Nombre de la instancia de base de datos de Kaspersky Security Center actual. El valor predeterminado es *.\KAV_CS_ADMIN_KIT*.

   - **Nombre de la base de datos**

     Nombre de la base de datos de Kaspersky Security Center SQL. El valor predeterminado es *KAV*.



Sección con información sobre la base de datos del Servidor de administración actual

4. Haga clic en el botón **Aceptar** para cerrar la ventana de propiedades del Servidor de administración.

Use el nombre de la base de datos para dirigirse a la base de datos en sus consultas SQL.

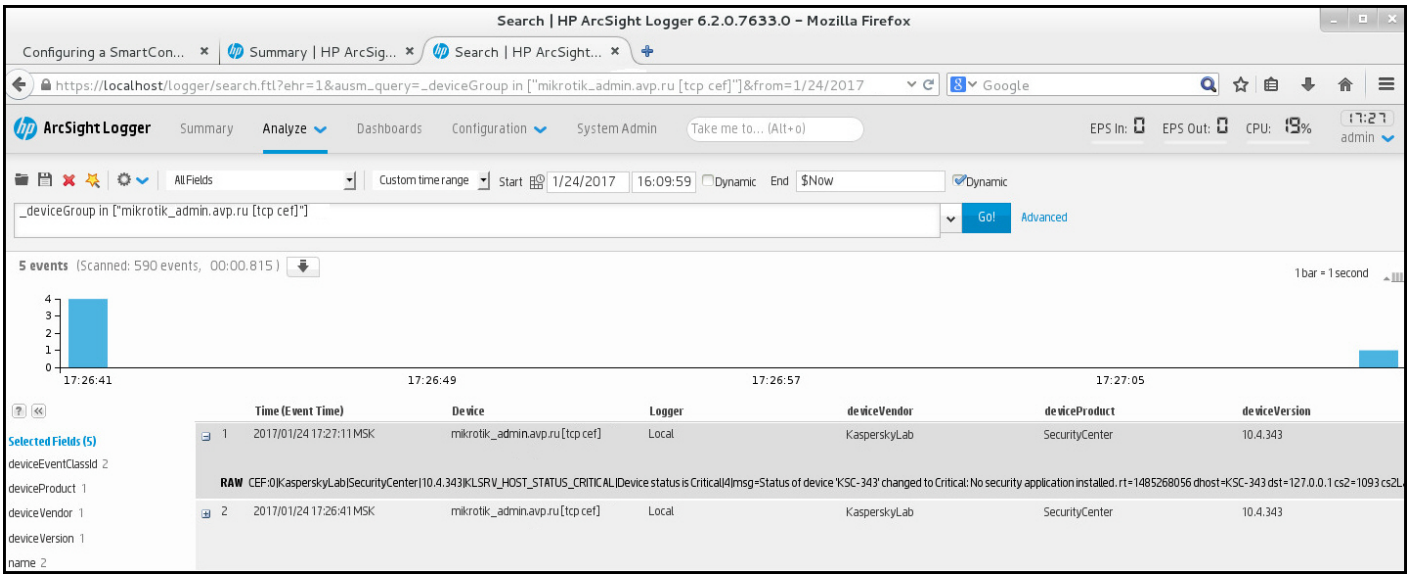
Visualización de resultados de exportación

Puede controlar la finalización correcta del procedimiento de exportación del evento. Para hacerlo, compruebe si los mensajes con eventos de exportación se reciben por su sistema SIEM.

Si los eventos enviados desde Kaspersky Security Center se reciben y analizan correctamente por su sistema SIEM, la configuración en ambos lados se realiza correctamente. De otra forma, compruebe la configuración que especificó en Kaspersky Security Center con respecto a la configuración en su sistema SIEM.

La figura a continuación muestra los eventos exportados a ArcSight. Por ejemplo, el primer evento es un evento crítico del Servidor de administración: "*El estado del dispositivo es crítico*".

La representación de eventos de exportación en el sistema SIEM varía según el sistema SIEM que use.



Ejemplo de eventos

Trabajo con Kaspersky Security Center 14 Web Console en un entorno de nube

Esta sección proporciona información sobre las características de Kaspersky Security Center 14 Web Console relacionadas con la implementación y el mantenimiento de Kaspersky Security Center en entornos de nube, como Amazon Web Services, Microsoft Azure o Google Cloud.

Para trabajar en un entorno de nube, necesita una licencia especial. Si no tiene dicha licencia, no se muestran los elementos de la interfaz relacionados con los dispositivos en la nube.

Asistente de configuración del entorno de nube de Kaspersky Security Center 14 Web Console

Para configurar Kaspersky Security Center usando este Asistente, debe tener lo siguiente:

- Credenciales para el entorno de nube:
  - Una función de IAM a la que se le ha otorgado el derecho de sondear el segmento de la nube o una cuenta de usuario de IAM a la que se le ha otorgado el derecho de sondear el segmento de la nube (para trabajar con Amazon Web Services)
  - Id. de la aplicación en Azure, contraseña y suscripción de Azure (para trabajar con Microsoft Azure)
  - Correo electrónico del cliente de Google, ID del proyecto y clave privada (para trabajar con Google Cloud)
- Complemento para Kaspersky Endpoint Security for Linux (complemento de Web Console)
- Complemento para Kaspersky Endpoint Security para Windows (complemento de Web Console)
- Agente de red para Windows
- Agente de red para Linux

- Paquete de instalación para Kaspersky Endpoint Security para Linux
- Paquete de instalación para Kaspersky Security for Windows Server

El Asistente de configuración del entorno de nube se inicia automáticamente en la primera conexión con el Servidor de administración a través de la Consola de administración si despliega Kaspersky Security Center desde una imagen lista para usar. También puede iniciar el Asistente de configuración del entorno de nube manualmente en cualquier momento.

Para iniciar el Asistente de configuración del entorno de nube manualmente,

En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → Asistente de configuración del entorno de nube**.

Se inicia el Asistente.

La sesión de trabajo promedio con este Asistente es aproximadamente 15 minutos.

Paso 1. Leer información sobre el Asistente

Lea sobre el Asistente de configuración del entorno de nube y haga clic en **Siguiente** para continuar.

Paso 2. Selección de la aplicación

Este paso solo se muestra si está utilizando un BYOL AMI y no ha activado la aplicación con una licencia de Kaspersky Security for Virtualization o una licencia de Kaspersky Hybrid Cloud Security.

Especifique la clave de licencia y haga clic en **Siguiente** para continuar.

La licencia se añade al almacenamiento del Servidor de administración.

Si vuelve a ejecutar el Asistente, este paso no se muestra.

Paso 3. Selección del entorno de nube

Esta sección describe las funciones que solo están disponibles en Kaspersky Security Center 12.1 o una versión posterior.

Especifique los siguientes parámetros:

- **Entorno de nube**

Seleccione el entorno de nube en el que está desplegando Kaspersky Security Center: AWS, Azure o Google Cloud.

Si planea trabajar con más de un entorno de nube, seleccione un entorno y luego ejecute el Asistente de nuevo.

- Nombre de la conexión

  Introduzca un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres de Unicode.

  Este nombre también se utilizará como el nombre del grupo de administración para los dispositivos de la nube.

  Si planea trabajar con más de un entorno de nube, es posible que desee incluir el nombre del entorno en el nombre de la conexión, por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google".

Ingrese sus credenciales para recibir autorización en el entorno de nube que especificó.

AWS

Si ha seleccionado AWS como el tipo de segmento de nube, necesita una función de IAM o una clave de acceso de AWS IAM para seguir sondeando el segmento de la nube.

- **Función de AWS IAM asignada a la instancia EC2**

  Seleccione esta opción si tiene una función de IAM con los derechos requeridos para el Servidor de administración.

- **Usuario de AWS IAM**

  Seleccione esta opción si tiene una clave de acceso de AWS IAM. Ingrese los datos de su clave:

  - Id. de la clave de acceso

    El Id. de clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Recibió el ID de clave cuando creó la cuenta de usuario de IAM.

    El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

  - Clave secreta

    La clave secreta que recibió con el Id. de clave de acceso cuando creó la cuenta de usuario de IAM.

    Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a introducir la clave secreta, aparecerá el botón **Mostrar**. Haga clic y mantenga pulsado este botón durante la cantidad de tiempo necesaria para ver los caracteres que introdujo.

    El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

    Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

Azure

Si ha seleccionado Azure, especifique la siguiente configuración para la conexión que se usará para el posterior sondeo del segmento de la nube:

- **Id. de la aplicación en Azure**

  Usted creó este Id. de la aplicación en el portal de Azure.

  Solo puede proporcionar un Id. de la aplicación en Azure para sondeos y otros fines. Si desea sondear otro segmento de Azure, primero debe eliminar la conexión de Azure existente.

- **Id. de suscripción de Azure**

  Usted creó la suscripción en el portal de Azure.

- **Contraseña de la aplicación Azure**

  Recibió la contraseña del Id. de la aplicación cuando creó el Id. de la aplicación.

  Los caracteres de la contraseña se muestran como asteriscos. Después de empezar a introducir la contraseña, el botón **Mostrar** estará disponible. Haga clic y mantenga presionado este botón para ver los caracteres que introdujo.

  Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

- **Nombre de la cuenta de almacenamiento de Azure**

  Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

- **Clave de acceso al almacenamiento de Azure**

  Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  La clave está disponible en la sección "Descripción general de la cuenta de almacenamiento de Azure", en la subsección "Claves".

  Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

Google Cloud

Si ha seleccionado Google Cloud como el tipo de segmento de nube, especifique la siguiente configuración para la conexión que se usará para el posterior sondeo del segmento de la nube:

- **Correo electrónico del cliente**

  El correo electrónico del cliente es el correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. del proyecto**

El id. del proyecto es el id. que recibió cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La clave privada es la secuencia de caracteres que recibió como clave privada cuando registró su proyecto en Google Cloud. Es posible que desee copiar y pegar esta secuencia para evitar errores.

  Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

La conexión que ha especificado se guarda en la configuración de la aplicación.

El Asistente de configuración del entorno de nube le permite especificar solo un segmento. Posteriormente, puede especificar más conexiones para administrar otros segmentos de la nube.

Haga clic en **Siguiente** para continuar.

Paso 4. Sondeo de segmentos, configuración de la sincronización con Cloud y elección de otras acciones

En este paso, se inicia al sondeo de segmentos de nube y se crea el grupo de administración especial para dispositivos de nube. Los dispositivos encontrados durante el sondeo se colocan en este grupo. El programa de sondeo de segmentos de nube está configurado (cada 5 minutos de forma predeterminada; puede cambiar esta configuración más adelante).

También se crea la regla de movimiento automática **Sincronizar con Cloud**. Para cada análisis posterior de la red en la nube, los dispositivos virtuales detectados se moverán al subgrupo correspondiente dentro del grupo **Dispositivos administrados\Cloud**.

Defina los siguientes parámetros:

- **Sincronizar grupos de administración con estructura de nube**

  Si esta opción está activada, el grupo **Cloud** se crea automáticamente en el grupo **Dispositivos administrados** y se inicia una detección de dispositivos de nube. Las instancias y máquinas virtuales detectadas durante cada análisis de la red de la nube se colocan en el grupo Cloud. La estructura de los subgrupos de administración dentro de este grupo coincide con la estructura de su segmento de la nube (en AWS, las zonas de disponibilidad y los grupos de ubicación no están representados en la estructura; en Azure, las subredes no están representadas en la estructura). Los dispositivos que no se han identificado como instancias en el entorno de nube están en el grupo **Dispositivos no asignados**. Esta estructura de grupo le permite usar tareas de instalación en grupo para instalar aplicaciones antivirus en instancias, así como configurar diferentes directivas para diferentes grupos.

  Si esta opción está desactivada, también se crea el grupo de la **nube** y también se inicia la detección de dispositivos de la nube; sin embargo, los subgrupos que coinciden con la estructura del segmento de la nube no se crean dentro del grupo. Todas las instancias detectadas están en el grupo de administración **Cloud**, por lo que se muestran en una lista sola. Si su trabajo con Kaspersky Security Center requiere sincronización, puede modificar las propiedades de la regla **Sincronizar con Cloud** y aplicarla. Aplicar esta regla cambia la estructura de los subgrupos en el grupo Cloud de modo que coincida con la estructura de su segmento de la nube.

  Esta opción está desactivada de forma predeterminada.

- Desplegar protección

  Si se selecciona esta opción, el Asistente crea una tarea para instalar las aplicaciones de seguridad en instancias. Una vez que finalice el Asistente, el Asistente de despliegue de la protección automáticamente comienza en dispositivos en sus segmentos de la nube, y usted podrá instalar el Agente de red y las aplicaciones de seguridad en esos dispositivos.

  Kaspersky Security Center puede realizar el despliegue con sus herramientas nativas. Si no tiene permisos para instalar las aplicaciones en instancias EC2 o máquinas virtuales Azure, puede configurar la tarea de Instalación remota manualmente y especificar una cuenta con los permisos requeridos. En este caso, la tarea de instalación remota no funcionará para los dispositivos detectados utilizando la API de AWS o Azure. Esta tarea solo funciona para los dispositivos descubiertos mediante el sondeo de Active Directory, el sondeo de dominios de Windows o el sondeo de rango de IP.

  Si esta opción no está seleccionada, el Asistente de despliegue de la protección no se inicia y no se crean tareas para instalar aplicaciones de seguridad en las instancias. Puede realizar manualmente ambas acciones más adelante.

Si selecciona la opción Desplegar protección, se torna disponible la sección **Reiniciando dispositivos**. En esta sección, puede elegir qué hacer cuando se deba reiniciar el sistema operativo de un dispositivo de destino. Seleccione si reiniciar instancias si el sistema operativo de su dispositivo debe reiniciarse durante la instalación de aplicaciones:

- No reiniciar

  Si se selecciona esta opción, el dispositivo no se reiniciará después de la instalación de la aplicación de seguridad.

- Reiniciar

  Si se selecciona esta opción, el dispositivo se reiniciará después de la instalación de la aplicación de seguridad.

Haga clic en **Siguiente** para continuar.

Para Google Cloud, solo puede realizar el despliegue con las herramientas nativas de Kaspersky Security Center. Si seleccionó Google Cloud, la opción **Desplegar protección** no está disponible.

Paso 5. Configuración de Kaspersky Security Network para Kaspersky Security Center

Especifique la configuración para transmitir la información sobre las operaciones de Kaspersky Security Center (KSN) a la base de conocimientos de Kaspersky Security Network. Seleccione una de las siguientes opciones:

- Acepto usar Kaspersky Security Network

Kaspersky Security Center y las aplicaciones administradas instaladas en dispositivos cliente transferirán automáticamente su información de operación a Kaspersky Security Network. La participación en Kaspersky Security Network garantiza actualizaciones más rápidas de bases de datos que contienen información sobre virus y otras amenazas, y asegura una respuesta más rápida ante amenazas de seguridad emergentes.

- **No acepto usar Kaspersky Security Network**

  Kaspersky Security Center y las aplicaciones administradas no proporcionarán información a Kaspersky Security Network.

  Si selecciona esta opción, se desactivará el uso de Kaspersky Security Network.

Kaspersky recomienda la participación en Kaspersky Security Network.

También se pueden mostrar los contratos de KSN para las aplicaciones administradas. Si acepta usar Kaspersky Security Network, la aplicación administrada enviará datos a Kaspersky. Si no acepta participar en Kaspersky Security Network, la aplicación administrada no enviará datos a Kaspersky. (Puede cambiar esta configuración más adelante en la directiva de la aplicación).

Haga clic en **Siguiente** para continuar.

Paso 6. Creación de una configuración inicial de protección

Puede consultar la lista de directivas y tareas que se crean.

Espere a que se complete la creación de directivas y tareas y luego haga clic en **Siguiente** para continuar. En la última página del Asistente, haga clic en el botón **Finalizar** para salir.

Sondeo de segmentos de red a través de Kaspersky Security Center 14 Web Console

El Servidor de administración recibe información sobre la estructura de la red (y los dispositivos que contiene) mediante sondeos regulares de los segmento de la nube utilizando instrumentos API de AWS, API de Azure o API de Google. Kaspersky Security Center usa esta información para actualizar los contenido de los dispositivos no asignados y las carpetas Dispositivos administrados. Si configuró dispositivos para que se trasladen de forma automática a grupos de administración, los dispositivos detectados se incluirán en los grupos de administración.

Para permitir que un Servidor de administración sondee segmentos de la nube, debe tener los derechos correspondientes, que se proveen junto con una función de IAM o una cuenta de usuario de IAM (en AWS) o con un id. de la aplicación y contraseña (en Azure), o con un correo electrónico de cliente de Google un ID de proyecto de Google y una clave privada.

Puede añadir y eliminar conexiones, así como configurar la planificación del sondeo de cada segmento de la nube.

Añadir conexiones para sondear segmentos de la nube

Para añadir una conexión para el sondeo de segmentos de la nube a la lista de conexiones disponibles:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → CLOUD**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en **Añadir**.

   Se abre la ventana **Configuración de segmentos de la nube**.
4. Especifique el nombre del entorno de nube para la conexión que se utilizará para seguir sondeando el segmento de la nube:

   - **Entorno de nube**

     Seleccione el entorno de nube en el que está desplegando Kaspersky Security Center: AWS, Azure o Google Cloud.

     Si planea trabajar con más de un entorno de nube, seleccione un entorno y luego ejecute el Asistente de nuevo.

   - **Nombre de la conexión**

     Introduzca un nombre para la conexión. El nombre no puede contener más de 256 caracteres. Solo se permiten caracteres de Unicode.

     Este nombre también se utilizará como el nombre del grupo de administración para los dispositivos de la nube.

     Si planea trabajar con más de un entorno de nube, es posible que desee incluir el nombre del entorno en el nombre de la conexión, por ejemplo, "Segmento de Azure", "Segmento de AWS" o "Segmento de Google".
5. Ingrese sus credenciales para recibir autorización en el entorno de nube que especificó.

   - Si ha seleccionado AWS, especifique la siguiente configuración:

     - **Usar la función de AWS IAM**

       Seleccione esta opción si ya ha creado una función de IAM para que el Servidor de administración use los servicios de AWS.

     - **Credenciales de la cuenta de usuario de AWS IAM**

       Seleccione esta opción si tiene una cuenta de usuario de IAM con los permisos necesarios y puede introducir una ID de clave y una clave secreta.

       Si especificó que tiene una Credenciales de la cuenta de usuario de AWS IAM, especifique lo siguiente:

       - **Id. de clave de acceso**

         El Id. de clave de acceso de IAM es una secuencia de caracteres alfanuméricos. Recibió el ID de clave cuando creó la cuenta de usuario de IAM.

         El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

- **Clave secreta**

  La clave secreta que recibió con el Id. de clave de acceso cuando creó la cuenta de usuario de IAM.

  Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a introducir la clave secreta, aparecerá el botón **Mostrar**. Haga clic y mantenga pulsado este botón durante la cantidad de tiempo necesaria para ver los caracteres que introdujo.

  El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

- Si ha seleccionado Azure, especifique la siguiente configuración:

  - **Id. de la aplicación en Azure**

    Usted creó este Id. de la aplicación en el portal de Azure.

    Solo puede proporcionar un Id. de la aplicación en Azure para sondeos y otros fines. Si desea sondear otro segmento de Azure, primero debe eliminar la conexión de Azure existente.

  - **Id. de suscripción de Azure**

    Usted creó la suscripción en el portal de Azure.

  - **Contraseña de la aplicación Azure**

    Recibió la contraseña del Id. de la aplicación cuando creó el Id. de la aplicación.

    Los caracteres de la contraseña se muestran como asteriscos. Después de empezar a introducir la contraseña, el botón **Mostrar** estará disponible. Haga clic y mantenga presionado este botón para ver los caracteres que introdujo.

    Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

  - **Nombre de la cuenta de almacenamiento de Azure**

    Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

  - **Clave de acceso al almacenamiento de Azure**

    Recibió una contraseña (clave) cuando creó la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

    La clave está disponible en la sección "Descripción general de la cuenta de almacenamiento de Azure", en la subsección "Claves".

    Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

Si ha seleccionado Google Cloud, especifique la siguiente configuración:

- **Correo electrónico del cliente**

  El correo electrónico del cliente es el correo electrónico que utilizó para registrar su proyecto en Google Cloud.

- **Id. del proyecto**

  El id. del proyecto es el id. que recibió cuando registró su proyecto en Google Cloud.

- **Clave privada**

  La clave privada es la secuencia de caracteres que recibió como clave privada cuando registró su proyecto en Google Cloud. Es posible que desee copiar y pegar esta secuencia para evitar errores.

  Para ver los caracteres que ha ingresado, haga clic y mantenga presionado el botón **Mostrar**.

6. Si quiere, haga clic en **Programar sondeo** y cambie la configuración predeterminada.

La conexión se guarda en la configuración de la aplicación.

Después de sondear por primera vez un nuevo segmento de la nube, aparece un subgrupo correspondiente a ese segmento en el grupo de administración **Dispositivos administrados\Cloud**.

Si especifica credenciales incorrectas, no se encontrarán instancias durante el sondeo del segmento de la nube y no aparecerá un nuevo subgrupo en el grupo de administración **Dispositivos administrados\Cloud**.

Eliminar una conexión para sondear segmentos de la nube

Si ya no tiene que sondear un segmento específico de la nube, puede eliminar la conexión correspondiente en la lista de conexiones disponibles. También puede eliminar una conexión si, por ejemplo, los permisos para sondear un segmento de la nube se han transferido a otro usuario que tiene diferentes credenciales.

Para eliminar una conexión:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → CLOUD**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en el nombre del segmento que desea eliminar.
4. Haga clic en **Eliminar**.
5. En la ventana que se abre, haga clic en el botón **Aceptar** para confirmar su selección.

La conexión se elimina. Los dispositivos en el segmento de la nube que correspondan a esta conexión se eliminan automáticamente de los grupos de administración.

Configuración de la programación de sondeo a través de Kaspersky Security Center 14 Web Console

El sondeo de segmentos de la nube se realiza según programación. Puede configurar la frecuencia del sondeo.

La frecuencia del sondeo está automáticamente configurada en 5 minutos por el Asistente de configuración del entorno de nube Puede cambiar este valor en cualquier momento y configurar otra planificación. Sin embargo, no se recomienda configurar el sondeo para que se ejecute con una frecuencia mayor a cada 5 minutos, porque esto podría dar lugar a errores en el funcionamiento de la API.

Para configurar una planificación de sondeo de segmentos de la nube:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → CLOUD**.
2. En la ventana que se abre, haga clic en **Propiedades**.
3. En la ventana **Configuración** que se abre, haga clic en el nombre del segmento cuya programación de sondeo desea configurar.

   De este modo, se abre la ventana **Configuración de segmentos de la nube**.
4. En la ventana **Configuración de segmentos de la nube**, haga clic en el botón **Programar sondeo**.

   De este modo, se abre la ventana **Programación**.
5. En la ventana **Programación**, defina los siguientes ajustes:

   - **Inicio programado**

     Opciones de planificación de sondeo:

     - Cada N días

       El sondeo se ejecuta regularmente, con el intervalo especificado en días, a partir de la fecha y la hora especificadas.

       De forma predeterminada, el sondeo se ejecuta cada día, a partir de la fecha y la hora actuales del sistema.

     - Cada N minutos

       El sondeo se ejecuta regularmente, con el intervalo especificado en minutos, a partir de la fecha y la hora especificadas.

       De forma predeterminada, el sondeo se ejecuta cada cinco minutos, a partir de la hora actual del sistema.

     - Por días de la semana

       El sondeo se ejecuta regularmente, en los días especificados de la semana y en el momento especificado.

       De forma predeterminada, el sondeo se realiza todos los viernes a las 6:00:00 p.m.

- **Cada mes, en días concretos de las semanas seleccionadas**

  El sondeo se realiza regularmente, en los días especificados de cada mes y en el momento especificado.

  De forma predeterminada, no se seleccionan días del mes; la hora de inicio predeterminada es las 6:00:00 p.m.

- **Intervalo de inicio (min)**

  Especifique a qué equivale N (minutos o días).

- **Inicio desde**

  Especifique cuándo comenzar el primer sondeo.

- **Ejecutar tareas no realizadas**

  Si el Servidor de administración está apagado o no está disponible durante la hora programada para el sondeo, el Servidor de administración puede iniciar el sondeo inmediatamente después de que se encienda o esperar a la próxima vez que se programe el sondeo.

  Si esta opción está activada, el Servidor de administración inicia el sondeo inmediatamente después de que se encienda.

  Si esta opción está desactivada, el Servidor de administración espera a la próxima vez que se programe el sondeo.

  Esta opción está activada de forma predeterminada.

6. Haga clic en **Guardar** para guardar los cambios.

El horario de sondeo del segmento queda configurado y guardado.

Ver los resultados del sondeo del segmento de la nube a través de Kaspersky Security Center 14 Web Console

Puede ver los resultados del sondeo del segmento de la nube, es decir, ver la lista de dispositivos en la nube administrados por el Servidor de administración.

Para ver los resultados del sondeo del segmento de la nube:

En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DETECCIÓN → CLOUD**.

Esto muestra los segmentos de nube disponibles para el sondeo.

Ver las propiedades de dispositivos de la nube a través de Kaspersky Security Center 14 Web Console

Puede ver las propiedades de cada dispositivo de la nube.

Para ver las propiedades de un dispositivo de la nube, siga estos pasos:

1. En el menú principal, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.
2. Haga clic en el nombre del dispositivo cuyas propiedades desea ver.

   Se abrirá una ventana de propiedades con la sección **Control de aplicaciones** seleccionada.
3. Si desea ver las propiedades específicas de los dispositivos de la nube, seleccione la sección **Sistema** en la ventana de propiedades.

   Las propiedades se muestran según la plataforma en la nube del dispositivo.

   Para los dispositivos en AWS, se muestran las siguientes propiedades:

   - **Dispositivo detectado usando API** (valor: **AWS**)
   - **Región de la nube**
   - **VPC en la nube**
   - **Zona de disponibilidad en la nube**
   - **Subred de nube**
   - **Grupo de ubicación en la nube** (esta unidad solo se muestra si la instancia pertenece a un grupo de ubicación; de lo contrario, no se muestra)

   Para los dispositivos en Azure, se muestran las siguientes propiedades:

   - **Dispositivo detectado usando API** (valor: **Microsoft Azure**)
   - **Región de la nube**
   - **Subred de nube**

   Para los dispositivos en Google Cloud, se muestran las siguientes propiedades:

   - **Dispositivo detectado usando API** (valor: **Google Cloud**)
   - **Región de la nube**
   - **VPC en la nube**
   - **Zona de disponibilidad en la nube**
   - **Subred de nube**

Sincronización con la nube: configuración de la regla móvil

Durante el funcionamiento del Asistente de configuración del entorno de nube, Sincronizar con Cloud se crea automáticamente. Esta regla le permite mover automáticamente las instancias detectadas en cada sondeo, desde el grupo Dispositivos no asignados al grupo Dispositivos administrados\Cloud para hacer que estos dispositivos queden disponibles para la administración centralizada. De forma predeterminada, la regla está activa tras crearse. Puede desactivar, modificar o aplicar la regla en cualquier momento.

Para modificar las propiedades de la regla Sincronizar con Cloud y / o aplicar la regla:

1. En el menú principal, vaya a **DETECCIÓN Y DESPLIEGUE → DESPLIEGUE Y ASIGNACIÓN → REGLAS DE MOVIMIENTO**.

   Esto abre una lista de reglas de movimiento.

2. En la lista de reglas de movimiento, seleccione **Sincronizar con subgrupo de la nube**.

   Esto abre la ventana de propiedades de la regla.

3. Si es necesario, especifique los siguientes ajustes en la pestaña **Condiciones de reglas** tab, in the **Segmentos de la nube**:

   - **El dispositivo está en un segmento de la nube**

     La regla solo se aplica a los dispositivos que se encuentran en el segmento de la nube seleccionado. De lo contrario, la regla se aplica a todos los dispositivos que han sido detectados.

     Esta opción está seleccionada de forma predeterminada.

   - **Incluir objetos secundarios**

     La regla se aplica a todos los dispositivos en el segmento seleccionado y a todas las subsecciones de la nube anidadas. De lo contrario, la regla solo se aplicará a los dispositivos que estén en el segmento raíz.

     Esta opción está seleccionada de forma predeterminada.

   - **Mover dispositivos desde objetos anidados a subgrupos correspondientes**

     Si esta opción está activada, los dispositivos se mueven automáticamente a los subgrupos que corresponden a su estructura.

     Si esta opción está desactivada, los dispositivos de los objetos anidados se mueven automáticamente a la raíz del subgrupo de la nube sin ninguna otra ramificación.

     Esta opción está activada de forma predeterminada.

   - **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente**

     Si esta opción está activada, cuando la estructura del grupo **Dispositivos administrados\Cloud** no tiene subgrupos que coincidan con la sección que contiene el dispositivo, Kaspersky Security Center crea tales subgrupos. Por ejemplo, si se descubre una nueva subred durante la detección de dispositivos, se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Grupo nube**.

     Si esta opción está desactivada, Kaspersky Security Center no crea ningún subgrupo nuevo. Por ejemplo, si se descubre una nueva subred durante el sondeo de la red, no se creará un nuevo grupo con el mismo nombre en el grupo **Dispositivos administrados\Cloud**, y los dispositivos que se encuentran en esa subred se moverán al grupo **Dispositivos administrados\Cloud**.

     Esta opción está activada de forma predeterminada.

- Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube

  Si esta opción está activada, la aplicación elimina del grupo de la nube todos los subgrupos que no coinciden con ningún objeto de nube existente.

  Si esta opción está desactivada, se conservan los subgrupos que no coinciden con ninguno de los objetos de nube existentes.

  Esta opción está activada de forma predeterminada.

Si habilitó la opción **Sincronizar grupos de administración con estructura de nube** al usar el Asistente de configuración del entorno de nube, la regla **Sincronizar con subgrupo de la nube** se crea con las opciones **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente** y **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube** activadas.

Si no habilitó la opción **Sincronizar grupos de administración con estructura de nube**, la regla **Sincronizar con subgrupo de la nube** se crea con estas opciones deshabilitadas (desactivadas). Si su trabajo con Kaspersky Security Center requiere que la estructura de los subgrupos en el subgrupo **Dispositivos administrados** \ **Cloud** coincida con la estructura de los segmentos de la nube, active las opciones **Crear subgrupos correspondientes a contenedores de dispositivos detectados recientemente** y **Eliminar subgrupos para los que no se encontró coincidencia en los segmentos de la nube** en las propiedades de la regla y luego haga cumplir la regla.

4. En la lista desplegable **Dispositivo descubierto mediante la API**, seleccione uno de los siguientes valores:

   - **error - código**. El dispositivo no se puede detectar con AWS, Azure o Google API, es decir, o bien está fuera del entorno de nube, o está en el entorno de nube pero no se puede detectar mediante API por algún motivo.
   - **AWS**. El dispositivo se descubre mediante la API de AWS, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de AWS.
   - **Azure**. El dispositivo se descubre mediante la Azure API, es decir, el dispositivo definitivamente se encuentra en el entorno de nube de Azure.
   - **Google Cloud**. El dispositivo se descubre mediante la API de Google, es decir, el dispositivo se encuentra definitivamente en el entorno de nube de Google.
   - Ningún valor. Este criterio no se puede aplicar.

5. Si es necesario, configure otras propiedades de reglas en otras secciones.

La regla de movimiento queda configurada.

Creación de una copia de seguridad de la tarea de datos del Servidor de administración utilizando un DBMS en la nube

Las tareas de Copias de seguridad son tareas del Servidor de administración. Puede crear una tarea de Copia de seguridad si desea usar un DBMS ubicado en un entorno de nube (AWS o Azure).

Para crear una tarea de creación de copias de seguridad de los datos del Servidor de administración:

1. En el menú principal, vaya a **DISPOSITIVOS** → **TAREAS**.
2. Haga clic en **Añadir**.

Se inicia el Asistente para añadir tareas.

3. En la primera página del Asistente, en la lista **Aplicación**, seleccione **Proveedor**, y en la lista **Tipo de tarea**, seleccione **Copia de seguridad de los datos del Servidor de administración**.

4. En la página correspondiente del Asistente, especifique la siguiente configuración:

   - Si está trabajando con una base de datos en AWS:

     - **Nombre del bucket S3**

       El nombre del bucket S3 que creó para la copia de seguridad.

     - **Id. de clave de acceso**

       Recibió el Id. de clave (secuencia de caracteres alfanuméricos) cuando creó la cuenta de usuario de IAM para trabajar con la instancia de almacenamiento de bucket S3.

       El campo está disponible Si ha seleccionado la base de datos de RDS en un bucket S3.

     - **Clave secreta**

       La clave secreta que recibió con el Id. de clave de acceso cuando creó la cuenta de usuario de IAM.

       Los caracteres de la clave secreta se muestran como asteriscos. Cuando comience a introducir la clave secreta, aparecerá el botón **Mostrar**. Haga clic y mantenga pulsado este botón durante la cantidad de tiempo necesaria para ver los caracteres que introdujo.

       El campo está disponible Si ha seleccionado una clave de acceso de AWS IAM para la autorización en lugar de una función de IAM.

   - Si está trabajando con una base de datos en Microsoft Azure:

     - **Nombre de la cuenta de almacenamiento de Azure**

       Creó el nombre de la cuenta de almacenamiento de Azure para trabajar con Kaspersky Security Center.

     - **Id. de suscripción de Azure**

       Usted creó la suscripción en el portal de Azure.

     - **Contraseña de Azure**

       Recibió la contraseña del Id. de la aplicación cuando creó el Id. de la aplicación.

       Los caracteres de la contraseña se muestran como asteriscos. Después de empezar a introducir la contraseña, el botón **Mostrar** estará disponible. Haga clic y mantenga presionado este botón para ver los caracteres que introdujo.

     - **Id. de la aplicación en Azure**

Usted creó este Id. de la aplicación en el portal de Azure.

Solo puede proporcionar un Id. de la aplicación en Azure para sondeos y otros fines. Si desea sondear otro segmento de Azure, primero debe eliminar la conexión de Azure existente.

- **Nombre del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en sus propiedades de Azure SQL Server.

- **Grupo de recursos del servidor SQL de Azure**

  El nombre y el grupo de recursos están disponibles en sus propiedades de Azure SQL Server.

- **Clave de acceso al almacenamiento de Azure**

  Disponible en las propiedades de su cuenta de almacenamiento, en la sección Claves de acceso. Puede utilizar cualquiera de las claves (clave1 o clave2).

La tarea se crea y se muestra en la lista de tareas. Si habilita la opción **Abrir los detalles de la tarea cuando se complete la creación**, puede modificar la configuración predeterminada de la tarea inmediatamente después de crearla. Si no activa esta opción, la tarea se creará con las configuraciones predeterminadas. Puede modificar la configuración predeterminada más tarde, en cualquier momento.

Diagnóstico remoto de los dispositivos cliente

Puede utilizar diagnósticos remotos para la ejecución remota de las siguientes operaciones en dispositivos cliente:

- Activación y desactivación del seguimiento, modificación del nivel de seguimiento y descarga del archivo de seguimiento
- Descarga de información del sistema y configuración de la aplicación
- Descarga de los registros de eventos
- Generación de un archivo de volcado para una aplicación
- Inicio del diagnóstico y descarga de los informes del diagnóstico
- Inicio, detención y reinicio de aplicaciones

Puede usar los registros de eventos e informes de diagnóstico descargados de un dispositivo cliente para solucionar problemas por su cuenta. Además, si se pone en contacto con un especialista del Servicio de soporte técnico de Kaspersky, éste puede pedirle que descargue archivos de seguimiento, archivos de volcado, registros de eventos e informes de diagnóstico desde un dispositivo cliente para un análisis más profundo en Kaspersky.

El diagnóstico remoto se realiza utilizando el Servidor de administración.

Abrir la ventana de diagnóstico remoto

Para realizar el diagnóstico remoto de un dispositivo cliente, debe abrir la ventana de diagnóstico remoto.

Para abrir la ventana de diagnóstico remoto:

1. Para seleccionar el dispositivo para el que desea abrir la ventana de diagnóstico remoto, realice una de las siguientes acciones:
   - Si el dispositivo pertenece a un grupo de administración, vaya a **DISPOSITIVOS** → **DISPOSITIVOS ADMINISTRADOS**.
   - Si el dispositivo pertenece al grupo Dispositivos no asignados, vaya a **DETECCIÓN Y DESPLIEGUE** → **DISPOSITIVOS NO ASIGNADOS**.
2. Haga clic en el nombre del dispositivo requerido.
3. En la ventana de propiedades del dispositivo que se abre, seleccione la pestaña **Avanzado**.
4. En la ventana que se abre, haga clic en **Diagnósticos remotos**.
   Esto abre la ventana **Diagnósticos remotos** del dispositivo cliente.

Habilitar y deshabilitar el seguimiento para aplicaciones

Puede habilitar y deshabilitar el seguimiento de aplicaciones, incluido el seguimiento de Xperf.

Habilitación y deshabilitación del seguimiento

Para activar o desactivar el seguimiento en un dispositivo remoto:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnósticos remotos haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, seleccione la sección **Aplicaciones de Kaspersky**.
   Esto abre la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
4. En la lista de aplicaciones, seleccione la aplicación para la que desea desactivar el seguimiento.
   Se muestra la lista de opciones de diagnósticos remotos.
5. Si desea activar el seguimiento:
   a. En la sección **Rastreo** de la lista, haga clic en **Activar rastreo**.
   b. En la ventana **Modificar nivel de seguimiento** que se abre, le recomendamos que mantenga los valores predeterminados de la configuración. Cuando sea necesario, un especialista del Servicio de soporte técnico lo guiará a través del proceso de configuración. Están disponibles los siguientes ajustes:
      - Nivel de seguimiento

El nivel de seguimiento define la cantidad de datos que contiene el archivo de seguimiento.

- Rastreo basado en rotación

  La aplicación sobrescribe la información de rastreo para evitar un aumento excesivo en el tamaño del archivo de seguimiento. Especifique la cantidad máximo de archivos que se utilizarán para almacenar la información de seguimiento y el tamaño máximo de cada archivo. Si se escribe el número máximo de archivos de seguimiento de tamaño máximo, el archivo de seguimiento más antiguo se eliminará para que se pueda escribir un nuevo archivo de seguimiento.

  Este ajuste está disponible solo en Kaspersky Endpoint Security.

c. Haga clic en **Guardar**.

El seguimiento queda activado para la aplicación seleccionada. En algunos casos la aplicación de seguridad y su tarea se deberán reiniciar para activar el seguimiento.

6. Si desea deshabilitar el seguimiento de la aplicación seleccionada, haga clic en **Desactivar rastreo**.

   El seguimiento queda desactivado para la aplicación seleccionada.

Activar el seguimiento de Xperf

Para Kaspersky Endpoint Security, un especialista del Servicio de soporte técnico puede solicitarle que habilite el seguimiento de Xperf para obtener información sobre el rendimiento del sistema.

Para habilitar y configurar el seguimiento de Xperf:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnósticos remotos haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, seleccione la sección **Aplicaciones de Kaspersky**.

   Esto abre la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
4. En la lista de aplicaciones, seleccione Kaspersky Endpoint Security para Windows.

   Se muestra la lista de opciones de diagnóstico remoto para Kaspersky Endpoint Security para Windows.
5. En la sección **Rastreo de Xperf** de la lista, haga clic en **Activar el seguimiento de Xperf**.

   Si el rastreo de Xperf ya está activado, se muestra el botón **Desactivar rastreo de Xperf** en su lugar.
6. En la ventana **Cambiar nivel de seguimiento de Xperf** que se abre, según lo que pida el especialista del Servicio de soporte técnico, siga las siguientes instrucciones:

   a. Seleccione uno de los siguientes niveles de seguimiento:

   - Nivel ligero

     Un archivo de seguimiento de este tipo contiene la cantidad mínima de información sobre el sistema.

     Esta opción está seleccionada de forma predeterminada.

   - Nivel profundo

Un archivo de seguimiento de este tipo contiene información más detallada que los archivos de seguimiento del tipo *Ligero* y puede ser solicitado por especialistas del Servicio de soporte técnico cuando un archivo de seguimiento del tipo *Ligero* no es suficiente para la evaluación del rendimiento. Un archivo de seguimiento *Profundo* contiene información técnica sobre el sistema, incluida información sobre hardware, sistema operativo, lista de procesos y aplicaciones iniciadas y terminadas, eventos utilizados para la evaluación del rendimiento y eventos de la Herramienta de evaluación del sistema de Windows.

b. Seleccione uno de los siguientes tipos de seguimientos de Xperf:

- **Tipo básico**

  La información de seguimiento se recibe durante el funcionamiento de la aplicación Kaspersky Endpoint Security.

  Esta opción está seleccionada de forma predeterminada.

- **Tipo de reinicio**

  La información de seguimiento se recibe cuando el sistema operativo se inicia en el dispositivo administrado. Este tipo de seguimiento es efectivo cuando el problema que afecta al rendimiento del sistema ocurre después de que se encienda el dispositivo y antes de que se inicie Kaspersky Endpoint Security.

También se le puede solicitar que habilite la opción de **Tamaño de archivos de rotación, en MB** para evitar un aumento excesivo en el tamaño del archivo de seguimiento. Después, especifique el tamaño máximo del archivo de seguimiento. Cuando el archivo alcanza el tamaño máximo, la información de seguimiento más antigua se sobrescribe con la información nueva.

c. Defina el tamaño del archivo de rotación.

d. Haga clic en **Guardar**.

El seguimiento de Xperf queda activado y configurado.

Para desactivar el seguimiento de Xperf:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnósticos remotos haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, seleccione la sección **Aplicaciones de Kaspersky**.

   Esto abre la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
4. En la lista de aplicaciones, seleccione Kaspersky Endpoint Security para Windows.

   Se muestran las opciones de seguimiento para Kaspersky Endpoint Security para Windows.
5. En la sección **Rastreo de Xperf** de la lista, haga clic en **Desactivar rastreo de Xperf**.

   Si el seguimiento de Xperf ya está desactivado, se muestra el botón **Activar rastreo de Xperf** en su lugar.

El seguimiento de Xperf queda desactivado.

Descargar un archivo de seguimiento de una aplicación:

Para descargar un archivo de seguimiento de una aplicación:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnósticos remotos haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, seleccione la sección **Aplicaciones de Kaspersky**.

   Esto abre la lista de aplicaciones de Kaspersky instaladas en el dispositivo.

   En la sección **Rastreo**, haga clic en el botón **Archivos de seguimiento**.

   Se abre la ventana **Registros de rastreo del dispositivo**, donde se muestra una lista de archivos de seguimiento.
4. En la lista de archivos de seguimiento, seleccione la subred que desee.
5. Realice una de las siguientes acciones:

   - Descargue el archivo seleccionado haciendo clic en el **Descargar archivo completo**.
   - Descargue una parte del archivo seleccionado:

     a. Haga clic en **Descargar una parte**.

     b. En la ventana que se abre, especifique el nombre y la parte del archivo que desea descargar, según sus necesidades.

     c. Haga clic en **Descargar**.

El archivo seleccionado, o su parte, se descarga en la ubicación que especifique.

Eliminar archivos de seguimiento

Puede eliminar archivos de seguimiento que ya no sean necesarios.

Para eliminar un archivo de seguimiento:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto que se abre, haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, asegúrese de que esté seleccionada la sección **Registros del sistema operativo**.
4. En la sección **Archivos de seguimiento**, haga clic en el botón **Registros de Windows Update** o en el botón **Registros de instalación remota**, según los archivos de seguimiento que desee eliminar.

   Esto abre la lista de archivos de seguimiento.
5. En la lista de archivos de seguimiento, seleccione el archivo que desea eliminar.

6. Haga clic en el botón **Eliminar**.

El archivo de seguimiento seleccionado se elimina.

Descarga de la configuración de las aplicaciones.

Para descargar la configuración de las aplicaciones desde un dispositivo cliente:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto que se abre, haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, asegúrese de que **Registros del sistema operativo** esté seleccionado en el panel derecho.
   - En la sección **Información del sistema**, haga clic en el botón **Descargar archivo** para descargar la información del sistema del dispositivo cliente.
   - En la sección **Configuración de la aplicación**, haga clic en **Descargar archivo** para descargar la información sobre la configuración de las aplicaciones instaladas en el dispositivo.

La información se descarga, en forma de archivo, en la ubicación que especifique.

Descarga de los registros de eventos

Para descargar un registro de eventos desde un dispositivo remoto:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnósticos remotos haga clic en **Registros de dispositivo**.
3. En la ventana **Todos los registros del dispositivo**, especifique el registro correspondiente.
4. Realice una de las siguientes acciones:
   - Haga clic en **Descargar archivo completo** para descargar el registro de eventos seleccionado.
   - Descargue una parte del registro seleccionado:
     a. Haga clic en **Descargar una parte**.
     b. En la ventana que se abre, especifique el nombre y la parte del archivo que desea descargar, según sus necesidades.
     c. Haga clic en **Descargar**.

El registro de eventos seleccionado, o su parte, se descarga en la ubicación que especifique.

Inicio, detención y reinicio de la aplicación.

Puede iniciar, detener y reiniciar aplicaciones en un dispositivo cliente.

Para iniciar, detener o reiniciar una aplicación:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnósticos remotos haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, seleccione la sección **Aplicaciones de Kaspersky**.

   Esto abre la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
4. En la lista de aplicaciones, seleccione la aplicación que desea iniciar, detener o reiniciar.
5. Seleccione una acción al hacer clic en uno de los siguientes botones:

   - **Detener aplicación**

     Este botón solo está disponible si la aplicación se está ejecutando.
   - **Reiniciar aplicación**

     Este botón solo está disponible si la aplicación se está ejecutando.
   - **Iniciar aplicación**

     Este botón está disponible solo si la aplicación no se está ejecutando.

Dependiendo de la acción seleccionada, la aplicación se iniciará, detendrá o reiniciará en el dispositivo cliente.

Si reinicia el Agente de red, se muestra un mensaje que indica que se perderá la conexión actual del dispositivo al Servidor de administración.

Ejecutar el diagnóstico remoto de una aplicación y descargar los resultados

Para iniciar el diagnóstico de una aplicación en un dispositivo remoto y descargar sus resultados:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnósticos remotos haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, seleccione la sección **Aplicaciones de Kaspersky**.

   Esto abre la lista de aplicaciones de Kaspersky instaladas en el dispositivo.
4. En la lista de aplicaciones, seleccione la aplicación para la que desea ejecutar diagnósticos remotos.

   Se muestra la lista de opciones de diagnósticos remotos.
5. En la sección **Informe de diagnóstico** de la lista, haga clic en el botón **Ejecutar diagnósticos**.

   Esto inicia el proceso de diagnóstico remoto y genera un informe de diagnóstico. Cuando se completa el proceso de diagnóstico, el botón **Descargar un informe de diagnóstico** se habilita.
6. Descargue el informe haciendo clic en el botón **Descargar un informe de diagnóstico**.

El informe se descarga en la ubicación que ha especificado.

Ejecutar una aplicación en un dispositivo cliente

Es posible que tenga que ejecutar una aplicación en el dispositivo cliente, si un especialista de soporte de Kaspersky se lo solicita.

No tiene que instalar la aplicación en ese dispositivo.

Para instalar una aplicación en el dispositivo cliente:

1. Abra la ventana de diagnóstico remoto de un dispositivo cliente.
2. En la ventana de diagnóstico remoto que se abre, haga clic en **Diagnósticos remotos**.
3. En la ventana **Estados y registros** que se abre, seleccione la sección **Ejecución de una aplicación remota**.
4. En la ventana **Ejecución de una aplicación remota**, en la sección **Archivos de aplicaciones**, realice una de las siguientes acciones, según lo que el especialista de Kaspersky le pida hacer:
   - Seleccione un archivo ZIP que contenga la aplicación que desea ejecutar en el dispositivo cliente al hacer clic en el botón **Examinar**.
   - De ser necesario, especifique una aplicación de línea de comandos y sus argumentos.
5. Siga las instrucciones del especialista.

Descargar y eliminar archivos de Cuarentena y Copia de seguridad

Esta sección brinda información sobre cómo descargar y eliminar archivos de Cuarentena y Copia de seguridad en Kaspersky Security Center 14 Web Console.

Descarga de archivos de Cuarentena y Copia de seguridad

Puede descargar archivos de archivos de Cuarentena y Copia de seguridad solo si se cumple una de estas dos condiciones: la opción **No desconectar del Servidor de administración** está activada en la configuración del dispositivo, o se está utilizando una puerta de enlace de conexión. De lo contrario, no es posible realizar la descarga.

Para guardar en el disco duro una copia del archivo Cuarentena o Copia de seguridad:

1. Realice una de las siguientes acciones:
   - Si desea guardar una copia de un archivo que se encuentra en Cuarentena, diríjase a **OPERACIONES → REPOSITORIOS → CUARENTENA**.
   - Si desea guardar una copia de un archivo que se encuentra en Copia de seguridad, diríjase a **OPERACIONES → REPOSITORIOS → COPIA DE SEGURIDAD**.
2. En la ventana que se abre, seleccione el archivo que desea descargar y haga clic en **Descargar**.

Los inicios de descarga. Una copia del archivo que se había colocado en Cuarentena en el dispositivo cliente se guarda en la carpeta especificada.

Acerca de la eliminación de objetos de los repositorios de Cuarentena, Copia de seguridad o Amenazas activas

Cuando las aplicaciones de seguridad de Kaspersky instaladas en los dispositivos cliente colocan objetos en los repositorios de Cuarentena, Copia de seguridad o Amenazas activas, envían la información sobre los objetos añadidos a las secciones **CUARENTENA**, **COPIA DE SEGURIDAD**, o **AMENAZAS ACTIVAS** en Kaspersky Security Center. Cuando abre una de estas secciones, elige un objeto de la lista y hace clic en el botón **Eliminar**, Kaspersky Security Center realiza una de las siguientes acciones o ambas acciones:

- Elimina el objeto seleccionado de la lista
- Elimina el objeto seleccionado del repositorio

La acción a realizar la define la aplicación de Kaspersky que colocó el objeto seleccionado en el repositorio. La aplicación de Kaspersky se especifica en el campo **Entrada añadida por**. Consulte la documentación de la aplicación de Kaspersky para obtener detalles sobre qué acción se realizará.

Guía de referencia de API

Esta guía de referencia de Kaspersky Security Center OpenAPI está diseñada para ayudar en las siguientes tareas:

- Automatización y personalización. Usted puede automatizar tareas que quizás no desee gestionar de forma manual mediante la Consola de administración. También puede implementar escenarios personalizados que aún no sean compatibles con la Consola de administración. Por ejemplo, como administrador, puede utilizar Kaspersky Security Center OpenAPI para crear y ejecutar scripts que faciliten el desarrollo de la estructura de los grupos de administración y la mantengan actualizada.

- Desarrollo a la medida. Por ejemplo, puede desarrollar una Consola de administración alternativa basada en MMC para sus clientes, que permita un conjunto limitado de acciones.

En la guía de referencia de OpenAPI puede usar el campo de búsqueda de la parte derecha de la pantalla para encontrar la información que necesita.

GUÍA DE REFERENCIA DE OPENAPI

Puede encontrar ejemplos de coincidencia entre algunos escenarios de usuario y métodos de OpenAPI en la siguiente tabla.

Coincidencia entre escenarios de usuario y ejemplos de métodos de Kaspersky Security Center OpenAPI

Muestra	Propósito de la muestra	Escenario
Log KlAkParams	Puede extraer y procesar datos utilizando la estructura de datos `KlAkParams`. La muestra indica cómo trabajar con esta estructura de datos. La salida de la muestra se puede presentar de diferentes maneras. Puede obtener los datos para enviar un método HTTP o para usarlo en su código.	Supervisión e informes
Crear y eliminar una jerarquía "principal/secundaria"	Puede añadir un Servidor de administración secundario para establecer una jerarquía "principal/secundario". Alternativamente, puede desconectar de la jerarquía el Servidor de administración secundario.	• Creación de una jerarquía de Servidores de administración: adición de un Servidor de administración secundario • Eliminación de una jerarquía de Servidores de administración
Crear la jerarquía de grupo con una estructura basada en la unidad de Active Directory	Puede sondear la unidad de Active Directory y formar una jerarquía de grupos con los dispositivos descubiertos.	Creación de grupos de administración
Crear la jerarquía de grupo con una estructura basada en la unidad de Active Directory en caché	Puede formar una jerarquía de los grupos de dispositivos administrados en función de la unidad de Active Directory sondeada anteriormente. Si después del último sonde aparecen nuevos dispositivos en el directorio activo, no se los añade al grupo porque no están en los resultados de sondeo guardados.	Creación de grupos de administración

Descargar archivos de lista de red mediante la pasarela de conexión en el dispositivo especificado	Puede conectarse al agente de red en el dispositivo necesario utilizando una pasarela de conexión y luego descargar un archivo con la lista de red a su dispositivo.	Ajuste de puntos de distribución y puertas de enlace de conexión
Instalar una clave de licencia almacenada en el repositorio del Servidor de administración principal en los Servidores de administración secundarios	Puede conectarse al Servidor de administración principal, cargar desde allí la clave de licencia necesaria y transmitirla a todos los Servidores de administración secundarios incluidos en una jerarquía.	Obtención de licencias de aplicaciones administradas
Crear un informe de derechos de usuario efectivos.	Puede crear diferentes informes Por ejemplo, puede generar el informe de derechos de usuario efectivos utilizando esta muestra. Este informe describe los derechos que tiene un usuario, dependiendo de su grupo y papel. Puede descargar el informe en formato HTML, PDF o Excel.	Generación y visualización de un informe
Iniciar una tarea para un dispositivo	Puede conectarse al Agente de red en el dispositivo necesario utilizando una pasarela de conexión y luego ejecutar la tarea necesaria.	Inicio de una tarea de forma manual
Creación de subredes IP basadas en el sitio y los servicios de Active Directory	Puede crear una subred IP según la unidad de Active Directory que use. La muestra inicia el sondeo del rango de IP especificado y elimina las subredes descubiertas para impedir que entren en conflicto con una nueva subred. Por lo tanto, no ejecute esta muestra en la red donde sea importante guardar subredes. Después de realizar el sondeo, la muestra recurre a Active Directory, examina cada dispositivo en él y crea la subred IP. Para ello, la muestra utiliza las máscaras y las direcciones IP de todos los dispositivos.	Configuración de protección de la red
Registrar puntos de distribución para dispositivos en un grupo	Puede asignar dispositivos administrados como puntos de distribución (antes conocidos como agentes de actualización).	Actualización de bases de datos Kaspersky y aplicaciones
Enumerar todos los grupos	Puede realizar varias acciones en los grupos de administración: El ejemplo muestra cómo hacer lo siguiente: • Obtener un identificador del grupo raíz "Dispositivos administrados" • Moverse a través de la jerarquía de grupo • Recuperar la jerarquía completa y ampliada de los grupos, junto con sus nombres y nivel de anidación.	Configuración del Servidor de administración
Enumerar tareas,	Puede averiguar la siguiente información:	Supervisión de la

consultar estadísticas de tareas y ejecutar una tarea	• Historial de progreso de la tarea • Estado de la tarea actual • Número de tareas en diferentes estados. También puedes ejecutar una tarea. De forma predeterminada, la muestra ejecuta una tarea después de emitir sus estadísticas.	ejecución de tareas
Crear y ejecuta una tarea	Puede crear una tarea. Especifique los siguientes parámetros de la tarea en la muestra: • Tipo • Método de ejecución • Nombre • Grupo de dispositivos para el cual se utilizará la tarea. De forma predeterminada, la muestra crea una tarea con el tipo "Mostrar mensaje". Puede ejecutar esta tarea para todos los dispositivos administrados del Servidor de administración. Si es necesario, puede especificar sus propios parámetros de tarea.	Creación de una tarea
Enumerar claves de licencia	Puede obtener una lista de todas las claves de licencia activas para aplicaciones Kaspersky instaladas en dispositivos administrados de Administration Server. La lista contiene datos detallados sobre cada clave de licencia, como un nombre, tipo o fecha de vencimiento.	Visualización de información sobre claves de licencias en uso
Crear y buscar un usuario interno	Puede crear una cuenta para un trabajo adicional.	Selección de una cuenta para iniciar el Servidor de administración
Crear una categoría personalizada	Puede crear la categoría de aplicación con los parámetros necesarios.	Creación de una categoría de aplicaciones con contenido agregado manualmente
Enumerar usuarios mediante SrvView	Puede usar la clase SrvView para solicitar información detallada al Servidor de administración. Por ejemplo, puede obtener una lista de usuarios utilizando esta muestra.	Administración de cuentas de usuario.

Aplicaciones que interactúan con Kaspersky Security Center a través de OpenAPI

Algunas aplicaciones interactúan con Kaspersky Security Center a través de OpenAPI. Entre esas aplicaciones están Kaspersky Anti Targeted Attack Platform y Kaspersky Security for Virtualization. También puede ser una aplicación cliente personalizada que usted desarrolló a partir de OpenAPI.

Las aplicaciones que interactúan con Kaspersky Security Center a través de OpenAPI se conectan al Servidor de administración. Si ha configurado un lista de direcciones IP permitidas para conectarse al Servidor de administración, agregue las direcciones IP de los dispositivos donde están instaladas las aplicaciones que utilizan Kaspersky Security Center OpenAPI. Para saber si la aplicación que utiliza funciona con OpenAPI, consulte la Ayuda de esta aplicación.

Prácticas recomendadas para proveedores de servicios

Esta sección proporciona información acerca de la configuración y el uso de Kaspersky Security Center.

Esta sección contiene recomendaciones sobre cómo desplegar, configurar y usar la aplicación y, además, describe formas de resolver los problemas habituales en la operación de la aplicación.

Planificación del despliegue de Kaspersky Security Center

Al planificar el despliegue de los componentes de Kaspersky Security Center en una red de la organización, debe tener en cuenta el tamaño y la cobertura del proyecto; específicamente, los factores siguientes:

- Número total de dispositivos.
- Número de clientes MSP.

Un Servidor de administración puede admitir un máximo de 100.000 dispositivos. Si el número total de dispositivos en una red de la organización supera los 100.000, el lado del proveedor de servicios debe desplegar varios Servidores de administración y combinarse en una jerarquía para una administración centralizada y cómoda.

Se pueden crear hasta 500 servidores virtuales en un solo Servidor de administración, por lo que se requiere un Servidor de administración particular por cada 500 clientes MSP.

En la etapa de la planificación del despliegue, debe considerarse la asignación del certificado especial X.509 al Servidor de administración. La asignación del certificado X.509 al Servidor de administración puede ser útil en los siguientes casos (lista parcial):

- Inspección del tráfico de la capa de sockets seguros (SSL) mediante la cancelación de SSL.
- Especificación de valores obligatorios en campos del certificado.
- Suministro de la fuerza de cifrado requerida de un certificado.

Suministro de acceso a Internet al Servidor de administración

Para permitir que los dispositivos de la red del cliente accedan al Servidor de administración mediante Internet, debe poner a su disposición los siguientes puertos del Servidor de administración:

- 13000 TCP: puerto TLS del Servidor de administración para conectar Agentes de red desplegados en la red del cliente
- 8061 TCP: puerto HTTPS para publicar paquetes independientes usando herramientas de la Consola de administración
- 8060 TCP: puerto HTTP para publicar paquetes independientes usando herramientas de la Consola de administración
- 13292 TCP: puerto de TLS solo requerido si hay dispositivos móviles que se deban administrar

Si tiene que proporcionar a clientes con opciones básicas de administración de la red mediante Kaspersky Security Center 14 Web Console, también debe abrir los siguientes puertos de Kaspersky Security Center 14 Web Console:

- 8081 TCP: puerto HTTPS
- 8080 TCP: puerto HTTP

Configuración estándar de Kaspersky Security Center

Se despliegan uno o varios Servidores de administración en los servidores de los MSP. El número de Servidores de administración puede seleccionarse según el hardware disponible, el número total de clientes MSP o el número total de dispositivos administrados.

Un Servidor de administración puede admitir hasta 100 000 dispositivos. Debe considerar la posibilidad de aumentar el número de dispositivos administrados en el futuro próximo: puede ser útil conectar un número ligeramente menor de dispositivos a un único Servidor de administración.

Se pueden crear hasta 500 servidores virtuales en un solo Servidor de administración, por lo que se requiere un Servidor de administración particular por cada 500 clientes MSP.

Si se utilizan varios servidores, se recomienda que los combine en una jerarquía. La utilización de una jerarquía de Servidores de administración le permite evitar directivas y tareas duplicadas, gestionar el conjunto entero de dispositivos administrados como si estuvieran administrados por un Servidor de administración único: es decir, buscar dispositivos, crear selecciones de dispositivos y crear informes.

En cada servidor virtual que corresponda a un cliente MSP, debe asignar uno o varios puntos de distribución. Si los clientes MSP y el Servidor de administración se vinculan por Internet, puede ser útil crear una tarea *Descargar actualizaciones en los repositorios de puntos de distribución*, de modo que las actualizaciones se descarguen directamente desde los servidores de Kaspersky y no desde el Servidor de administración.

Si algunos dispositivos en la red del cliente MSP no tienen acceso directo a Internet, debe cambiar los puntos de distribución al modo de puerta de enlace de conexión. En este caso, los Agentes de red en los dispositivos en la red del cliente MSP se conectarán, para mayor sincronización, al Servidor de administración, pero mediante la puerta de enlace, no de manera directa.

Dado que lo más probable es que el Servidor de administración no pueda sondear la red del cliente MSP, puede ser útil trasladar esta función a un punto de distribución.

El Servidor de administración no podrá enviar notificaciones al puerto UDP 15000 a dispositivos administrados localizados detrás de la NAT en la red del cliente MSP. Para resolver este problema, puede ser útil activar el modo de conexión continua con el Servidor de administración en las propiedades de los dispositivos que funcionan como puntos de distribución y se ejecutan en el modo de puerta de enlace de conexión (casilla de verificación **No desconectar del Servidor de administración**). El modo de conexión continua está disponible si el número total de puntos de distribución no supera los 300.

Acerca de los puntos de distribución

Los dispositivos que tengan instalado el Agente de red pueden utilizarse como punto de distribución. En este modo, el Agente de red puede realizar las siguientes funciones:

- Distribuir actualizaciones (que pueden recuperarse del Servidor de administración o de servidores de actualización de Kaspersky). En este último caso, debe crearse la tarea *Descargar actualizaciones en los repositorios de puntos de distribución* para el dispositivo que sirve como punto de distribución.
- Instalar software (incluido el despliegue inicial de Agentes de red) en otros dispositivos.

- Sondear la red para detectar dispositivos nuevos y actualizar la información sobre los existentes. Un punto de distribución puede aplicar los mismos métodos de detección de dispositivos que el Servidor de administración.

El despliegue de puntos de distribución en una red de la organización cumple los siguientes objetivos:

- Reducir la carga en el Servidor de administración si funciona como la fuente de actualizaciones.
- Optimizar el tráfico de Internet dado que, en este caso, no es necesario que cada dispositivo en la red del cliente del proveedor de servicios administrados tenga acceso a servidores de Kaspersky o el Servidor de administración para actualizaciones.
- Proporcionar al Servidor de administración acceso a dispositivos detrás de la NAT (con relación al Servidor de administración) de la red del cliente MSP, lo que permite que el Servidor de administración realice las acciones siguientes:
  - Envíe notificaciones a dispositivos mediante UDP en la red IPv4 o IPv6.
  - Sondee la red IPv4 o IPv6.
  - Realice el despliegue inicial.
  - Actúe como un servidor push.

Se asigna un punto de distribución para un grupo de administración. En este caso, la cobertura del punto de distribución incluye todos los dispositivos dentro del grupo de administración y todos sus subgrupos. Sin embargo, el dispositivo que funciona como el punto de distribución no debe incluirse en el grupo de administración al cual se ha asignado.

Puede realizar una función de punto de distribución como una puerta de enlace de conexión. En este caso, los dispositivos en la cobertura del punto de distribución se conectarán al Servidor de administración a través de la puerta de enlace, no directamente. Puede usar este modo en situaciones que no permitan el establecimiento de una conexión directa entre dispositivos con el Agente de red y un Servidor de administración.

Los dispositivos que funcionan como puntos de distribución se deben proteger, incluida la protección física, contra cualquier acceso no autorizado.

Jerarquía de Servidores de administración

Un MSP puede ejecutar varios Servidores de administración. Puede resultar incómodo administrar varios Servidores de administración independientes, por lo tanto, se puede aplicar una jerarquía. Una configuración de "principal/secundario" para dos Servidores de administración proporciona las siguientes opciones:

- Un Servidor de administración secundario hereda directivas y tareas del Servidor de administración principal, lo que evita la copia de la configuración.
- Las selecciones de dispositivos en el Servidor de administración principal pueden incluir dispositivos de Servidores de administración secundarios.
- Los informes sobre el Servidor de administración principal pueden contener datos (incluida información detallada) de Servidores de administración secundarios.

Servidores de administración virtual

Sobre la base de un Servidor de administración físico, se pueden crear varios Servidores de administración virtuales, que serán similares a los Servidores de administración secundarios. Comparado con el modelo de acceso discrecional, que se basa en listas de control de acceso (ACL), el modelo del Servidor de administración virtual es más funcional y proporciona un mayor nivel de aislamiento. Además de una estructura dedicada de grupos de administración para dispositivos asignados con directivas y tareas, cada Servidor de administración virtual presenta su propio grupo de dispositivos no asignados, sus propios conjuntos de informes, dispositivos seleccionados y eventos, paquetes de instalación, reglas móviles, etc. Para el aislamiento mutuo máximo de clientes MSP, recomendamos que elija Servidores de administración virtuales como la funcionalidad que se utilizará. Asimismo, la creación de un Servidor de administración virtual para cada cliente MSP le permite proporcionar a clientes opciones básicas de administración de la red mediante Kaspersky Security Center 14 Web Console.

Los Servidores de administración virtuales son muy similares a los Servidores de administración secundarios, pero con las distinciones siguientes:

- Un Servidor de administración virtual carece de la configuración más global y sus propios puertos TCP.
- Un Servidor de administración virtual no tiene Servidores de administración secundarios.
- Un Servidor de administración virtual no tiene otros Servidores de administración virtuales.
- Un Servidor de administración físico ve dispositivos, grupos, eventos y objetos en dispositivos administrados (elementos en Cuarentena, registro de aplicaciones, etc.) de todos sus Servidores de administración virtuales.
- Un Servidor de administración virtual solo puede analizar la red con puntos de distribución conectados.

Administración de dispositivos móviles con Kaspersky Endpoint Security for Android

Los dispositivos móviles con Kaspersky Endpoint Security for Android™ instalado (en adelante, denominados dispositivos KES) se administran por medio del Servidor de administración. Kaspersky Security Center 10 Service Pack 1, así como versiones anteriores, admite las siguientes funciones para administrar dispositivos KES:

- Manipulación de dispositivos móviles como dispositivos cliente:
  - Pertenencia a grupos de administración
  - Supervisión, por ejemplo, ver estados, eventos e informes
  - Modificación de la configuración local y asignación de directivas para Kaspersky Endpoint Security for Android
- Envío de comandos en modo centralizado
- Instalación de paquetes de aplicaciones móviles remotamente

El Servidor de administración gestiona los dispositivos KES mediante TLS, puerto TCP 13292.

Despliegue y configuración inicial

Kaspersky Security Center es una aplicación distribuida. Kaspersky Security Center incluye las aplicaciones siguientes:

- Servidor de administración: componente principal, diseñado para administrar dispositivos de una organización y almacenar datos en DBMS.
- Consola de administración: herramienta básica para el administrador. La Consola de administración se envía junto con el Servidor de administración, pero también puede instalarse individualmente en uno o varios dispositivos ejecutados por el administrador.
- Kaspersky Security Center 14 Web Console es una interfaz web para el Servidor de administración diseñada para las operaciones básicas. Puede instalar este componente en cualquier dispositivo que cumpla requisitos de software y hardware.
- Agente de red: diseñado para administrar la aplicación de seguridad instalada en un dispositivo, así como para recibir información sobre ese dispositivo. Los Agentes de red se instalan en los dispositivos de una organización.

El despliegue de Kaspersky Security Center en una red de la organización se realiza del siguiente modo:

- Instalación del Servidor de administración.
- La Instalación de Kaspersky Security Center 14 Web Console.
- Instalación de la Consola de administración en el dispositivo del administrador.
- Instalación del Agente de red y la aplicación de seguridad en los dispositivos de la empresa.

Recomendaciones para la instalación del Servidor de administración

Esta sección contiene recomendaciones sobre cómo instalar el Servidor de administración. Esta sección también proporciona situaciones para usar una carpeta compartida en el dispositivo del Servidor de administración a fin de desplegar el Agente de red en dispositivos cliente.

Creación de cuentas para los servicios del Servidor de administración en un clúster de conmutación por error

De forma predeterminada, el instalador crea automáticamente cuentas sin privilegios para los servicios del Servidor de administración. Este comportamiento es el más cómodo para la instalación del Servidor de administración en un dispositivo ordinario.

Sin embargo, la instalación del Servidor de administración en un clúster de conmutación por error requiere una situación diferente:

1. Cree cuentas de dominio sin privilegios para servicios del Servidor de administración y hágalas miembros de un grupo de seguridad de dominio global denominado KLAdmins.
2. En el programa de instalación del Servidor de administración, especifique las cuentas de dominio que se han creado para los servicios.

Selección de un DBMS

Al instalar el Servidor de administración, puede seleccionar el DBMS que usará el Servidor de administración. Al seleccionar el sistema de gestión de bases de datos (DBMS) para que lo utilice un Servidor de administración, debe tomar en cuenta el número de dispositivos abarcados por el Servidor de administración.

La siguiente tabla enumera las opciones de DBMS válidas, así como las restricciones en su uso.

Restricciones en DBMS

DBMS	Restricciones
SQL Server Express Edition 2012 o posterior	No se recomienda si tiene la intención de ejecutar un único Servidor de administración para más de 10 000 dispositivos o usar Control de aplicaciones.
Edición de SQL Server local, no Express, 2012 o posterior	Sin limitaciones.
Edición de SQL Server remota, no Express, 2012 o posterior	Solo es válido si ambos dispositivos están en el mismo dominio Windows®; si los dominios difieren, se debe establecer una relación de confianza bidireccional entre ellos.
Local o remota MySQL 5.5, 5.6 o 5.7 (Las versiones de MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4 y 5.5.5 ya no son compatibles)	No se recomienda si tiene la intención de ejecutar un único Servidor de administración para más de 10 000 dispositivos o usar Control de aplicaciones.
MySQL 8.0.20 o versión posterior local o remoto	No se recomienda si tiene la intención de ejecutar un único Servidor de administración para más de 50 000 dispositivos o usar Control de aplicaciones.
Servidor MariaDB 10.3 local o remoto	No se recomienda si tiene la intención de ejecutar un único Servidor de administración para más de 20 000 dispositivos o usar el Control de aplicaciones.

Si está utilizando SQL Server 2019 como DBMS y no tiene el parche acumulativo CU12 o posterior, debe realizar lo siguiente después de instalar Kaspersky Security Center:

1. Conéctese a SQL Server con SQL Management Studio.
2. Ejecute los siguientes comandos (si eligió un nombre diferente para la base de datos, use ese nombre en lugar de KAV):

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

3. Reinicie el servicio SQL Server 2019.

De lo contrario, el uso de SQL Server 2019 puede generar errores, como "There is insufficient system memory in resource pool 'internal' to run this query".

Se prohíbe estrictamente el uso concurrente de SQL Server Express Edition DBMS por el Servidor de administración y otra aplicación.

Especificación de la dirección del Servidor de administración

Al instalar el Servidor de administración, debe especificar la dirección externa del Servidor de administración. Esta dirección se utilizará como la dirección predeterminada al crear paquetes de instalación del Agente de red. Después de esto, podrá cambiar la dirección del dispositivo con el Servidor de administración usando herramientas de la Consola de administración; la dirección no cambiará automáticamente en los paquetes de instalación del Agente de red que ya hayan sido creados.

Configuración de un sistema de protección en la red de la organización cliente

Una vez completada la instalación del Servidor de administración, la Consola de administración se inicia y le solicita realizar la configuración inicial a través del asistente relevante. Cuando el Asistente de inicio rápido se está ejecutando, se crean las siguientes directivas y tareas en el grupo de administración de raíz:

- Directiva de Kaspersky Endpoint Security
- Tarea de grupo para actualizar Kaspersky Endpoint Security
- Tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security
- Directiva del Agente de red
- Tarea de análisis de vulnerabilidades (tarea del Agente de red)
- Tarea de instalación de actualizares y reparación de vulnerabilidades (tarea del Agente de red)

Las directivas y las tareas se crean con las configuraciones predeterminadas, que pueden resultar subóptimas o, incluso, inadmisibles para la organización. Por lo tanto, debe comprobar las propiedades de los objetos que se han creado y modificarlas manualmente, si es necesario.

Esta sección contiene la información sobre la configuración manual de directivas, tareas, y otra configuración del Servidor de administración e información sobre el punto de distribución, la construcción de una estructura del grupo de administración y la jerarquía de tareas y otros ajustes.

Configuración manual de la directiva de Kaspersky Endpoint Security

Esta sección proporciona recomendaciones sobre cómo configurar la directiva de Kaspersky Endpoint Security, que es creada por el Asistente de inicio rápido. Puede realizar la configuración en la ventana de propiedades de la directiva.

Al modificar un ajuste de configuración, tenga en cuenta que debe hacer clic en el icono de bloqueo sobre el ajuste relevante a fin de permitir que se use su valor en una estación de trabajo.

Configuración de la directiva en la sección Protección avanzada contra amenazas

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

En la sección **Protección avanzada contra amenazas**, puede configurar el uso de Kaspersky Security Network para Kaspersky Endpoint Security para Windows. También puede configurar los módulos de Kaspersky Endpoint Security para Windows, como detección de comportamiento, prevención de exploits, prevención de intrusiones en el host y motor de reparación.

En la subsección **Kaspersky Security Network**, le recomendamos que active la opción **Usar proxy KSN**. Utilice esta opción para redistribuir y optimizar el tráfico en la red. También puede habilitar el uso de servidores KSN si el servicio Proxy KSN no está disponible. Los servidores de KSN pueden estar localizados en el lado de Kaspersky (cuando se usa KSN global) o en el lado de terceros (cuando se usa KSN privada).

Configuración de la directiva en la sección Protección frente a amenazas básicas

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

A continuación, se describen las acciones de configuración adicionales que recomendamos que realice en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Protección frente a amenazas básicas**.

Sección Protección frente a amenazas básicas, subsección Firewall

Compruebe la lista de redes en las propiedades de la directiva. La lista puede no contener todas las redes.

Para comprobar la lista de redes, siga estos pasos:

1. En las propiedades de la directiva, en la sección **Protección frente a amenazas básicas**, seleccione la subsección **Firewall**.
2. En la sección **Redes disponibles**, haga clic en el botón **Configuración**.

   De este modo, se abre la ventana **Firewall**. Esta ventana muestra la lista de redes en la ficha **Redes**.

Sección Protección frente a amenazas básicas, subdivisión Protección frente a amenazas en archivos

La activación del análisis de las unidades de red puede aplicar una carga significativa a las unidades de red. Resulta más cómodo realizar un análisis indirecto en los servidores de archivo.

Para desactivar el análisis de unidades de red:

1. En las propiedades de la directiva, en la sección **Protección frente a amenazas básicas**, seleccione la subsección **Protección frente a amenazas en archivos**.
2. En la sección **Nivel de seguridad**, haga clic en el botón **Configuración**.

3. En la ventana **Protección frente a amenazas en archivos** que se abre, en la ficha **General**, desactive la casilla **Todas las unidades de red**.

Configuración de la directiva en la sección Configuración general

Para obtener una descripción completa de la configuración en esta sección, consulte la documentación de Kaspersky Endpoint Security para Windows.

A continuación, se describen las acciones de configuración avanzadas que recomendamos realizar en la ventana de propiedades de la directiva de Kaspersky Endpoint Security para Windows, en la sección **Configuración general**.

Sección Configuración general, subsección Informes y Almacenamiento

En la sección **Transferencia de datos al Servidor de administración**, tenga en cuenta la configuración siguiente:

Casilla **Acerca de las aplicaciones iniciadas**: si esta casilla está seleccionada, la base de datos del Servidor de administración guarda la información acerca de todas las versiones de todos los módulos de software en los dispositivos en red. Esta información puede requerir una cantidad significativa de espacio en el disco en la base de datos de Kaspersky Security Center (docenas de gigabytes). Por lo tanto, si la casilla **Acerca de las aplicaciones iniciadas** aún está seleccionada en la directiva de alto nivel, se debe borrar.

Sección Configuración general, subsección Interfaz

Si la protección antivirus en la red de la organización debe administrarse en el modo centralizado a través de la Consola de administración, debe desactivar la visualización de la interfaz de usuario de Kaspersky Endpoint Security para Windows en las estaciones de trabajo (al desactivar la casilla **Mostrar interfaz de la aplicación** en la sección **Interacción con el usuario**) y activar la protección con contraseña (al seleccionar la casilla **Activar protección con contraseña** en la sección **Protección de contraseñas**).

Configuración de la directiva en la sección Configuración de eventos

En la sección **Configuración de eventos**, debe desactivar el guardado de todos los eventos en el Servidor de administración, excepto los siguientes:

- En la ficha **Evento crítico**:
  - La ejecución automática de la aplicación está desactivada
  - Acceso denegado
  - Inicio de aplicación prohibido
  - La desinfección no es posible
  - Contrato de licencia violado
  - No se pudo cargar el módulo de cifrado

- No se pueden iniciar dos tareas al mismo tiempo
- Se detectó una amenaza activa. Iniciar Desinfección avanzada
- Se detectó un ataque de red
- No todos los componentes fueron actualizados
- Error de activación
- Error al activar el modo portátil
- Error en la interacción con Kaspersky Security Center
- Error al desactivar el modo portátil
- Error al cambiar los componentes de la aplicación
- Error al aplicar las reglas de cifrado/descifrado del archivo
- La directiva no se puede aplicar
- El proceso finalizó
- Actividad de red bloqueada

- En la pestaña **Fallo operativo**: Configuración incorrecta de la tarea. Configuración no aplicada
- En la ficha **Advertencia**:
  - La autoprotección está desactivada
  - Clave de reserva incorrecta
  - El usuario ha decidido excluirse de la directiva de cifrado
- En la pestaña **Información**: Inicio de la aplicación prohibido en el modo de prueba

Configuración manual de la tarea de actualización de grupo para Kaspersky Endpoint Security

La información de esta subsección solo es aplicable a Kaspersky Security Center 10 Maintenance Release 1 y versiones posteriores.

Si el Servidor de administración actúa como fuente de actualizaciones, la opción de programación óptima y recomendada para Kaspersky Endpoint Security 10 y versiones posteriores es **Cuando se descargan nuevas actualizaciones en el repositorio** cuando la casilla **Utilizar retardo aleatorio automático para el inicio de tareas** esté seleccionada.

Para una tarea de actualización grupal en Kaspersky Endpoint Security versión 8, debe especificar explícitamente el retraso del lanzamiento (1 hora o más) y seleccionar la casilla **Utilizar retardo aleatorio automático para el inicio de tareas**.

Si se crea una tarea local para descargar actualizaciones de servidores de Kaspersky al repositorio en cada punto de distribución, la programación periódica será óptima y recomendada para la tarea de actualización del grupo de Kaspersky Endpoint Security. En este caso, el valor del intervalo de aleatorización debería configurarse en 1 hora.

Configuración manual de la tarea de grupo para analizar un dispositivo con Kaspersky Endpoint Security

El Asistente de inicio rápido crea una tarea de grupo para analizar un dispositivo. De forma predeterminada, se asigna a la tarea la programación **Ejecutar el viernes a las 7:00 p. m.** con asignación aleatoria automática y la casilla **Ejecutar tareas no realizadas** está desmarcada.

Esto significa que si los dispositivos de una organización se apagan, por ejemplo, los viernes a las 6:30 p.m., la tarea de análisis de los dispositivos nunca se ejecutará. Debe configurar la programación más cómoda para esta tarea según las reglas del lugar de trabajo adoptadas en la organización.

Programación de la tarea Buscar vulnerabilidades y actualizaciones requeridas

El Asistente de inicio rápido crea la tarea *Buscar vulnerabilidades y actualizaciones requeridas* para el Agente de red. De forma predeterminada, se asigna a la tarea la programación **Ejecutar los martes a las 7:00 p. m.** con asignación aleatoria automática y la casilla **Ejecutar tareas no realizadas** está marcada.

Si las reglas del lugar de trabajo de la organización garantizan que todos los dispositivos se apagan en este momento, la tarea *Buscar vulnerabilidades y actualizaciones requeridas* se ejecutará después de que los dispositivos se enciendan nuevamente, es decir, el miércoles por la mañana. Tal actividad puede ser indeseable porque un análisis de vulnerabilidades puede aumentar la carga en los subsistemas del disco y las CPU. Debe configurar la programación más cómoda para la tarea según las reglas del lugar de trabajo adoptadas en la organización.

Configuración manual de la tarea de grupo para la instalación de actualizaciones y la reparación de la vulnerabilidad

El Asistente de inicio rápido crea una tarea de grupo para la instalación de actualizaciones y la reparación de la vulnerabilidad para el Agente de red. De forma predeterminada, la tarea está configurada para ejecutarse todos los días a la 01:00 A.M., con asignación aleatoria automática y la opción **Ejecutar tareas pendientes** está desactivada.

Si las reglas del lugar de trabajo de la organización garantizan el apagado de dispositivos durante la noche, la instalación de las actualizaciones nunca se ejecutará. Debe configurar la programación más cómoda para la tarea de análisis de vulnerabilidades según las reglas del lugar de trabajo adoptadas en la organización. También es importante tener en cuenta que la instalación de actualizaciones puede requerir reiniciar el dispositivo.

Creación de una estructura de grupos de administración y asignación de puntos de distribución

Una estructura de grupos de administración en Kaspersky Security Center realiza las funciones siguientes:

- Configura la cobertura de las directivas.

  Existe otra forma de aplicar ajustes pertinentes en dispositivos: mediante el uso de perfiles de directiva. En este caso, la cobertura de directivas se configura mediante etiquetas, ubicaciones del dispositivo en unidades organizativas de Active Directory, pertenencia a grupos de seguridad de Active Directory, etc.

- Configura la cobertura de las tareas de grupo.

  Existe un enfoque para definir la cobertura de las tareas de grupo que no se basan en una jerarquía de los grupos de administración: el uso de tareas para selecciones de dispositivos y tareas para dispositivos específicos.

- Configura los derechos de acceso a dispositivos, Servidores de administración virtuales y Servidores de administración secundarios.

- Asigna puntos de distribución.

Al construir la estructura de los grupos de administración, debe tener en cuenta la topología de la red de la organización para la asignación óptima de puntos de distribución. La distribución óptima de los puntos de distribución le permite ahorrar tráfico de la red de la organización.

Según el organigrama y la topología de red adoptada por el cliente MSP, pueden aplicarse las siguientes configuraciones estándares a la estructura de grupos de administración:

- Oficina única

- Varias pequeñas oficinas separadas

Configuración estándar de un cliente MSP: oficina única

En una configuración de "oficina única" estándar, todos los dispositivos están dentro de la red de la organización. La red de la organización puede consistir en unas partes independientes (redes o segmentos de red) vinculadas por canales estrechos.

Los métodos siguientes de crear la estructura de grupos de administración son posibles:

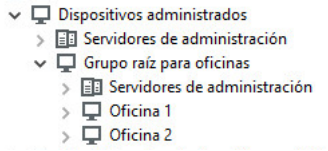
- Crear la estructura de grupos de administración tomando en consideración la topología de red. La estructura de grupos de administración puede no reflejar la topología de red con precisión absoluta. Una coincidencia entre las partes independientes de la red y ciertos grupos de administración sería suficiente. Puede usar la asignación automática de puntos de distribución o asignarlos manualmente.

- La creación de la estructura de grupos de administración, sin tomar la topología de red en cuenta. En este caso, debe desactivar la asignación automática de puntos de distribución y luego asignar uno o varios dispositivos para que actúen como puntos de distribución para un grupo de administración de raíz en cada una de las partes independientes de la red, por ejemplo, para el grupo **Dispositivos administrados**. Todos los puntos de distribución estarán al mismo nivel y presentarán la misma cobertura que abarca a todos los dispositivos en la red de la organización. En este caso, cada Agente de red se conectará con el punto de distribución que tenga la ruta más corta. La ruta a un punto de distribución se puede rastrear con la herramienta tracert.

Configuración estándar de un cliente MSP: varias pequeñas oficinas remotas

Esta configuración estándar sirve para varias pequeñas oficinas remotas, que se pueden comunicar con la oficina central mediante Internet. Cada oficina remota está ubicada detrás de la NAT, es decir, la conexión de una oficina remota a otra no es posible porque las oficinas están aisladas la una de la otra.

La configuración se debe reflejar en la estructura de los grupos de administración: se debe crear un grupo de administración independiente para cada oficina remota (grupos **Oficina 1** y **Oficina 2** en la imagen a continuación).



Las oficinas remotas se incluyen en la estructura del grupo de administración

Se deben asignar uno o varios puntos de distribución a cada grupo de administración correspondiente a una oficina. Los puntos de distribución deben ser dispositivos en la oficina remota que tienen una cantidad suficiente de espacio libre en disco. Los dispositivos desplegados en el grupo **Oficina 1**, por ejemplo, accederán a los puntos de distribución asignados al grupo de administración de **Oficina 1**.

Si algunos usuarios se mueven entre oficinas físicamente con sus equipos portátiles, debe seleccionar dos o más dispositivos (además de los puntos de distribución existentes) en cada oficina remota y asignarlos para que funcionen como puntos de distribución para un grupo de administración de alto nivel (**Grupo raíz para oficinas** en la imagen anterior).

Ejemplo: Un equipo portátil se despliega en el grupo de administración de la **Oficina 1** y luego se mueve físicamente a la oficina que corresponde al grupo de administración de la **Oficina 2**. Después de que se mueve el equipo portátil, el Agente de red intenta acceder a los puntos de distribución asignados al grupo de la **Oficina 1**, pero esos puntos de distribución no están disponibles. Entonces, el Agente de red empieza a intentar acceder a los puntos de distribución que se han asignado al **Grupo raíz para oficinas**. Como las oficinas remotas están aisladas la una de la otra, los intentos de acceder a los puntos de distribución asignados al grupo de administración del **Grupo raíz para oficinas** solo tendrán éxito cuando el Agente de red intente acceder a los puntos de distribución en el grupo de la **Oficina 2**. Es decir, el equipo portátil permanecerá en el grupo de administración que corresponde a la oficina inicial, pero el equipo portátil usará el punto de distribución de la oficina donde físicamente se ubica en este momento.

Jerarquía de directivas, uso de perfiles de directiva

Esta sección proporciona información sobre cómo aplicar directivas a dispositivos en grupos de administración. Esta sección también proporciona información sobre los perfiles de la directiva admitidos en Kaspersky Security Center, que comienza en la versión 10 Service Pack 1.

Jerarquía de directivas

En Kaspersky Security Center, se usan directivas para definir un conjunto único de opciones en varios dispositivos. Por ejemplo, la cobertura de la directiva de la aplicación P definida para el grupo de administración G incluye dispositivos administrados con la aplicación P instalada que se hayan desplegado en el grupo G y todos sus subgrupos, excepto los subgrupos en los que la casilla **Heredar del grupo primario** esté desactivada en las propiedades.

Una directiva se diferencia de cualquier parámetro local por iconos de bloqueo (🔒) al lado de su parámetro. Si un parámetro (o un grupo de parámetros) está bloqueado en las propiedades de la directiva, debe usar, en primer lugar, este parámetro (o el grupo de parámetros) al crear la configuración efectiva y, en segundo lugar, debe escribir el parámetro o el grupo de parámetros en la directiva hacia abajo.

La creación de parámetros efectivos en un dispositivo se puede describir de la forma siguiente: los valores de todos los parámetros que no se han bloqueado se toman de la directiva, luego, se sobrescriben con los valores de los parámetros locales y, luego, la recopilación se sobrescribe con los valores de los parámetros bloqueados tomados de la directiva.

Las directivas de la misma aplicación se afectan mutuamente mediante la jerarquía de los grupos de administración: los parámetros Bloqueados de la directiva ascendente sobrescriben los mismos parámetros de la directiva descendente.

Existe una directiva especial para los usuarios fuera de la oficina. Esta directiva entra en vigor en un dispositivo cuando el dispositivo cambia a modo fuera de la oficina. Las directivas fuera de la oficina no afectan otras directivas mediante la jerarquía de grupos de administración.

La directiva fuera de la oficina no se admitirá en versiones posteriores de Kaspersky Security Center. Los perfiles de directiva se utilizarán en vez de directivas fuera de la oficina.

Perfiles de directiva

Aplicar directivas a dispositivos solo a través de la jerarquía de los grupos de administración puede ser incómodo en muchas circunstancias. Puede que sea necesario crear varias instancias de una sola directiva que se diferencie en uno o dos parámetros para diferentes grupos de administración y sincronizar el contenido de esas directivas en el futuro.

Para ayudarle a evitar tales problemas, Kaspersky Security Center, a partir de la versión 10 Service Pack 1, admite *perfiles de directiva*. Un perfil de directiva es un subconjunto de parámetros de la directiva denominado. Este subconjunto se distribuye en dispositivos de destino junto con la directiva, y se complementa en una condición específica denominada la *Condición de activación de perfil*. Los perfiles solo contienen parámetros que se diferencian de la directiva "básica", que está activa en el dispositivo cliente (equipo o dispositivo móvil). Al activarse un perfil se modifica la configuración de directiva que se encontraba activa en el dispositivo antes de que se activara el perfil. Esa configuración toma los valores especificados en el perfil.

Actualmente se imponen las siguientes restricciones en perfiles de directiva:

- Una directiva puede incluir un máximo de 100 perfiles.
- Un perfil de directiva no puede contener otros perfiles.
- Un perfil de directiva no puede contener configuraciones de notificación.

Contenido de un perfil

Un perfil de directiva contiene las siguientes partes constituyentes:

- Los perfiles de nombre con nombres idénticos se afectan mutuamente mediante la jerarquía de los grupos de administración con reglas comunes.
- Subconjunto de configuración de la directiva. A diferencia de la directiva, que contiene todos los parámetros, un perfil solo contiene los parámetros que realmente se requieren (parámetros bloqueados).
- La condición de activación es una expresión lógica con las propiedades del dispositivo. Un perfil está activo (complementa la directiva) solo cuando la condición de activación de perfil es verdadera. En todos los demás casos, el perfil es inactivo y se ignora. Las siguientes propiedades del dispositivo se pueden incluir en esa expresión lógica:

- Estado de modo fuera de la oficina.
- Propiedades de entorno de la red — Nombre de la regla activa para la conexión de Agente de red.
- Presencia o ausencia de etiquetas específicas en el dispositivo.
- Ubicación del dispositivo en una unidad de Active Directory: explícita (el dispositivo está en la UO especificada) o implícita (el dispositivo está en una UO, que está dentro de la UO especificada en cualquier nivel de anidamiento).
- Pertenencia del dispositivo al grupo de seguridad de Active Directory (explícita o implícita).
- Pertenencia del propietario del dispositivo al grupo de seguridad de Active Directory (explícita o implícita).

- Casilla de desactivación del perfil. Los perfiles desactivados siempre se ignoran y sus respectivas condiciones de activación no se verifican.
- Prioridad del perfil. Las condiciones de activación de diferentes perfiles son independientes, por lo tanto, es posible activar varios perfiles simultáneamente. Si los perfiles activos contienen recopilaciones no superpuestas de parámetros, no surgirán problemas. Sin embargo, si dos perfiles activos contienen valores diferentes del mismo parámetro, se producirá una ambigüedad. Esta ambigüedad se debe evitar a través de prioridades del perfil: el valor de la variable ambigua se tomará del perfil que tiene la prioridad más alta (el que tenga el valor más alto en la lista de perfiles).

Comportamiento de los perfiles cuando las directivas se afectan mutuamente mediante la jerarquía

Los perfiles con el mismo nombre se fusionan según las reglas de fusión de directivas. Los perfiles de una directiva hacia arriba tienen una prioridad más alta que los perfiles de una directiva hacia abajo. Si se prohíbe la modificación de parámetros en la directiva hacia arriba (están bloqueados), la directiva hacia abajo usa las condiciones de activación de perfil de la directiva hacia arriba. Si se permite la modificación de parámetros en la directiva hacia arriba, se utilizan las condiciones de activación de perfil de la directiva hacia abajo.

Ya que un perfil de directiva puede contener la propiedad **El dispositivo está desconectado** en su condición de activación, los perfiles reemplazan completamente la función de directivas para los usuarios fuera de la oficina, que ya no se admitirán.

Una directiva para los usuarios fuera de la oficina puede contener perfiles, pero sus perfiles solo se pueden activar después de que el dispositivo cambia al modo fuera de la oficina.

Tareas

Kaspersky Security Center administra las aplicaciones de seguridad de Kaspersky instaladas en dispositivos mediante la creación y ejecución de *tareas*. Las tareas son necesarias para instalar, iniciar y detener aplicaciones, analizar archivos, actualizar bases de datos y módulos de software, y realizar otras acciones en las aplicaciones.

Las tareas para una aplicación específica solo se pueden crear si el complemento de administración para esa aplicación está instalado.

Las tareas se pueden realizar en el Servidor de administración y en los dispositivos.

Las siguientes tareas se realizan en el Servidor de administración:

- Distribución automática de informes
- Descarga de actualizaciones al repositorio del Servidor de administración
- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de bases de datos
- Sincronización de Windows Update
- Creación de un paquete de instalación basado en la imagen del SO de un dispositivo de referencia

Los siguientes tipos de tareas se realizan en dispositivos:

- *Tareas locales*: tareas que se realizan en un dispositivo específico

  Las tareas locales pueden ser modificadas por el administrador usando herramientas de la Consola de administración, o por el usuario de un dispositivo remoto (por ejemplo, a través de la interfaz de la aplicación de seguridad). Si una tarea local ha sido modificada simultáneamente por el administrador y el usuario de un dispositivo administrado, los cambios hechos por el administrador entrarán en vigor, ya que tienen una prioridad más alta.

- *Tareas de grupo*: tareas que se realizan en todos los dispositivos de un grupo específico

  A menos que se especifique lo contrario en las propiedades de la tarea, una tarea de grupo también afecta a todos los subgrupos del grupo seleccionado. Las tareas de grupo también afectan (opcionalmente) los dispositivos que se han conectado a Servidores de administración virtuales y secundarios desplegados en ese grupo o cualquiera de sus subgrupos.

- *Tareas globales*: tareas que se realizan en un conjunto de dispositivos, independientemente de si se incluyen en algún grupo

Para cada aplicación, puede crear cualquier número de tareas de grupo, tareas globales o tareas locales.

Puede realizar cambios en la configuración de tareas, ver el progreso de las tareas y copiar, exportar, importar y eliminar tareas.

Una tarea se inicia en un dispositivo solo si la aplicación para la que se creó la tarea se está en ejecución.

Los resultados de las tareas se guardan en el registro de eventos de Microsoft Windows y en el registro de eventos de Kaspersky Security Center, tanto de manera central en el Servidor de administración como de manera local en cada dispositivo.

No incluya datos confidenciales en la configuración de la tarea. Por ejemplo, no especifique la contraseña del administrador de dominio.

Reglas de movimiento de dispositivos

Recomendamos que automatice la asignación de dispositivos a grupos de administración en el servidor virtual que corresponda a un cliente MSP con *reglas de movimiento de dispositivos*. Una regla de movimiento de dispositivo consiste en tres partes principales: nombre, condición de ejecución (expresión lógica con atributos del dispositivo) y grupo de administración de destino. Una regla mueve un dispositivo al grupo de administración de destino si los atributos del dispositivo cumplen la condición de ejecución de la regla.

Todas las reglas de movimiento de dispositivos tienen prioridades. El Servidor de administración comprueba los atributos del dispositivo en cuanto a si cumplen la condición de ejecución de cada regla, en orden ascendente de prioridad. Si los atributos del dispositivo cumplen la condición de ejecución de una regla, el dispositivo se mueve al grupo de destino, por lo que el procesamiento de la regla está completo para ese dispositivo. Si los atributos del dispositivo cumplen las condiciones de varias reglas, el dispositivo se mueve al grupo de destino de la regla con la prioridad más alta (es decir, el que tiene el rango más alto en la lista de reglas).

Las reglas de movimiento de dispositivos se pueden crear implícitamente. Por ejemplo, en las propiedades de un paquete de instalación o una tarea de instalación remota, puede especificar el grupo de administración al cual el dispositivo se debe mover después de que el Agente de red se instala en él. Además, el administrador de Kaspersky Security Center puede crear reglas de movimiento de dispositivos explícitamente en la lista de reglas de movimiento. La lista se ubica en la Consola de administración, en las propiedades del grupo **Dispositivos no asignados**.

De forma predeterminada, una regla de movimiento de dispositivo está destinada para la asignación inicial única de dispositivos a grupos de administración. La regla mueve dispositivos del grupo **Dispositivos no asignados** solo una vez. Si esta regla movió un dispositivo una vez, la regla nunca lo moverá nuevamente, aun si devuelve el dispositivo al grupo **Dispositivos no asignados** manualmente. Esta es la forma recomendada de aplicar reglas de movimiento.

Puede mover dispositivos que ya se hayan asignado a algunos de los grupos de administración. Para hacer esto, en las propiedades de una regla, desactive la casilla **Mover solo dispositivos que no pertenezcan a ningún grupo de administración**.

Aplicar reglas de movimiento a dispositivos que ya se han asignado a algunos de los grupos de administración aumenta considerablemente la carga en el Servidor de administración.

Puede crear una regla de movimiento que afectaría un solo dispositivo repetidamente.

Recomendamos encarecidamente que evite mover un dispositivo solo desde un grupo a otro repetidamente (por ejemplo, a fin de aplicar una directiva especial a ese dispositivo, ejecutar una tarea de grupo especial o actualizar el dispositivo a través de un punto de distribución específico).

Tales situaciones no se admiten, porque aumentan la carga en Servidor de administración y el tráfico de red a un grado extremo. Estas situaciones también entran en conflicto con los principios de funcionamiento de Kaspersky Security Center (en particular, en el área de derechos de acceso, eventos e informes). Otra solución se debe encontrar, por ejemplo, a través del uso de perfiles de directiva, tareas para selecciones de dispositivos, asignación de agentes de red según el guion estándar, etcétera.

Clasificación del software

La herramienta principal para supervisar la ejecución de aplicaciones son las *categorías de Kaspersky* (en adelante, también denominadas *categorías KL*). Las categorías KL ayudan a los administradores de Kaspersky Security Center a simplificar la asistencia de la clasificación del software y minimizar el tráfico que va a dispositivos administrados.

Las categorías de usuario solo se deben crear para aplicaciones que no pueden clasificarse en ninguna de las categorías KL existentes (por ejemplo, para el software hecho a la medida). Las categorías de usuario se crean basándose en el paquete de instalación de una aplicación (MSI) o una carpeta con paquetes de instalación.

Si una recopilación grande del software está disponible, que no se ha clasificado mediante categorías KL, puede ser útil crear una categoría que se actualiza automáticamente. Las sumas de comprobación de archivos ejecutables se añadirán automáticamente a esta categoría en cada modificación de la carpeta que contiene paquetes de distribución.

No es posible crear ninguna categoría de software que se actualice automáticamente sobre la base de las carpetas Mis documentos, %windir% y %ProgramFiles%. El grupo de archivos en estas carpetas está sujeto a cambios frecuentes, lo que lleva a un aumento en la carga en el Servidor de administración y un mayor tráfico de red. Debe crear una carpeta dedicada con la recopilación de software y periódicamente añadir nuevos elementos a ella.

Acerca de las aplicaciones de tenencia múltiple

Kaspersky Security Center permite a los administradores de proveedores de servicios y administradores de inquilinos usar las aplicaciones de Kaspersky con soporte de tenencia múltiple. Después de instalar una aplicación Kaspersky de tenencia múltiple en la infraestructura de un proveedor de servicios, los usuarios pueden comenzar a usar la aplicación.

Para separar tareas y directivas relacionadas con diferentes usuarios, debe crear un Servidor de administración Virtual dedicado en Kaspersky Security Center para cada usuario. Todas las tareas y directivas para aplicaciones de tenencia múltiple que se ejecutan para un usuario deben crearse para el grupo de administración de dispositivos administrados del Servidor de administración virtual correspondiente a ese usuario. Las tareas creadas para los grupos de administración relacionados con el Servidor de administración principal no afectan a los dispositivos de los usuarios.

A diferencia de los administradores de proveedores de servicios, un administrador de usuarios puede crear y ver tareas y directivas de aplicación solo para los dispositivos del usuario correspondiente. Los conjuntos de tareas y configuraciones de directivas disponibles para los administradores de proveedores de servicios y los administradores de usuarios son diferentes. Algunas de las tareas y la configuración de directivas no están disponibles para los administradores de usuarios.

Dentro de la estructura jerárquica de un usuario, las directivas creadas para aplicaciones de tenencia múltiple se heredan a los grupos de administración de nivel inferior, así como a los grupos de administración de nivel superior: la directiva se propaga a todos los dispositivos cliente que pertenecen al usuario.

Creación de copias de seguridad y restauración de la configuración del Servidor de administración

La copia de seguridad de la configuración del Servidor de administración y su base de datos se realiza a través de la tarea de copia de seguridad y la utilidad klbackup. Una copia de seguridad incluye toda la configuración principal y los objetos que pertenecen al Servidor de administración, por ejemplo, certificados, claves principales para el cifrado de unidades en dispositivos administrados, claves para varias licencias, la estructura de los grupos de administración con todo su contenido, tareas, directivas, etc. Con una copia de seguridad puede recuperar el funcionamiento de un Servidor de administración en el menor tiempo posible, entre una docena de minutos y un par de horas.

Si no hay ninguna copia de seguridad disponible, un fallo puede provocar una pérdida irrevocable de certificados y toda la configuración del Servidor de administración. Esto requerirá configurar nuevamente Kaspersky Security Center desde el principio y realizar el despliegue inicial del Agente de red en la red de la organización otra vez. Todas las claves principales para el cifrado de unidades en dispositivos administrados también se perderán, arriesgando la pérdida irrevocable de datos cifrados en dispositivos con Kaspersky Endpoint Security. Por tanto, no debe dejar de crear, a intervalos regulares, copias de seguridad del Servidor de administración mediante la tarea de copia de seguridad estándar.

El Asistente de inicio rápido crea la tarea de copia de seguridad para la configuración del Servidor de administración y la configura para que se ejecute diariamente a las 4:00 A.M. Las copias de seguridad se guardan de forma predeterminada en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskySC.

Si se utiliza una instancia de Microsoft SQL Server instalada en otro dispositivo como DBMS, debe modificar la tarea de copia de seguridad al especificar una ruta de UNC, que está disponible para escritura tanto del servicio del Servidor de administración como del servicio de SQL Server, como la carpeta para almacenar copias de seguridad. Este requisito, que no es obvio, deriva de una función especial de copia de seguridad en DBMS de Microsoft SQL Server.

Si se utiliza una instancia local de Microsoft SQL Server como DBMS, también recomendamos guardar copias de seguridad en un medio dedicado a fin de protegerlas contra el daño junto con el Servidor de administración.

Como una copia de seguridad contiene datos importantes, la tarea de copia de seguridad y la utilidad klbackup proporcionan la protección con contraseña de las copias de seguridad. De forma predeterminada, la tarea de creación de copia de seguridad se crea con una contraseña en blanco. Debe configurar una contraseña en las propiedades de la tarea de creación de copia de seguridad. Descuidar este requisito causa una situación donde todas las claves de los certificados del Servidor de administración, las claves para licencias y las claves principales para el cifrado de unidades de disco en los dispositivos administrados permanecen sin cifrar.

Además de la copia de seguridad habitual, también debe crear una copia de seguridad antes de cada cambio significativo, incluida la instalación de actualizaciones y parches del Servidor de administración.

Para minimizar el tamaño de las copias de seguridad, active la opción **Comprimir copia de seguridad** en la configuración de SQL Server.

La restauración desde una copia de seguridad se realiza con la utilidad klbackup en una instancia operable del Servidor de administración que se acaba de instalar y tiene la misma versión (o posterior) para la cual se creó la copia de seguridad.

La instancia del Servidor de administración en el cual se debe realizar la restauración debe utilizar un DBMS del mismo tipo (mismo SQL Server, MySQL o MariaDB) y la misma versión (o una posterior). La versión del Servidor de administración puede ser la misma (con un parche idéntico o posterior) o posterior.

Esta sección describe las situaciones estándares para restaurar la configuración y los objetos del Servidor de administración.

Un dispositivo con el Servidor de administración es inoperable

Si un dispositivo con el Servidor de administración es inoperable debido a una omisión, se recomienda realizar las acciones siguientes:

- Se debe asignar la misma dirección al nuevo Servidor de administración: el nombre NetBIOS, FQDN o IP estática (según cuál de estas opciones se configuró cuando se desplegaron los Agentes de red).

- Instale el Servidor de administración usando un DBMS del mismo tipo, de la misma versión (o posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la configuración inicial a través del Asistente.

- En el menú **Iniciar**, ejecute la utilidad klbackup y realice la restauración.

La configuración del Servidor de administración o la base de datos están dañadas

Si el Servidor de administración es inoperable debido a parámetros o base de datos dañados (por ej., después de una sobretensión), se recomienda usar la situación de restauración siguiente:

1. Analice el sistema de archivos en el dispositivo dañado.

2. Desinstale la versión inoperable del Servidor de administración.

3. Instale nuevamente el Servidor de administración usando un DBMS del mismo tipo y de la misma versión (o posterior). Puede instalar la misma versión del Servidor con el mismo parche (o uno posterior), o una versión posterior. Después de la instalación, no realice la configuración inicial a través del Asistente.

4. En el menú **Iniciar**, ejecute la utilidad klbackup y realice la restauración.

Se prohíbe restaurar el Servidor de administración si no es a través de la utilidad klbackup.

Cualquier intento de restaurar el Servidor de administración mediante software de terceros bloqueará la sincronización de los datos en los nodos de la aplicación distribuida Kaspersky Security Center y, por consiguiente, afectará al funcionamiento correcto de la aplicación.

Despliegue del Agente de red y la aplicación de seguridad

Para administrar dispositivos en una organización, debe instalar el Agente de red en cada uno de ellos. El despliegue de Kaspersky Security Center distribuido en dispositivos corporativos normalmente comienza con la instalación del Agente de red en dichos dispositivos.

En Microsoft Windows XP, el Agente de red podría no realizar las siguientes operaciones correctamente: descargar actualizaciones directamente desde los servidores de Kaspersky (como un punto de distribución); funcionando como Proxy KSN (como un punto de distribución); detectar vulnerabilidades de terceros (si se usa la Administración de vulnerabilidades y parches).

Despliegue inicial

Si el Agente de red ya se ha instalado en un dispositivo, la instalación remota de aplicaciones en ese dispositivo se realiza a través de este Agente de red. El paquete de distribución de una aplicación que se instalará se transfiere mediante canales de comunicación entre Agentes de red y el Servidor de administración, junto con la configuración de la instalación definida por el administrador. Para transferir el paquete de distribución, puede usar nodos de distribución de transferencia, es decir puntos de distribución, entrega de la difusión múltiple, etc. Para obtener más información sobre cómo instalar aplicaciones en dispositivos administrados con el Agente de red ya instalado, consulte a continuación de esta sección.

Puede realizar la configuración inicial del Agente de red en dispositivos que ejecutan Windows usando uno de los métodos siguientes:

- Con herramientas de terceros para la instalación remota de aplicaciones.
- Con directivas de grupo de Windows: usando herramientas de administración de Windows estándar para directivas de grupo.
- En modo forzado, usando opciones especiales en la tarea de instalación remota de Kaspersky Security Center.
- Al enviar a usuarios del dispositivo enlaces con paquetes independientes generados por Kaspersky Security Center. Los paquetes independientes son módulos ejecutables que contienen los paquetes de distribución de las aplicaciones seleccionadas con su configuración definida.
- Manualmente, al ejecutar instaladores de la aplicación en dispositivos.

En plataformas que no sean de Microsoft Windows, debe realizar la instalación inicial del Agente de red en los dispositivos administrados mediante las herramientas de terceros existentes, o manualmente, mediante el envío a los usuarios un archivo con un paquete de distribución configurado previamente. Puede actualizar el Agente de red a una nueva versión o instalar otras aplicaciones de Kaspersky en plataformas que no sean Windows, usando Agentes de red (ya instalados en dispositivos) para realizar tareas de instalación remotas. En este caso, la instalación es idéntica a la de los dispositivos con Microsoft Windows instalado.

Al seleccionar un método y una estrategia para el despliegue de aplicaciones en una red administrada, debe considerar varios factores (lista parcial):

- Configuración de la red corporativa.
- Número total de dispositivos.
- La presencia de dominios de Windows en la red administrada, la posibilidad de modificar directivas del grupo de Active Directory en esos dominios.
- El reconocimiento de las cuentas de usuario con derechos de administrador locales en los dispositivos en los que se ha planeado el despliegue inicial de aplicaciones de Kaspersky (es decir, la disponibilidad de una cuenta de usuario de dominio con derechos de administrador locales o la presencia de cuentas de usuario locales unificadas con derechos de administrador en esos dispositivos).
- El tipo de conexión y el ancho de banda de los canales de red entre el Servidor de administración y las redes del cliente MSP, así como el ancho de banda de los canales dentro de esas redes.
- La configuración de seguridad que se aplicó en dispositivos remotos al inicio del despliegue (por ejemplo, el uso de UAC y el modo de uso compartido simple de archivos).

Configuración de instaladores

Antes de iniciar el despliegue de aplicaciones de Kaspersky en una red, debe especificar la configuración de la instalación, es decir, los parámetros definidos durante la instalación de la aplicación. Al instalar el Agente de red, debe especificar, como mínimo, una dirección para la conexión con el Servidor de administración y la configuración del proxy; también se pueden requerir algunos parámetros avanzados. Según el método de instalación que ha seleccionado, puede definir la configuración de formas diferentes. En el caso más sencillo (instalación interactiva manual en un dispositivo seleccionado), toda la configuración relevante puede definirse mediante la interfaz de usuario del instalador, por lo que, en algunos casos, el despliegue inicial incluso puede realizarse mediante el envío a usuarios un enlace al paquete de distribución del Agente de red junto con la configuración (dirección del Servidor de administración, etc.) que el usuario debe introducir en la interfaz del instalador.

Este método no se recomienda para su uso, ya que es inoportuno para los usuarios, dado que implica un alto riesgo de errores al definir la configuración manualmente; además, no puede utilizarse con la instalación silenciosa no interactiva de aplicaciones en grupos del dispositivo. En general, el administrador debe especificar valores para la configuración en el modo centralizado; esos valores se pueden utilizar posteriormente para la creación de paquetes independientes. Los paquetes independientes son archivos de extracción automática que contienen paquetes de distribución con la configuración definida por el administrador. Los paquetes independientes pueden ubicarse en recursos que permiten tanto la descarga por parte de usuarios finales (por ejemplo, en Servidor web de Kaspersky Security Center) como la instalación no interactiva en dispositivos en red seleccionados.

Paquetes de instalación

El primer y más importante método para definir la configuración de la instalación de aplicaciones es de uso múltiple y, por lo tanto, es conveniente para todos los métodos de instalación, tanto con herramientas de Kaspersky Security Center como con la mayor parte de las herramientas de terceros. Este método consiste en crear paquetes de instalación de aplicaciones en Kaspersky Security Center.

Los paquetes de instalación se generan usando los métodos siguientes:

- Automáticamente, desde paquetes de distribución especificados, sobre la base de *descriptores* incluidos (archivos con la extensión kud que contienen reglas para instalación y el análisis de resultados y otra información)

- Desde archivos ejecutables de instaladores o desde instaladores con formato Microsoft Windows Installer (MSI) para aplicaciones estándar o admitidas

Los paquetes de instalación generados se organizan jerárquicamente como carpetas con subcarpetas anidadas y archivos. Además del paquete de distribución original, un paquete de instalación contiene configuración editable (incluida la configuración del instalador y reglas para procesar tales casos como la necesidad de reiniciar el sistema operativo a fin de completar la instalación), así como módulos auxiliares menores.

Los valores de configuración de la instalación que son específicos para que se admita una aplicación seleccionada pueden especificarse en la interfaz de usuario de la Consola de administración al crear un paquete de instalación (encontrará más configuración en las propiedades de un paquete de instalación que ya se ha creado). Al realizar la instalación remota de aplicaciones mediante herramientas de Kaspersky Security Center, se entregan paquetes de instalación a dispositivos de destino de modo que la ejecución del instalador de una aplicación ponga toda la configuración definida por los administradores a disposición. Al usar herramientas de terceros para la instalación de aplicaciones de Kaspersky, solo debe garantizar la disponibilidad del paquete de instalación completo en el dispositivo de destino, es decir, la disponibilidad del paquete de distribución y su configuración. Kaspersky Security Center crea y almacena los paquetes de instalación en una subcarpeta dedicada de la carpeta de datos compartida.

No especifique ningún detalle de cuentas privilegiadas en los parámetros de los paquetes de instalación.

Para obtener instrucciones sobre el uso de este método de configuración para las aplicaciones de Kaspersky antes de el despliegue a través de herramientas de terceros, consulte la sección "Despliegue con directivas de grupo de Microsoft Windows".

Inmediatamente después de la instalación de Kaspersky Security Center, se generan automáticamente algunos paquetes de instalación; están listos para la instalación e incluyen paquetes del Agente de red y paquetes de la aplicación de seguridad para Microsoft Windows.

En algunos casos, la utilización de paquetes de instalación para el despliegue de aplicaciones en una red del cliente MSP implica la necesidad de crear paquetes de instalación en Servidores virtuales que correspondan a clientes MSP. La creación de paquetes de instalación en Servidores virtuales le permite usar diferente configuración de instalación para diferentes clientes MSP. En la primera instancia, esto resulta útil al gestionar paquetes de instalación del Agente de red, ya que los Agentes de red desplegados en las redes de los diferentes clientes MSP utilizan diferentes direcciones para conectarse al Servidor de administración. En realidad, la dirección de conexión determina el Servidor al cual se conecta el Agente de red.

Además de la posibilidad de crear nuevos paquetes de instalación inmediatamente en un Servidor de administración virtual, el modo de operación principal para los paquetes de instalación en Servidores de administración virtuales es la "distribución" de paquetes de instalación del Servidor de administración principal a Servidores de administración virtuales. Puede distribuir paquetes de instalación seleccionados (o todos) a Servidores de administración virtuales seleccionados (incluidos todos los Servidores dentro de un grupo de administración seleccionado) con la tarea del Servidor de administración correspondiente. Además, puede seleccionar la lista de paquetes de instalación del Servidor de administración principal al crear un nuevo Servidor de administración virtual. Los paquetes que ha seleccionado se distribuirán inmediatamente a un Servidor de administración virtual creado recientemente.

Al distribuir un paquete de instalación, su contenido no se copia completamente. El repositorio del archivo en un Servidor de administración virtual, que corresponde al paquete de instalación que se distribuye, solo almacena archivos de la configuración específica de ese Servidor virtual. La parte principal del paquete de instalación (incluido el paquete de distribución de la aplicación que se instala) permanece sin alterar; solo se almacena en el repositorio del Servidor de administración principal. Esto le permite aumentar el rendimiento del sistema drásticamente y reducir el volumen de disco requerido. Al gestionar paquetes de instalación distribuidos a Servidores de administración virtuales (es decir, al ejecutar tareas de instalación remotas o crear paquetes de instalación independientes), los datos del paquete de instalación original del Servidor de administración principal "se fusionan" con los archivos de configuración, que corresponden al paquete distribuido en el Servidor de administración virtual.

Aunque la clave de licencia para una aplicación puede configurarse en las propiedades del paquete de instalación, es aconsejable evitar este método de distribución de la licencia, ya que es sencillo obtener accidentalmente acceso de lectura a los archivos en la carpeta. Debe usar claves de licencia distribuidas automáticamente o tareas de instalación para claves de licencia.

Propiedades de MSI y archivos de transformación

Otra forma de configurar la instalación en la plataforma de Windows es definir propiedades MSI y archivos de transformación. Este método puede utilizarse al realizar la instalación mediante herramientas de terceros destinadas para instaladores en el formato de Microsoft Installer, así como al realizar la instalación mediante directivas de grupo de Windows usando herramientas de Microsoft estándares u otras herramientas de terceros diseñadas para gestionar directivas de grupo de Windows.

Despliegue con herramientas de terceros para la instalación remota de aplicaciones

Cuando están disponibles herramientas para la instalación remota de aplicaciones (por ejemplo, Microsoft System Center) en una organización, es cómodo realizar el despliegue inicial usando estas herramientas.

Se deben realizar las acciones siguientes:

- Seleccione el método para configurar la instalación que se adapte mejor a la herramienta de despliegue que se utilizará.
- Defina el mecanismo para la sincronización entre la modificación de la configuración de los paquetes de instalación (a través de la interfaz de la Consola de administración) y el funcionamiento de herramientas de terceros seleccionadas usadas para el despliegue de aplicaciones desde datos del paquete de instalación.

Información general sobre las tareas de instalación remota en Kaspersky Security Center

Kaspersky Security Center proporciona una amplia variedad de métodos para la instalación remota de aplicaciones, que se implementan como tareas de instalación remota. Puede crear una tarea de instalación remota tanto para un grupo de administración específico como para dispositivos específicos o una selección de dispositivos (tales tareas se muestran en la Consola de administración, en la carpeta **Tareas**). Al crear una tarea, puede seleccionar paquetes de instalación (los del Agente de red u otra aplicación) para que se instalen con esta tarea, así como especificar determinada configuración que defina el método de instalación remota.

Las tareas para grupos de administración afectan ambos dispositivos incluidos en un grupo específico y todos los dispositivos en todos los subgrupos dentro de ese grupo de administración. Una tarea abarca dispositivos de Servidores de administración secundarios incluidos en un grupo o cualquiera de sus subgrupos si el parámetro correspondiente está activado en la tarea.

Las tareas para dispositivos específicos actualizan la lista de dispositivos cliente en cada ejecución de acuerdo con el contenido de la selección en el momento en que se inicia la tarea. Si una selección incluye dispositivos que se han conectado a Servidores de administración secundarios, la tarea también se ejecutará en esos dispositivos.

Para garantizar el funcionamiento correcto de una tarea de instalación remota en dispositivos conectados a Servidores de administración secundarios, debe usar la tarea de distribución para distribuir paquetes de instalación utilizados por su tarea a los Servidores de administración secundarios correspondientes de antemano.

Despliegue con directivas de grupo de Microsoft Windows

Se recomienda que realice el despliegue inicial de Agentes de red a través de directivas de grupo de Microsoft Windows si se cumplen las condiciones siguientes:

- Este dispositivo pertenece al dominio de Active Directory.
- El acceso al controlador de dominio se concede con los derechos de administrador, que le permiten crear y modificar directivas del grupo de Active Directory.
- Los paquetes de instalación configurados pueden moverse a la red que aloja los dispositivos administrados (a una carpeta compartida que está disponible para su lectura para todos los dispositivos de destino).
- El esquema de despliegue le permite esperar el siguiente reinicio rutinario de los dispositivos de destino antes del despliegue inicial de los Agentes de red en ellos (o puede forzar que se aplique una directiva de grupo de Windows en esos dispositivos).

Este esquema de despliegue consiste en lo siguiente:

- El paquete de distribución de aplicación con formato de Microsoft Installer (paquete MSI) se ubica en una carpeta compartida (una carpeta donde las cuentas de LocalSystem de dispositivos de destino tienen permisos de lectura).

- En la directiva de grupo de Active Directory, se crea un objeto de instalación para el paquete de distribución.

- La cobertura de instalación se configura al especificar la unidad organizativa (OU) o el grupo de seguridad, que incluye los dispositivos de destino.

- La próxima vez un dispositivo de destino inicia sesión en el dominio (antes de que los usuarios del dispositivo inicien sesión en el sistema), todas las aplicaciones instaladas se examinan para comprobar la presencia de la aplicación requerida. Si la aplicación no se encuentra, el paquete de distribución se descarga desde el recurso especificado en la directiva y, luego, se instala.

Una ventaja de este esquema de despliegue consiste en que las aplicaciones asignadas se instalan en dispositivos de destino mientras el sistema operativo se está cargando, es decir, incluso antes de que el usuario inicie sesión en el sistema. Aun si un usuario con derechos suficientes elimina la aplicación, esta se instalará de nuevo en el siguiente lanzamiento del sistema operativo. El defecto de este esquema de despliegue es que los cambios hechos por el administrador a la directiva de grupo no entrarán en vigor hasta que los dispositivos se reinicien (si no se involucra ninguna herramienta avanzada).

Puede usar directivas de grupo para instalar tanto el Agente de red como otras aplicaciones si sus respectivos instaladores tienen el formato de Windows Installer.

Asimismo, cuando selecciona este método de despliegue, también debe evaluar la carga en el recurso de archivo del cual se copiarán los archivos a los dispositivos de destino después de aplicar la directiva de grupo de Windows. También debe elegir el método de entrega del paquete de instalación configurado a ese recurso, así como el método de sincronización de los cambios relevantes en su configuración.

Administración de directivas de Microsoft Windows mediante la tarea de instalación remota de Kaspersky Security Center

Este método de despliegue solo está disponible si es posible acceder al controlador de dominio, que contiene los dispositivos de destino, desde el dispositivo del Servidor de administración, mientras que la carpeta compartida del Servidor de administración (el que almacena los paquetes de instalación) es accesible para su lectura desde dispositivos de destino. Debido a los motivos indicados anteriormente, este método de despliegue no se considera aplicable al MSP.

Instalación no asistida de aplicaciones mediante directivas de Microsoft Windows

El administrador puede crear objetos requeridos para la instalación en una directiva de grupo de Windows en su propio nombre. En este caso, debe cargar los paquetes a un servidor de archivos independiente y proporcionar un enlace a ellos.

Pueden producirse las siguientes situaciones de instalación:

- El administrador crea un paquete de instalación y configura sus propiedades en la Consola de administración. A continuación, el administrador copia la subcarpeta EXEC completa de este paquete desde la carpeta compartida de Kaspersky Security Center a una carpeta en un recurso de archivo dedicado de la organización. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en una subcarpeta en el recurso de archivo dedicado de la organización.

- El administrador descarga el paquete de distribución de aplicaciones (incluido el del Agente de red) de Internet y lo carga al recurso de archivo dedicado de la organización. El objeto de la directiva de grupo proporciona un enlace al archivo MSI de este paquete almacenado en una subcarpeta en el recurso de archivo dedicado de la

organización. La configuración de la instalación se define al configurar las propiedades MSI o al configurar archivos de transformación MST.

Despliegue forzado mediante la tarea de instalación remota de Kaspersky Security Center

Para realizar el despliegue inicial de Agentes de red u otras aplicaciones, puede forzar la instalación de paquetes de instalación seleccionados usando la tarea de instalación remota de Kaspersky Security Center — a condición de que todos los dispositivos tengan una cuenta o cuentas de usuario con derechos de administrador local y que al menos un dispositivo con el Agente de red instalado actúe como punto de distribución en cada subred.

En este caso, puede especificar dispositivos de destino ya sea explícitamente (con una lista) o al seleccionar el grupo de administración de Kaspersky Security Center al cual pertenecen, o al crear una selección de dispositivos basada en un criterio específico. El tiempo del inicio de la instalación es definido por la programación de la tarea. Si el parámetro **Ejecutar tareas no realizadas** está activado en las propiedades de la tarea, la tarea se puede ejecutar inmediatamente después de que se enciendan los dispositivos de destino o cuando se muevan al grupo de administración de destino.

La instalación forzada consiste en la entrega de paquetes de instalación a puntos de distribución, la copia subsecuente de archivos al recurso de admin$ en cada uno de los dispositivos de destino y el registro remoto de los servicios de compatibilidad en esos dispositivos. La entrega de paquetes de instalación a puntos de distribución se realiza mediante una función de Kaspersky Security Center que garantiza la interacción de la red. Las siguientes condiciones deben cumplirse en este caso:

- Los dispositivos de destino son accesibles desde el lado del punto de distribución.
- La resolución del nombre para los dispositivos de destino funciona correctamente en la red.
- Los usos compartidos administrativos (admin$) permanecen activados en los dispositivos de destino.
- El servicio del sistema del Servidor se ejecuta en los dispositivos de destino (de manera predeterminada, se está ejecutando).
- Los siguientes puertos están abiertos en los dispositivos de destino para permitir el acceso remoto a través de las herramientas de Windows: TCP 139, TCP 445, UDP 137 y UDP 138.
- En los dispositivos de destino que ejecutan Microsoft Windows XP, el modo de uso compartido sencillo de archivos está desactivado.
- En los dispositivos de destino, el modelo de acceso compartido y seguridad se configura como *Clásico: los usuarios locales se autentican como ellos mismos*, no puede ser de ninguna manera *Solo invitados: los usuarios locales se autentican como invitados*.
- Los dispositivos de destino son miembros del dominio, o bien se crean cuentas uniformes con derechos de administrador en los dispositivos de destino de antemano.

Los dispositivos en los grupos de trabajo pueden ajustarse de acuerdo con los requisitos indicados anteriormente usando la utilidad riprep.exe, que se describe en el sitio web del Servicio de soporte técnico de Kaspersky.

Durante la instalación en nuevos dispositivos que todavía no se han asignado a ninguno de los grupos de administración de Kaspersky Security Center, puede abrir las propiedades de la tarea de instalación remota y especificar el grupo de administración al cual se moverán los dispositivos después de la instalación del Agente de red.

Al crear una tarea de grupo, tenga en cuenta que cada tarea de grupo afecta todos los dispositivos en todos los grupos anidados dentro de un grupo seleccionado. Por lo tanto, debe evitar duplicar las tareas de instalación en los subgrupos.

La instalación automática es una forma simplificada de crear tareas para la instalación forzada de aplicaciones. Para hacer esto, abra las propiedades del grupo de administración, abra la lista de paquetes de instalación y seleccione los que deben instalarse en los dispositivos en este grupo. Como resultado, los paquetes de instalación seleccionados se instalarán automáticamente en todos los dispositivos en este grupo y todos sus subgrupos. El intervalo de tiempo durante el cual los paquetes se instalarán depende del rendimiento de la red y del número total de dispositivos en red.

Para permitir la instalación forzada, debe asegurarse de que los puntos de distribución estén presentes en cada una de las subredes aisladas que alojan dispositivos de destino.

Tenga en cuenta que este método de instalación coloca una carga significativa en los dispositivos que funcionan como puntos de distribución. Por lo tanto, se recomienda que seleccione dispositivos eficaces con unidades de almacenamiento de alto rendimiento como puntos de distribución. Además, el espacio disponible en disco en la partición con la carpeta *%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit* debe superar, por muchas veces, el tamaño total de los paquetes de distribución de las aplicaciones instaladas.

La ejecución de paquetes independientes creada por Kaspersky Security Center

Los métodos descritos anteriormente de despliegue inicial del Agente de red y otras aplicaciones no siempre pueden implementarse porque no es posible cumplir todas las condiciones aplicables. En tales casos, puede crear un archivo ejecutable común llamado un *paquete de instalación independiente* a través de Kaspersky Security Center, usando paquetes de instalación con la configuración de la instalación relevante que hayan sido preparados por el administrador. Un paquete de instalación independiente puede publicarse en un Servidor web interno (incluido en Kaspersky Security Center) si esto se considera razonable (se configuró el acceso externo a ese Servidor web para usuarios de dispositivos de destino), o en un Servidor web desplegado exclusivamente incluido en Kaspersky Security Center 14 Web Console. También puede copiar paquetes independientes a otro Servidor web.

Puede usar Kaspersky Security Center para enviar a usuarios seleccionados un mensaje de correo electrónico que contenga un enlace al archivo del paquete independiente en el Servidor web que se utilice actualmente, solicitándoles ejecutar el archivo (ya sea en modo interactivo o con la clave "-s" para la instalación silenciosa). Puede adjuntar el paquete de instalación independiente a un mensaje de correo electrónico y luego enviarlo a los usuarios de dispositivos que no tengan acceso al Servidor web. El administrador también puede copiar el paquete independiente a un dispositivo externo, entregarlo a un dispositivo relevante y luego ejecutarlo más adelante.

Puede crear un paquete independiente a partir de un paquete del Agente de red, un paquete de otra aplicación (por ejemplo, la aplicación de seguridad), o ambos. Si el paquete independiente se ha creado a partir de un Agente de red y otra aplicación, la instalación comienza con el Agente de red.

Al crear un paquete independiente con el Agente de red, puede especificar el grupo de administración al cual se moverán automáticamente los nuevos dispositivos (los que no hayan sido asignados a ninguno de los grupos de administración) cuando la instalación del Agente de red se complete en ellos.

Los paquetes independientes pueden ejecutarse en modo interactivo (de forma predeterminada), mostrando el resultado para la instalación de las aplicaciones que contienen, o pueden ejecutarse en modo silencioso (cuando se ejecutan con la clave "-s"). El modo silencioso puede utilizarse para la instalación a partir de scripts, por ejemplo, de scripts configurados para ejecutarse después de que se despliega una imagen del sistema operativo. El resultado de la instalación en modo silencioso está determinado por el código de devolución del proceso.

Opciones para la instalación manual de aplicaciones

Los administradores o los usuarios experimentados pueden instalar aplicaciones manualmente en modo interactivo. Pueden usar paquetes de distribución originales o paquetes de instalación generados a partir de ellos y almacenados en la carpeta compartida de Kaspersky Security Center. De forma predeterminada, los instaladores se ejecutan en modo interactivo y solicitan a los usuarios todos los valores requeridos. Sin embargo, al ejecutar el proceso setup.exe desde la raíz de un paquete de instalación con la clave "-s", el instalador se ejecutará en modo silencioso y con la configuración que se haya definido al configurar el paquete de instalación.

Al ejecutar setup.exe desde la raíz de un paquete de instalación, el paquete se copiará primero a una carpeta local temporal y, luego, el instalador de la aplicación se ejecutará desde la carpeta local.

Instalación remota de aplicaciones en dispositivos con el Agente de red instalado

Si el Agente de red operable conectado al Servidor de administración principal (o a alguno de sus Servidores secundarios) está instalado en un dispositivo, puede actualizar el Agente de red en este dispositivo, así como instalar, actualizar o eliminar cualquier aplicación admitida a través del Agente de red.

Puede activar esta opción seleccionando la casilla de verificación **Usar el Agente de red** en las propiedades de la tarea de instalación remota.

Si esta casilla está seleccionada, los paquetes de instalación con la configuración de la instalación definida por el administrador se transferirán a los dispositivos de destino mediante canales de comunicación entre el Agente de red y el Servidor de administración.

Para optimizar la carga en el Servidor de administración y minimizar el tráfico entre el Servidor de administración y los dispositivos, es útil asignar puntos de distribución en cada red remota o en cada dominio de difusión (consulte las secciones Acerca de los puntos de distribución y Creación de una estructura de grupos de administración y asignación de puntos de distribución). En este caso, los paquetes de instalación y la configuración del instalador se distribuyen desde el Servidor de administración a los dispositivos de destino a través de puntos de distribución.

Asimismo, puede usar puntos de distribución para la entrega por difusión (multidifusión) de paquetes de instalación, que permite reducir el tráfico de red considerablemente al desplegar aplicaciones.

Al transferir paquetes de instalación a dispositivos de destino sobre canales de comunicación entre Agentes de red y el Servidor de administración, todos los paquetes de instalación que se han preparado para la transferencia también se ocultarán en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Al usar varios paquetes de instalación grandes de diversos tipos e implicar un gran número de puntos de distribución, el tamaño de esta carpeta puede aumentar drásticamente.

Los archivos no pueden eliminarse de la carpeta FTServer manualmente. Cuando los paquetes de instalación originales se eliminen, los datos correspondientes se eliminarán automáticamente de la carpeta FTServer.

Todos los datos recibidos en el lado de los puntos de distribución se guardan en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Los archivos no pueden eliminarse de la carpeta $FTCITmp manualmente. A medida que las tareas que usan datos de esta carpeta se completan, el contenido de esta carpeta se elimina automáticamente.

Como los paquetes de instalación se distribuyen por canales de comunicación entre el Servidor de administración y los Agentes de red desde un repositorio intermedio en un formato optimizado para las transferencias de red, no se permiten cambios en los paquetes de instalación almacenados en la carpeta original de cada paquete de instalación. Esos cambios no serán registrados automáticamente por el Servidor de administración. Si debe modificar los archivos de los paquetes de instalación manualmente (aunque se recomienda evitar esta situación), debe modificar la configuración de un paquete de instalación en la Consola de administración. La modificación de la configuración de un paquete de instalación en la Consola de administración hace que el Servidor de administración actualice la imagen del paquete en el caché que se ha preparado para la transferencia a los dispositivos de destino.

Administración de reinicios de dispositivos en la tarea de instalación remota

Los dispositivos a menudo deben reiniciarse para completar la instalación remota de aplicaciones (en particular, en Windows).

Si usa la tarea de instalación remota de Kaspersky Security Center, en el Asistente para añadir tareas o en la ventana de propiedades de la tarea que se ha creado (sección **Reinicio del sistema operativo**), puede seleccionar la acción para realizar cuando se requiera un reinicio:

- **No reiniciar el dispositivo**. En este caso, no se realizará ningún reinicio automático. Para completar la instalación, debe reiniciar el dispositivo (por ejemplo, manualmente o a través de la tarea de administración del dispositivo). La información sobre el reinicio requerido se guardará en los resultados de la tarea y en el estado del dispositivo. Esta opción es conveniente para las tareas de instalación en servidores y otros dispositivos donde la operación continua es crítica.

- **Reiniciar el dispositivo**. En este caso, el dispositivo siempre se reinicia automáticamente si se requiere un reinicio para la finalización de la instalación. Esta opción es útil para las tareas de instalación en dispositivos que ofrecen pausas habituales en su funcionamiento (cierre o reinicio).

- **Solicitar al usuario una acción**. En este caso, en la pantalla del dispositivo cliente se mostrará el recordatorio de reinicio para que el usuario lo reinicie manualmente. Es posible definir parte de la configuración avanzada para esta opción: el texto del mensaje para el usuario, la frecuencia de la visualización del mensaje y el intervalo de tiempo después del cual se forzará el reinicio (sin la confirmación del usuario). La opción **Solicitar al usuario una acción** es la más conveniente para las estaciones de trabajo donde los usuarios necesitan la posibilidad de seleccionar la hora más cómoda para un reinicio.

Conveniencia de la actualización de bases de datos en un paquete de instalación de una aplicación antivirus

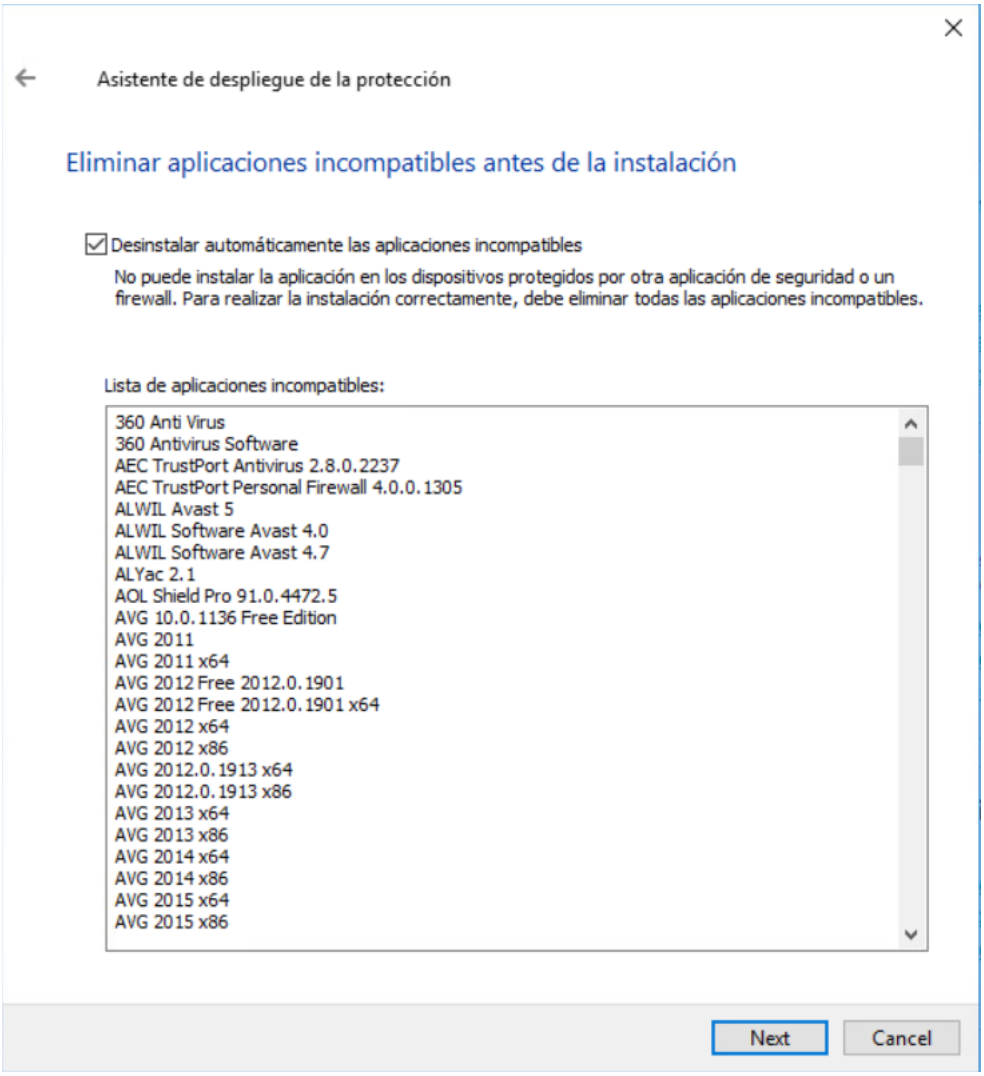
Antes de iniciar el despliegue de la protección, debe tener en cuenta la posibilidad de actualizar las bases de datos antivirus (incluidos los módulos de los parches automáticos) que se envían junto con el paquete de distribución de la aplicación de seguridad. Es útil actualizar las bases de datos en el paquete de instalación de la aplicación antes de iniciar el despliegue (por ejemplo, usando el comando correspondiente en el menú contextual de un paquete de instalación seleccionado). Esto reducirá el número de reinicios requeridos para la finalización del despliegue de la protección en los dispositivos de destino. Si su instalación remota involucra paquetes de instalación que se han transmitido a Servidores virtuales desde el Servidor de administración principal, solo debe actualizar las bases de datos en el paquete original en el Servidor del principal. En este caso, no es necesario que actualice bases de datos en paquetes transmitidos en Servidores virtuales.

Eliminación de las aplicaciones de seguridad de terceros incompatibles

La Instalación de aplicaciones de seguridad de Kaspersky a través de Kaspersky Security Center puede requerir la eliminación del software de terceros incompatible con la aplicación instalada. Existen dos formas principales de eliminar las aplicaciones de terceros.

Eliminación automática de aplicaciones incompatibles con el instalador

Al ejecutar el instalador, muestra una lista de aplicaciones incompatibles con una aplicación de Kaspersky:



La lista de aplicaciones incompatibles que aparece en el Asistente de instalación remota

Kaspersky Security Center detecta software incompatible. Por tanto, puede seleccionar la casilla de verificación **Desinstalar automáticamente las aplicaciones incompatibles** para continuar con la instalación. Si desactiva esta casilla de verificación y no desinstala el software incompatible, se produce el error y la aplicación de Kaspersky no se instala.

La eliminación automática de aplicaciones incompatibles es compatible con varios tipos de instalación.

Eliminación de aplicaciones incompatibles mediante una tarea dedicada

Para eliminar las aplicaciones incompatibles, use la tarea *Desinstalar aplicación en remoto*. Esta tarea debería ejecutarse en dispositivos antes de la tarea de instalación de la aplicación de seguridad. Por ejemplo, en la tarea de instalación, puede seleccionar el tipo de la programación **Al completar otra tarea**, donde la otra tarea es *Desinstalar aplicación en remoto*.

Este método de desinstalación es útil cuando el instalador de la aplicación de seguridad no puede eliminar correctamente una aplicación incompatible.

Utilización de herramientas para la instalación remota de aplicaciones en Kaspersky Security Center para ejecutar archivos ejecutables relevantes en dispositivos administrados

Con el Asistente de nuevo paquete, puede seleccionar cualquier archivo ejecutable y definir la configuración de la línea de comandos para este. Para hacerlo, puede añadir al paquete de instalación el propio archivo seleccionado o la carpeta completa en la cual se almacena este archivo. Luego, debe crear la tarea de instalación remota y seleccionar el paquete de instalación que se ha creado.

Mientras la tarea se está ejecutando, el archivo ejecutable especificado con la configuración definida de la solicitud de comando se ejecutará en los dispositivos de destino.

Si usa instaladores con formato Microsoft Windows Installer (MSI), Kaspersky Security Center analiza los resultados de instalación por medio de herramientas estándar.

Si está disponible una licencia de Administración de vulnerabilidades y parches, Kaspersky Security Center (al crear un paquete de instalación para cualquier aplicación admitida en el entorno corporativo) también usa reglas para la instalación y el análisis de los resultados de la instalación que están en su base de datos que se actualiza.

De otro modo, la tarea predeterminada para los archivos ejecutables espera la finalización del proceso en ejecución y de todos sus procesos secundarios. Después de la finalización de todos los procesos en ejecución, la tarea se completará correctamente independientemente del código de devolución del proceso inicial. Para cambiar tal comportamiento de esta tarea, antes de crear la tarea, debe modificar manualmente los archivos .kpd generados por Kaspersky Security Center en la carpeta del paquete de instalación recientemente creada.

Para que la tarea no espere la finalización del proceso en ejecución, configure el valor del parámetro Wait en 0 en la sección [SetupProcessResult]:

```
Ejemplo:
[SetupProcessResult]
Wait=0
```

Para que la tarea solo espere la finalización del proceso en ejecución en Windows, no la finalización de todos los procesos secundarios, configure el valor del parámetro WaitJob en 0 en la sección [SetupProcessResult], por ejemplo:

```
Ejemplo:
[SetupProcessResult]
WaitJob=0
```

Para que la tarea se complete correctamente o devuelva un error según el código de devolución del proceso en ejecución, enumere los códigos de devolución correctos en [SetupProcessResult_SuccessCodes], sección, por ejemplo:

```
Ejemplo:
[SetupProcessResult_SuccessCodes]
0=
3010=
```

En este caso, cualquier código además de los enumerados causará la devolución de un error.

Para que se muestre una cadena con un comentario sobre la finalización correcta de la tarea o un error en los resultados de la tarea, introduzca breves descripciones de los errores que correspondan a códigos de devolución del proceso en las secciones [SetupProcessResult_SuccessCodes] y [SetupProcessResult_ErrorCodes], por ejemplo:

Ejemplo:

[SetupProcessResult_SuccessCodes]

0=La instalación ha finalizado correctamente

3010=Se requiere un reinicio para completar la instalación

[SetupProcessResult_ErrorCodes]

1602=La instalación fue cancelada por el usuario

1603=Error grave durante la instalación.

Para usar herramientas de Kaspersky Security Center para administrar el reinicio del dispositivo (si se requiere un reinicio para completar una operación), enumere los códigos de devolución del proceso que indican que se debe realizar un reinicio, en la sección [SetupProcessResult_NeedReboot]:

Ejemplo:

[SetupProcessResult_NeedReboot]

3010=

Supervisión del despliegue

Para supervisar el despliegue de Kaspersky Security Center y asegurarse de que una aplicación de seguridad y el Agente de red estén instalados en los dispositivos administrados, debe comprobar el semáforo en la sección **Despliegue**. Este semáforo se localiza en el espacio de trabajo del nodo del Servidor de administración en la ventana principal de Consola de administración. El semáforo refleja el estado de despliegue actual. El número de dispositivos con el Agente de red y la aplicación de seguridad instalados se muestra al lado del semáforo. Cuando se está ejecutando una tarea de instalación, puede supervisar su progreso aquí. Si ocurre algún error de instalación, el número de errores se muestra aquí. Puede ver los detalles de cualquier error haciendo clic en el enlace.

También puede usar el gráfico de despliegue en el espacio de trabajo de la carpeta **Dispositivos administrados** en la pestaña **Grupos**. El gráfico refleja el proceso de despliegue y muestra el número de dispositivos sin el Agente de red, con el Agente de red o con el Agente de red y una aplicación de seguridad.

Para obtener más información sobre el progreso del despliegue (o el funcionamiento de una tarea de instalación específica), abra la ventana de resultados de la tarea de instalación remota relevante: haga clic con el botón secundario del ratón en la tarea y seleccione **Resultados** el menú contextual. La ventana muestra dos listas: la superior contiene los estados de la tarea en los dispositivos, mientras que la inferior contiene los eventos de la tarea en el dispositivo que está seleccionado actualmente en la lista superior.

Se añade información sobre los errores de despliegue en el Registro de eventos de Kaspersky en el Servidor de administración. La información sobre errores también está disponible en la selección correspondiente de eventos en la carpeta **Informes y notificaciones**, la subcarpeta **Eventos**.

Configuración de instaladores

Esta sección proporciona información sobre los archivos de los instaladores de Kaspersky Security Center y la configuración de la instalación, así como recomendaciones sobre cómo instalar el Servidor de administración y el Agente de red en modo silencioso.

Información general

Los instaladores de los componentes de Kaspersky Security Center 14 (Servidor de administración, Agente de red y Consola de administración) utilizan la tecnología de Windows Installer. Un paquete MSI es el núcleo de un instalador. Este formato de paquete permite usar todas las ventajas proporcionadas por Windows Installer: la escalabilidad, la disponibilidad de un sistema de parches, el sistema de transformación, la instalación centralizada a través de soluciones de terceros y el registro transparente con el sistema operativo.

Instalación en modo silencioso (con un archivo de respuesta)

Los instaladores del Servidor de administración y el Agente de red tienen la función de trabajar con el archivo de respuesta (ss_install.xml), donde está integrada la parámetros para la instalación en modo silencioso sin la participación del usuario. El archivo ss_install.xml se ubica en la misma carpeta que el paquete MSI; se utiliza automáticamente durante la instalación en modo silencioso. Puede habilitar el modo de instalación silenciosa con la clave de línea de comando "/s".

A continuación, se proporciona una descripción general de una ejecución de ejemplo:

```
setup.exe /s
```

El archivo ss_install.xml es una instancia del formato interno de la parámetros del instalador de Kaspersky Security Center. Los paquetes de distribución contienen el archivo ss_install.xml con la parámetros predeterminada.

> No modifique ss_install.xml manualmente. Este archivo puede modificarse mediante las herramientas de Kaspersky Security Center al modificar la parámetros de los paquetes de instalación en la Consola de administración.

Instalación del Agente de red en modo silencioso (sin un archivo de respuesta)

Puede instalar el Agente de red con un único paquete msi, especificando los valores de las propiedades MSI de la forma estándar. Esta situación permite que el Agente de red se instale usando directivas de grupo. Para evitar conflictos entre los parámetros definida mediante las propiedades MSI y los parámetros definida en el archivo de respuesta, puede desactivar el archivo de respuesta al configurar la propiedad `DONT_USE_ANSWER_FILE=1`. A continuación, se especifica un ejemplo de una ejecución del instalador del Agente de red con un paquete msi.

La instalación del Agente de red en modo no interactivo requiere la aceptación de las condiciones del Contrato de licencia de usuario final. Utilice el parámetro `EULA=1` solo si ha leído, y entiende y acepta todas las condiciones del Contrato de licencia de usuario final.

Ejemplo:

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

También puede definir los parámetros de la instalación para un paquete msi al preparar el archivo de respuesta de antemano (uno con la extensión mst). Este comando aparece de la forma siguiente:

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

Puede especificar varios archivos de respuesta en un solo comando.

Configuración de la instalación parcial a través de setup.exe

Al ejecutar la instalación de aplicaciones mediante setup.exe, puede añadir los valores de cualquiera de las propiedades de MSI al paquete MSI.

Este comando aparece de la forma siguiente:

Ejemplo:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parámetros de la instalación del Servidor de administración

La siguiente tabla describe las propiedades MSI que puede configurar al instalar el Servidor de administración. Toda los parámetros es opcional, excepto EULA y PRIVACYPOLICY.

Parámetros de la instalación del Servidor de administración en modo no interactivo

Propiedad de MSI	Descripción	Valores disponibles
EULA	Aceptación de las condiciones del Contrato de licencia (requerido)	• 1: He leído, y entiendo y acepto todas las condiciones del Contrato de licencia de usuario final. • Otro valor o sin valor: no acepto las condiciones del Contrato de licencia (no se realiza la instalación).
PRIVACYPOLICY	Aceptación de las condiciones de la Política de privacidad (requerido)	• 1: Entiendo y acepto que todos mis datos serán manejados y transmitidos (incluso a terceros países) como se describe en la Política de privacidad. Confirmo que he leído y entendido completamente la Política de privacidad. • Otro valor o sin valor: No acepto las condiciones de la Política de privacidad (no se realiza la instalación).
INSTALLATIONMODETYPE	Tipo de instalación del Servidor de administración	• Estándar. • Personalizada.
INSTALLDIR	Carpeta de instalación de la aplicación	Valor de cadena.
ADDLOCAL	Lista de componentes para	CSAdminKitServer, NAgent,

	instalar (separados por comas)	CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Lista mínima de componentes suficientes para la instalación apropiada del Servidor de administración: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Tamaño de la red	• NRT_1_100: de 1 a 100 dispositivos. • NRT_100_1000: De 101 a 1000 dispositivos. • NRT_GREATER_1000: más de 1000 dispositivos. Este parámetro confirma que ha leído, entiende y acepta todas las condiciones del Contrato de licencia de usuario final.
SRV_ACCOUNT_TYPE	Forma de especificar el usuario para el funcionamiento del servicio del Servidor de administración	• SrvAccountDefault: La cuenta de usuario se creará automáticamente. • SrvAccountUser: La cuenta de usuario se define manualmente.
SERVERACCOUNTNAME	Nombre de usuario para el servicio	Valor de cadena.
SERVERACCOUNTPWD	Contraseña de usuario para el servicio	Valor de cadena.
DBTYPE	Tipo de la base de datos	• MySQL: se utilizará una base de datos MySQL o MariaDB. • MSSQL: se utilizará una base de datos Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Nombre completo del servidor MySQL o MariaDB	Valor de cadena.
MYSQLSERVERPORT	Número de puerto para la conexión al servidor MySQL o MariaDB	Valor numérico.
MYSQLDBNAME	Nombre de la base de datos del servidor MySQL o MariaDB	Valor de cadena.
MYSQLACCOUNTNAME	Nombre de usuario para la conexión con la base de datos del servidor MySQL o MariaDB	Valor de cadena.

MYSQLACCOUNTPWD	Contraseña de usuario para la conexión con la base de datos del servidor MySQL o MariaDB	Valor de cadena.
MSSQLCONNECTIONTYPE	Tipo de uso de la base de datos de MSSQL	• InstallMSSEE: Instalar desde un paquete. • ChooseExisting: Usar el servidor instalado.
MSSQLSERVERNAME	Nombre completo de la instancia de SQL Server	Valor de cadena.
MSSQLDBNAME	Nombre de la base de datos de SQL Server	Valor de cadena.
MSSQLAUTHTYPE	Método de autenticación para la conexión con SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nombre de usuario para la conexión con SQL Server en modo SQLServer	Valor de cadena.
MSSQLACCOUNTPWD	Contraseña de usuario para la conexión con SQL Server en modo SQLServer	Valor de cadena.

CREATE_SHARE_TYPE	Método de especificación de la carpeta compartida	• Create: Cree una nueva carpeta compartida. En este caso, se deben definir las propiedades siguientes:
		  • SHARELOCALPATH: Ruta a una carpeta local.
		  • SHAREFOLDERNAME: Nombre de red de una carpeta.
		• Null: La propiedad de EXISTSHAREFOLDERNAME se debe especificar.

EXISTSHAREFOLDERNAME	Ruta completa a una carpeta compartida existente	Valor de cadena.
SERVERPORT	Número de puerto para conectar con el Servidor de administración	Valor numérico.
SERVERSSLPORT	Número de puerto para establecer la conexión SSL al Servidor de administración	Valor numérico.
SERVERADDRESS	Dirección de Servidor de administración	Valor de cadena.
SERVERCERT2048BITS	Tamaño de la clave del certificado del Servidor de administración (bits)	• 1: El tamaño de la clave del certificado del Servidor de administración es de 2048

		bits. • 0: El tamaño de la clave del certificado del Servidor de administración es de 1024 bits. • Si no se especifica ningún valor, el tamaño de la clave del certificado del Servidor de administración es de 1.024 bits.
MOBILESERVERADDRESS	Dirección del Servidor de administración para la conexión de dispositivos móviles; se ignora si no se ha seleccionado el componente MobileSupport	Valor de cadena.

Parámetros de la instalación del Agente de red

La siguiente tabla describe las propiedades MSI que puede configurar al instalar el Agente de red. Toda los parámetros es opcional, excepto EULA y SERVERADDRESS.

Parámetros de la instalación del Agente de red en modo no interactivo

Propiedad de MSI	Descripción	Valores disponibles
EULA	Aceptación de las condiciones del Contrato de licencia	• 1: He leído, y entiendo y acepto todas las condiciones del Contrato de licencia de usuario final. • 0—I: No acepto los términos del Contrato de licencia (no se realiza la instalación). • Sin valor: No acepto las condiciones del Contrato de licencia (no se realiza la instalación).
DONT_USE_ANSWER_FILE	Leer la configuración de la instalación del archivo de respuesta	• 1—No utilizar. • Otro valor o ningún valor—Leer.
INSTALLDIR	Ruta a la carpeta de instalación del Agente de red	Valor de cadena.
SERVERADDRESS	Dirección del Servidor de administración (requerida)	Valor de cadena.
SERVERPORT	Número de un puerto para la conexión al Servidor de administración	Valor numérico.
SERVERSSLPORT	Número del puerto para conexión cifrada	Valor numérico.

	al Servidor de administración usando el protocolo SSL	
USESSL	Si se debe utilizar una conexión SSL	• 1: Utilizar. • Otro valor o ningún valor: No utilizar.
OPENUDPPORT	Si se debe abrir un puerto UDP	• 1: Abrir. • Otro valor o ningún valor: No abrir.
UDPPORT	Número de puerto UDP	Valor numérico.
USEPROXY	Si se debe utilizar un servidor proxy	• 1: Utilizar. • Otro valor o ningún valor: No utilizar.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Dirección del proxy y número de puerto para la conexión con el servidor proxy	Valor de cadena.
PROXYLOGIN	Contraseña para la conexión a un servidor proxy	Valor de cadena.
PROXYPASSWORD	Contraseña de la cuenta para la conexión a un servidor proxy (no especifique ningún detalle de las cuentas privilegiadas en los parámetros de los paquetes de instalación).	Valor de cadena.
GATEWAYMODE	Modo de uso de la puerta de enlace de conexión	• 0: No usar puerta de enlace de conexión. • 1: Usar este Agente de red como puerta de enlace de conexión. • 2: Conectar con el Servidor de administración usando la puerta de enlace de conexión.
GATEWAYADDRESS	Dirección de la puerta de enlace de conexión	Valor de cadena.
CERTSELECTION	Método de recepción de un certificado	• GetOnFirstConnection: Recibir un certificado del Servidor de administración.

		• GetExistent: seleccione un certificado existente. Si esta opción está seleccionada, debe especificarse la propiedad CERTFILE.
CERTFILE	Ruta al archivo de certificado	Valor de cadena.
VMVDI	Activar el modo dinámico de Infraestructura de Escritorio Virtual (VDI)	• 1: Activar. • 0: No activar. • Sin valor: no activar.
LAUNCHPROGRAM	Si se debe ejecutar el servicio del Agente de red tras la instalación	• 1: Iniciar. • Otro valor o ningún valor: No iniciar.
NAGENTTAGS	Etiqueta para el Agente de red (tiene prioridad sobre la etiqueta dada en el archivo de respuestas)	Valor de cadena.

Infraestructura virtual

Kaspersky Security Center admite el uso de máquinas virtuales. Puede instalar el Agente de red y la aplicación de seguridad en cada máquina virtual, y puede proteger las máquinas virtuales a nivel del hipervisor. En el primer caso, puede usar una aplicación de seguridad estándar o Kaspersky Security for Virtualization o Light Agent para proteger sus máquinas virtuales. En el segundo caso, puede utilizar Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center admite la reversión de máquinas virtuales a su estado anterior.

Sugerencias para reducir la carga en máquinas virtuales

Al instalar el Agente de red en una máquina virtual, se le aconseja considerar desactivar algunas funciones de Kaspersky Security Center que parecen ser de poco uso para las máquinas virtuales.

Al instalar el Agente de red en una máquina virtual o en una plantilla diseñada para la generación de máquinas virtuales, recomendamos realizar las acciones siguientes:

- Si está ejecutando una instalación remota, en la ventana de propiedades del paquete de instalación del Agente de red (en la sección **Avanzado**), seleccione la opción **Optimizar la configuración para VDI**.
- Si está ejecutando una instalación interactiva a través de un Asistente, en la ventana del Asistente, seleccione la opción **Optimizar la configuración del Agente de red para la infraestructura virtual**.

Seleccionar esas opciones altera la configuración del Agente de red de modo que las funciones siguientes permanecen desactivadas de forma predeterminada (antes de aplicar una directiva):

- Recuperación de información sobre el software instalado.
- Recuperación de información sobre el hardware.
- Recuperación de información sobre las vulnerabilidades detectadas.
- Recuperación de información sobre las actualizaciones requeridas.

Por lo general, estas funciones no son necesarias en máquinas virtuales porque usan software uniforme y hardware virtual.

La desactivación de las funciones es irreversible. Si se requiere alguna de las funciones desactivadas, puede activarla a través de la directiva del Agente de red, o a través de la configuración local del Agente de red. La configuración local del Agente de red está disponible a través del menú contextual del dispositivo relevante en la Consola de administración.

Compatibilidad para máquinas virtuales dinámicas

Kaspersky Security Center admite máquinas virtuales dinámicas (solo Windows). Si se ha desplegado una infraestructura virtual en la red de la organización, en ciertos casos pueden usarse máquinas virtuales (temporales) dinámicas. Las máquinas virtuales dinámicas se crean bajo nombres únicos según una plantilla preparada por el administrador. El usuario trabaja en la máquina virtual un tiempo, luego, después de apagarse, esta máquina virtual se eliminará de la infraestructura virtual. Si Kaspersky Security Center se ha desplegado en la red de la organización, se añadirá una máquina virtual con el Agente de red instalado a la base de datos del Servidor de administración. Después de que se apague una máquina virtual, la entrada correspondiente también se debe eliminar de la base de datos del Servidor de administración.

Para hacer funcional la función de la eliminación automática de entradas en máquinas virtuales, al instalar el Agente de red en una plantilla para máquinas virtuales dinámicas, seleccione la opción **Activar modo dinámico para VDI**:

- Para la instalación remota: en la ventana de propiedades del paquete de instalación del Agente de red (sección **Avanzado**)
- Para la instalación interactiva: en el Asistente de instalación del Agente de red

> En ningún caso seleccione la opción **Activar modo dinámico para VDI** al instalar el Agente de red en dispositivos físicos.

Si desea que los eventos de las máquinas virtuales dinámicas se almacenen en el Servidor de administración durante un tiempo después de eliminar esas máquinas virtuales, en la ventana de propiedades del Servidor de administración, en la sección **Repositorio de eventos**, seleccione la opción **Almacenar eventos tras la eliminación de los dispositivos** y especifique el plazo de almacenamiento máximo para los eventos (en días).

Compatibilidad para la copia de máquinas virtuales

La copia de una máquina virtual con el Agente de red instalado o la creación un desde una plantilla con el Agente de red instalado son idénticas al despliegue de Agentes de red mediante la captura y la copia de una imagen del disco duro. De este modo, en el caso general, al copiar máquinas virtuales, tiene que realizar las mismas acciones que al desplegar el Agente de red al copiar una imagen de disco.

Sin embargo, los dos casos descritos a continuación muestran el Agente de red, que detecta la copia automáticamente. Debido a los motivos indicados anteriormente, no debe realizar las operaciones sofisticadas descritas en "Despliegue al capturar y copiar el disco duro de un dispositivo":

- La opción **Activar modo dinámico para VDI** estaba seleccionada cuando el Agente de red se instaló: después de cada reinicio del sistema operativo, esta máquina virtual se reconocerá como un nuevo dispositivo, sin tener en cuenta si se lo ha copiado o no.

- Uno de los siguientes hipervisores está en uso: VMware™, HyperV® o Xen®: el Agente de red detecta la copia de la máquina virtual por los ID cambiados del hardware virtual.

El análisis de los cambios en el hardware virtual no es absolutamente confiable. Antes de aplicar este método de forma generalizada, debe probarlo en un pequeño grupo de máquinas virtuales para comprobar la versión del hipervisor que se usa actualmente en su organización.

Compatibilidad de la reversión del sistema de archivos para dispositivos con el Agente de red

Kaspersky Security Center es una aplicación distribuida. La reversión del sistema de archivos a un estado anterior en un dispositivo con el Agente de red instalado llevará a la cancelación de la sincronización de los datos y el funcionamiento incorrecto de Kaspersky Security Center.

El sistema de archivos (o parte de este) puede revertirse en los siguientes casos:

- Al copiar una imagen del disco duro.

- Al restaurar un estado de la máquina virtual por medio de la infraestructura virtual.

- Al restaurar datos desde una copia de seguridad o un punto de recuperación.

Las situaciones en las cuales el software de terceros en dispositivos con el Agente de red instalado afecta la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ son situaciones solo críticas para Kaspersky Security Center. Por lo tanto, siempre debe excluir esta carpeta del procedimiento de recuperación, de ser posible.

Dado que las reglas del lugar de trabajo de algunas organizaciones ofrecen la reversión del sistema de archivos en los dispositivos, se ha habilitado la reversión del sistema de archivos en los dispositivos con el Agente de red instalado en Kaspersky Security Center a partir de la versión 10 Maintenance Release 1 (el Servidor de administración y los Agentes de red deben ser de la versión 10 Maintenance Release 1 o posteriores). Cuando se detectan, esos dispositivos se vuelven a conectar automáticamente al Servidor de administración con el borrado de todos datos y la sincronización completa.

De forma predeterminada, la compatibilidad con la detección de la reversión del sistema de archivos está activada en Kaspersky Security Center 14.

Siempre que sea posible, evite revertir la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ en los dispositivos con el Agente de red instalado, porque la resincronización completa de datos requiere una gran cantidad de recursos.

La reversión del estado del sistema está totalmente prohibida en un dispositivo con el Servidor de administración instalado. Tampoco se permite la reversión de la base de datos usada por el Servidor de administración.

Puede restaurar un estado del Servidor de administración desde una copia de seguridad solo con la utilidad klbackup estándar.

Acerca de los perfiles de conexión para usuarios fuera de la oficina

Puede que los usuarios "fuera de la oficina" de equipos portátiles (en adelante, también denominados "dispositivos") deban cambiar el método de conexión a un Servidor de administración o cambiar entre Servidores de administración según la ubicación actual del dispositivo en la red empresarial.

Los perfiles de conexión solo son compatibles con dispositivos que ejecutan Windows y MacOS.

Uso de diferentes direcciones de un único Servidor de administración

El siguiente procedimiento se aplica únicamente a Kaspersky Security Center 10 Service Pack 1 y versiones posteriores.

Los dispositivos con el Agente de red instalado pueden conectarse al Servidor de administración ya sea mediante la intranet de la organización o por Internet. Esta situación puede requerir que el Agente de red utilice direcciones diferentes para la conexión con el Servidor de administración: la dirección del Servidor de administración externa para la conexión a Internet y la dirección del Servidor de administración interna para la conexión a la intranet.

Para esto, debe añadir un perfil (para la conexión con el Servidor de administración de Internet) a la directiva del Agente de red. Añada el perfil en las propiedades de la directiva (sección **Conectividad**, subsección **Perfiles de conexión**). En la ventana de creación de perfil, debe desactivar la opción **Usar solo para recibir actualizaciones** y seleccionar la opción **Sincronizar la configuración de la conexión con la configuración del Servidor de administración especificada para este perfil**. Si usa una puerta de enlace de conexión para acceder al Servidor de administración (por ejemplo, en una configuración de Kaspersky Security Center como la que se describe en Acceso a Internet: el Agente de red como puerta de enlace en DMZ), debe especificar la dirección de la puerta de enlace de conexión en el campo correspondiente del perfil de conexión.

Cambio entre Servidores de administración según la red actual

El siguiente procedimiento se aplica únicamente a Kaspersky Security Center 10 Service Pack 2 Maintenance Release 1 y versiones posteriores.

Si la organización tiene varias oficinas con Servidores de administración diferentes y algunos de los dispositivos con el Agente de red instalado se mueven entre ellas, necesita el Agente de red para la conexión con el Servidor de administración de la red local en la oficina donde se ubica el dispositivo actualmente.

En este caso, debe crear un perfil para la conexión con el Servidor de administración en las propiedades de la directiva del Agente de red para cada una de las oficinas, excepto la oficina principal donde se ubica el Servidor de administración principal. Debe especificar las direcciones de los Servidores de administración en los perfiles de conexión y activar o desactivar la opción **Usar solo para recibir actualizaciones**:

- Seleccione la opción si necesita que el Agente de red se sincronice con el Servidor de administración principal, mientras el Servidor local se usa solo para descargar actualizaciones.
- Desactive esta opción si es necesario que el Agente de red sea completamente administrado por el Servidor de administración local.

Después de esto, debe configurar las condiciones de conmutación a los perfiles recientemente creados: al menos, una condición para cada una de las oficinas, excepto la oficina principal. El objetivo de cada condición consiste en la detección de elementos que sean específicos del entorno de red de una oficina. Si una condición es verdadera, se activa el perfil correspondiente. Si ninguna de las condiciones es verdadera, el Agente de red cambia al Servidor de administración principal.

Despliegue de la Función de Administración de dispositivos móviles

Esta sección proporciona información sobre la implementación inicial de la función de administración de dispositivos móviles.

Conexión de dispositivos KES al Servidor de administración

Según el método usado para la conexión de dispositivos al Servidor de administración, son posibles dos esquemas de despliegue para Kaspersky Device Management for iOS para los dispositivos KES:

- Esquema de despliegue con conexión directa de dispositivos al Servidor de administración
- Esquema de despliegue que involucra a Forefront® Threat Management Gateway (TMG)

Conexión directa de dispositivos al Servidor de administración

Los dispositivos KES pueden conectarse directamente al puerto 13292 del Servidor de administración.

Según el método usado para la autenticación, son posibles dos opciones para la conexión de dispositivos KES al Servidor de administración:

- Conexión de dispositivos con un certificado de usuario
- Conexión de dispositivos sin un certificado de usuario

Conexión de un dispositivo con un certificado de usuario

Al conectar un dispositivo con un certificado de usuario, ese dispositivo está asociado con la cuenta de usuario a la cual se ha asignado el certificado correspondiente a través de las herramientas del Servidor de administración.

En este caso, se utilizará la autenticación SSL bidireccional (autenticación mutua). Tanto el Servidor de administración como el dispositivo serán autenticados con certificados.

Conexión de un dispositivo sin un certificado de usuario

Al conectar un dispositivo sin un certificado de usuario, ese dispositivo no está asociado con ninguna de las cuentas de usuario en el Servidor de administración. Sin embargo, cuando el dispositivo reciba cualquier certificado, el dispositivo se asociará con el usuario al cual se haya asignado el certificado correspondiente a través de las herramientas del Servidor de administración.

Al conectar ese dispositivo al Servidor de administración, se aplicará la autenticación SSL unidireccional, lo que significa que solo el Servidor de administración se autentica con el certificado. Después de que el dispositivo recupere el certificado de usuario, el tipo de autenticación cambiará a la autenticación SSL bidireccional (autenticación SSL bidireccional, autenticación mutua).

Esquema para conectar dispositivos KES al servidor con la delegación limitada de Kerberos (KCD)

El esquema para conectar dispositivos KES al Servidor de administración que involucra la delegación limitada de Kerberos (KCD) brinda lo siguiente:

- Integración con Microsoft Forefront TMG.
- Uso de la delegación limitada de Kerberos (en adelante, denominada KCD) para la autenticación de dispositivos móviles.
- Integración con la infraestructura de clave pública (en adelante, denominada PKI) para aplicar certificados de usuario.

Al usar este esquema de conexión, tenga en cuenta lo siguiente:

- El tipo de conexión de dispositivos KES a TMG debe ser la "Autenticación SSL bidireccional", es decir, un dispositivo debe conectarse a TMG a través de su certificado de usuario patentado. Para esto, debe integrar el certificado de usuario en el paquete de instalación de Kaspersky Endpoint Security for Android, que se ha instalado en el dispositivo. Este paquete KES debe ser creado por el Servidor de administración específicamente para este dispositivo (usuario).
- Debe especificar el certificado especial (personalizado) en vez del certificado del servidor predeterminado para el protocolo móvil:

  1. En la ventana de propiedades del Servidor de administración, en la sección **Configuración**, seleccione la casilla **Abrir puerto para dispositivos móviles** y, luego, seleccione **Agregar certificado** en la lista desplegable.
  2. En la ventana que se abre, especifique el mismo certificado que se configuró en TMG cuando se publicó el punto de acceso al protocolo móvil en el Servidor de administración.

- Los certificados de usuario para los dispositivos KES deben ser emitidos por la entidad de certificación (CA) del dominio. Tenga en cuenta que si el dominio incluye varios CA raíz, los certificados de usuario deben ser emitidos por la CA que se haya configurado en la publicación de TMG.

  Puede asegurarse de que el certificado de usuario cumpla con los requisitos especificados anteriormente con uno de los siguientes métodos:

  - Especifique el certificado de usuario especial en el Asistente para nuevo paquete de Instalación y en el Asistente de instalación de certificados.
  - Integre el Servidor de administración con la PKI del dominio y defina la configuración correspondiente en las reglas para la emisión de certificados:

    1. En el árbol de consola, expanda la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.

2. En el espacio de trabajo de la carpeta **Certificados**, haga clic en el botón **Configurar reglas de emisión de certificados** para abrir la ventana **Reglas de emisión de certificados**.

3. En la sección **Integración con la PKI**, configure la integración con la infraestructura de clave pública.

4. En la sección **Emisión de certificados móviles**, especifique el origen de los certificados.

A continuación, se especifica un ejemplo de la configuración de la delegación limitada de Kerberos (KCD) con las siguientes suposiciones:

- El punto del acceso al protocolo móvil en el lado del Servidor de administración está configurado en el puerto 13292.
- El nombre del dispositivo con TMG es tmg.mydom.local.
- El nombre del dispositivo con el Servidor de administración es ksc.mydom.local.
- El nombre de la publicación externa del punto de acceso al protocolo móvil es kes4mob.mydom.global.

Cuenta de dominio para el Servidor de administración

Debe crear una cuenta de dominio (por ejemplo, KSCMobileSrvcUsr) en la que se ejecutará el servicio del Servidor de administración. Puede especificar una cuenta para el servicio del Servidor de administración al instalar el Servidor de administración o a través de la utilidad klsrvswch. La utilidad klsrvswch se ubica en la carpeta de instalación del Servidor de administración.

Debe especificarse una cuenta de dominio por las siguientes razones:

- La función para la administración de dispositivos KES es una parte integral del Servidor de administración.
- Para asegurar el correcto funcionamiento de la delegación limitada de Kerberos (KCD), el lado de recepción (es decir, el Servidor de administración) se debe ejecutar bajo una cuenta de dominio.

Nombre principal del servicio para http/kes4mob.mydom.local

En el dominio, en la cuenta de KSCMobileSrvcUsr, añada un SPN para publicar el servicio del protocolo móvil en el puerto 13292 del dispositivo con el Servidor de administración. Para el dispositivo kes4mob.mydom.local con el Servidor de administración, esto aparecerá de la siguiente forma:

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

Configuración de las propiedades de dominio del dispositivo con TMG (tmg.mydom.local)

Para delegar el tráfico, confíe al dispositivo con TMG (tmg.mydom.local) el servicio definido por el SPN (http/kes4mob.mydom.local:13292).

Para confiar al dispositivo con TMG el servicio definido por el SPN (http/kes4mob.mydom.local:13292), el administrador debe realizar las siguientes acciones:

1. En el complemento de MMC denominado "Equipos y usuarios de Active Directory", seleccione el dispositivo con TMG instalado (tmg.mydom.local).

2. En las propiedades del dispositivo, en la ficha **Delegación**, configure la opción de **Confiar en este equipo para la delegación al servicio especificado únicamente** en **Usar cualquier protocolo de autenticación**.

3. En la lista **Servicios a los que esta cuenta puede presentar credenciales delegadas**, añada el SPN http/kes4mob.mydom.local:13292.

Certificado especial (personalizado) para la publicación (kes4mob.mydom.global)

Para publicar el protocolo móvil del Servidor de administración, debe emitir un certificado especial (personalizado) para FQDN kes4mob.mydom.global y especificarlo en vez del certificado del servidor predeterminado en la configuración del protocolo móvil del Servidor de administración en la Consola de administración. Para hacerlo, en la ventana de propiedades del Servidor de administración, en la sección **Configuración**, seleccione la casilla **Abrir puerto para dispositivos móviles** y, luego, seleccione **Agregar certificado** en la lista desplegable.

Tenga en cuenta que el contenedor del certificado del servidor (el archivo con la extensión p12 o pfx) también debe contener una cadena de certificados raíz (claves públicas).

Configuración de la publicación en TMG

En TMG, para el tráfico que va desde el lado del dispositivo móvil al puerto 13292 de kes4mob.mydom.global, debe configurar KCD en el SPN (http/kes4mob.mydom.local:13292) usando el certificado del servidor emitido para FQND kes4mob.mydom.global. Tenga en cuenta que el punto del acceso de publicación y publicado (puerto 13292 del Servidor de administración) deben compartir el mismo certificado del servidor.

Uso de Google Cloud Firebase Messaging

Para garantizar las respuestas oportunas de los dispositivos KES en Android a los comandos del administrador, debe activar el uso de Google™ Firebase Cloud Messaging (en adelante, denominado FCM) en las propiedades del Servidor de administración.

Para activar el uso de FCM:

1. En la Consola de administración, seleccione el nodo **Administración de dispositivos móviles** y la carpeta **Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos móviles**, seleccione **Propiedades**.
3. En las propiedades de la carpeta, seleccione la sección **Configuración de Google Firebase Cloud Messaging**.
4. En los campos **ID de remitente** y **Clave de servidor**, especifique la configuración de FCM: SENDER_ID y de la Clave de API.

El servicio de FCM se ejecuta en los siguientes rangos de direcciones:

- Desde el lado del dispositivo KES, se requiere acceso a los puertos 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) y 5230 (HTTPS) de las siguientes direcciones:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Todas las direcciones IP enumeradas en ASN de Google de 15169

- Desde el lado del Servidor de administración, se requiere acceso al puerto 443 (HTTPS) de las siguientes direcciones:
  - fcm.googleapis.com
  - Todas las direcciones IP enumeradas en ASN de Google de 15169

Si la configuración del servidor proxy (**Avanzado**/**Configuración del acceso a Internet**) se ha definido en las propiedades del Servidor de administración en la Consola de administración, se utilizarán para la interacción con FCM.

Configuración de FCM: recuperación de SENDER_ID y la clave de API

Para configurar FCM, el administrador debe realizar las siguientes acciones:

1. Regístrese en el portal de Google.
2. Vaya al portal para programadores.
3. Cree un nuevo proyecto haciendo clic en el botón **Crear proyecto** y especifique el nombre del proyecto y el ID.
4. Espere que el proyecto se cree.

   En la primera página del proyecto, en la parte superior de la página, el campo **Número de proyecto** muestra el SENDER_ID relevante.
5. Vaya a la sección **API y autenticación/APIs** y active **Google Firebase Cloud Messaging para Android**.
6. Vaya a la sección **API y autenticación/Credenciales** y haga clic en **Crear nueva clave**.
7. Haga clic en el botón **Clave de servidor**.
8. Imponga restricciones (si corresponde) y haga clic en el botón **Crear**.
9. Recupere la clave de API desde las propiedades de la clave recién creada (campo **Clave de servidor**).

Integración con la infraestructura de clave pública

La integración con la infraestructura de clave pública (en adelante, denominada PKI) está diseñada principalmente para simplificar la emisión de certificados de usuario de dominio por parte del Servidor de administración.

El administrador puede asignar un certificado de dominio para un usuario en la Consola de administración. Esto puede realizarse usando uno de los métodos siguientes:

- Asigne al usuario un certificado especial (personalizado) de un archivo en el Asistente de Conexión de nuevo dispositivo o en el Asistente de instalación de certificados.
- Realice la integración con la PKI y asigne la PKI para que funcione como el origen de certificados para un tipo específico de certificados o para todos los tipos de certificados.

La configuración de integración con PKI está disponible en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados** haciendo clic en el enlace **Integrar con la infraestructura de clave pública**.

Principio general de integración con la PKI para la emisión de certificados de usuario de dominio

En la Consola de administración, haga clic en el enlace **Integrar con la infraestructura de clave pública** en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados** para especificar una cuenta de dominio que utilizará el Servidor de administración para emitir certificados de usuario de dominio a través de la CA del dominio (en adelante, se hace referencia como la cuenta bajo la cual se realiza la integración con la PKI).

Tenga en cuenta lo siguiente:

- La configuración de la integración con la PKI le proporciona la posibilidad de especificar la plantilla predeterminada para todos los tipos de certificados. Tenga en cuenta que las reglas para la emisión de certificados (disponibles en el espacio de trabajo de la carpeta **Administración de dispositivos móviles** / **Certificados** haciendo clic en **Configurar reglas de emisión de certificados**) le permiten especificar una plantilla individual para cada tipo de certificado.

- Un certificado especial de Agente de inscripción (EA) debe instalarse en el dispositivo con el Servidor de administración, en el repositorio de certificados de la cuenta bajo la cual se realiza la integración con la PKI. El certificado del Agente de inscripción (EA) es emitido por el administrador de la CA (entidad de certificación) del dominio.

La cuenta bajo la cual se realiza la integración con la PKI debe cumplir los siguientes criterios:

- Ser un usuario de dominio.

- Ser un administrador local del dispositivo con el Servidor de administración desde el cual se inicia la integración con la PKI.

- Tener el permiso para *Iniciar sesión como servicio*.

- El dispositivo con el Servidor de administración instalado debe ejecutarse al menos una vez con esta cuenta para crear un perfil de usuario permanente.

Servidor web de Kaspersky Security Center

El Servidor web de Kaspersky Security Center (en adelante, denominado Servidor web) es un componente de Kaspersky Security Center. El Servidor web está diseñado para publicar paquetes de instalación independientes, paquetes de instalación independientes para dispositivos móviles y archivos de una carpeta compartida.

Los paquetes de instalación que se han creado se publican en el Servidor web automáticamente y, luego, se eliminan después de la primera descarga. El administrador puede enviar el nuevo enlace al usuario de cualquier forma que convenga; por ejemplo, por correo electrónico.

Al hacer clic en el enlace, el usuario puede descargar la información necesaria en un dispositivo móvil.

Configuración del servidor web

Si se requiere la configuración avanzada del Servidor web, sus propiedades le permiten cambiar puertos para HTTP (8060) y HTTPS (8061). Además del cambio de puertos, puede reemplazar el certificado del servidor para HTTPS y cambiar FQDN del Servidor web por HTTP.

Otro trabajo de rutina

Esta sección proporciona recomendaciones sobre el trabajo rutinario con Kaspersky Security Center.

Semáforos en la Consola de administración

La Consola de administración le permite evaluar rápidamente el estado actual de Kaspersky Security Center y los dispositivos administrados al comprobar los semáforos. Los semáforos se muestran en el espacio de trabajo del nodo del **Servidor de administración**, en la ficha **Supervisión**. La ficha proporciona seis paneles de información con semáforos. Un semáforo es una barra vertical de color en el lado izquierdo de un panel. Cada panel con un semáforo equivale a una cobertura funcional específica de Kaspersky Security Center (consulte la tabla a continuación).

Coberturas abarcadas por semáforos en la Consola de administración

Nombre del panel	Cobertura del semáforo
Despliegue	Instalación del Agente de red y aplicaciones de seguridad en dispositivos en una red de la organización
Plan de administración	Estructura de grupos de administración. Análisis de la red. Reglas de movimiento de dispositivos
Configuración de protección	Funcionalidad de la aplicación de seguridad: estado de la protección, análisis antivirus
Actualizar	Actualizaciones y parches
Supervisión	Estado de la protección
Servidor de administración	Funciones y propiedades del Servidor de administración

Cada semáforo puede ser de cualquiera de estos cinco colores (consulte la tabla a continuación). El color del semáforo depende del estado actual de Kaspersky Security Center y de los eventos que se registraron.

Códigos de los colores de los semáforos

Estado	Color del semáforo	Significado del color del semáforo
Informativo	Verde	No se requiere la intervención del administrador.
Advertencia	Amarillo	Se requiere la intervención del administrador.
Crítico	Rojo	Se han detectado graves problemas. Se requiere la intervención del administrador para solucionarlos.
Informativo	Celeste	Se han registrado eventos que no están relacionados con amenazas posibles o reales en la seguridad de dispositivos administrados.
Informativo	Gris	Los detalles de los eventos no están disponibles o todavía no se han recuperado.

El objetivo del administrador es mantener los semáforos en todos los paneles de información en la ficha **Supervisión** en verde.

Acceso remoto a dispositivos administrados

Esta sección proporciona información sobre el acceso remoto a dispositivos administrados.

Uso de la opción “No desconectar del Servidor de administración” para proporcionar conectividad continua entre un dispositivo administrado y el Servidor de administración

Si no usa servidores push, Kaspersky Security Center no proporciona conectividad continua entre los dispositivos administrados y el Servidor de administración. Los Agentes de red en los dispositivos administrados establecen conexiones periódicamente y se sincronizan con el Servidor de administración. El intervalo entre esas sesiones de sincronización se define en una directiva del Agente de red. Si se requiere una sincronización temprana, el Servidor de administración (o un punto de distribución, si está en uso) envía un paquete de red firmado a través de una red IPv4 o IPv6 al puerto UDP del Agente de red. De forma predeterminada el número de puerto es el 15000. Si no es posible establecer ninguna conexión a través de UDP entre el Servidor de administración y un dispositivo administrado, la sincronización se ejecutará en la siguiente conexión periódica del Agente de red con el Servidor de administración dentro del intervalo de sincronización.

Algunas operaciones no pueden realizarse sin una conexión temprana entre el Agente de red y el Servidor de administración, por ejemplo, ejecutar y detener tareas locales, recibir estadísticas de una aplicación administrada o crear un túnel. Para resolver este problema, si no utiliza servidores push, puede utilizar la opción **No desconectar del Servidor de administración** para asegurarse de que haya una conectividad continua entre un dispositivo administrado y el Servidor de administración.

Para proporcionar una conectividad continua entre un dispositivo administrado y el Servidor de administración:

1. Realice una de las siguientes acciones:

   - Si el dispositivo administrado accede al Servidor de administración directamente (es decir, no a través de un punto de distribución):

     a. En el árbol de consola, seleccione la carpeta **Dispositivos administrados**.

     b. En el espacio de trabajo de la carpeta, seleccione el dispositivo administrado con el que desea proporcionar conectividad continua.

     c. En el menú contextual del dispositivo, seleccione **Propiedades**.

     Se abre la ventana de propiedades del dispositivo seleccionado.

   - Si el dispositivo administrado accede al Servidor de administración mediante un punto de distribución que se ejecuta en modo de puerta de enlace, no directamente:

     a. En el árbol de consola, haga clic en el nodo del **Servidor de administración**.

     b. En el menú contextual del nodo, seleccione **Propiedades**.

     c. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Puntos de distribución**.

     d. En la lista, seleccione el punto de distribución necesario y, luego, haga clic en **Propiedades**.

Se abre la ventana de propiedades del punto de distribución.

2. En la sección **General** de la ventana seleccione la opción **No desconectar del Servidor de administración**.

La conectividad continua está establecida entre el dispositivo administrado y el Servidor de administración.

El número total máximo de dispositivos con la opción **No desconectar del Servidor de administración** seleccionada es 300.

Acerca de la comprobación de la hora de conexión entre un dispositivo y el Servidor de administración

Después de cerrar un dispositivo, el Agente de red notifica el Servidor de administración de este evento. En la Consola de administración, ese dispositivo se muestra como apagado. Sin embargo, el Agente de red no puede notificar al Servidor de administración de todos estos eventos. El Servidor de administración, por lo tanto, analiza periódicamente el atributo **Conectado al Servidor de administración** (el valor de este atributo se muestra en la Consola de administración, en las propiedades del dispositivo, en la sección **General**) para cada dispositivo y lo compara con el intervalo de sincronización de la configuración actual del Agente de red. Si un dispositivo no ha respondido durante más de tres intervalos de sincronización sucesivos, ese dispositivo se marca como apagado.

Acerca de la sincronización forzada

Si bien Kaspersky Security Center sincroniza el estado, la configuración, las tareas y las directivas para los dispositivos administrados automáticamente, en algunos casos, el administrador debe saber exactamente si la sincronización ya se ha realizado para un dispositivo específico en ese momento.

En el menú contextual de los dispositivos administrados en la Consola de administración, el elemento de menú **Todas las tareas** contiene el comando **Forzar sincronización**. Cuando Kaspersky Security Center 14 ejecuta este comando, el Servidor de administración intenta conectarse al dispositivo. Si el intento tiene éxito, se realizará la sincronización forzada. De lo contrario, la sincronización se forzará y la casilla se desactivará únicamente después de la siguiente conexión planificada entre el Agente de red y el Servidor de administración.

Acerca de la conexión de túnel

Kaspersky Security Center permite los túneles de conexiones de TCP desde la Consola de administración mediante el Servidor de administración y, luego, mediante el Agente de red a un puerto especificado en un dispositivo administrado. El túnel está diseñado para conectar una aplicación cliente en un dispositivo con la Consola de administración instalada en un puerto TCP en un dispositivo administrado si una conexión directa entre la Consola de administración y el dispositivo de destino no es posible.

Por ejemplo, el túnel se utiliza para las conexiones con un escritorio remoto, tanto para la conexión con una sesión existente como para crear una nueva sesión remota.

El túnel también puede activarse usando herramientas externas. Por ejemplo, el administrador puede ejecutar la utilidad putty, el cliente VNC y otras herramientas de esta manera.

Guía de dimensionamiento

Esta sección proporciona información sobre las escalas de Kaspersky Security Center.

Acerca de esta Guía

La Guía de dimensionamiento de Kaspersky Security Center 14 (también conocida como Kaspersky Security Center) está dirigida a los profesionales que instalan y administran Kaspersky Security Center, así como para los que proporcionan soporte técnico a las organizaciones que utilizan Kaspersky Security Center.

Todas las recomendaciones y los cálculos son para redes en las que Kaspersky Security Center administra la protección de dispositivos con el software Kaspersky instalado, incluyendo dispositivos móviles. Si los dispositivos móviles o cualquier otro dispositivo administrado, se deben considerar por separado, esto se establece específicamente.

Para obtener y mantener un rendimiento óptimo en diferentes condiciones operativas, debe tener en cuenta la cantidad de dispositivos en red, la topología de red y el conjunto de funciones de Kaspersky Security Center que necesita.

Esta guía también contiene la siguiente información:

- Limitaciones de Kaspersky Security Center
- Cálculos para los nodos clave de Kaspersky Security Center (Servidores de administración y puntos de distribución):
  - Requisitos de hardware para Servidores de administración y puntos de distribución
  - Cálculo del número y jerarquía de los Servidores de administración
  - Cálculo del número y la configuración de los puntos de distribución
- Configuración del registro de eventos en la base de datos según la cantidad de dispositivos en red
- Configuración de tareas específicas destinadas a un rendimiento óptimo de Kaspersky Security Center
- Tasa de tráfico (carga de red) entre el Servidor de administración de Kaspersky Security Center y cada dispositivo protegido

Se recomienda consultar esta guía en los siguientes casos:

- Al planear recursos antes de la instalación de Kaspersky Security Center
- Al planear cambios significativos en la escala de la red en la que se implementa Kaspersky Security Center
- Al dejar de utilizar Kaspersky Security Center dentro de un segmento de red limitado (un entorno de prueba) y cambiar al despliegue total de Kaspersky Security Center en la red corporativa
- Al realizar cambios en el conjunto de funciones de Kaspersky Security Center utilizadas

Información sobre limitaciones de Kaspersky Security Center

La siguiente tabla muestra las limitaciones de la versión actual de Kaspersky Security Center.

Limitaciones de Kaspersky Security Center

Tipo de limitación	Valor
Número máximo de dispositivos administrados por Servidor de administración	100000
Número máximo de dispositivos con la opción **No desconectar del Servidor de administración** de verificación seleccionada	300
Número máximo de grupos de administración	10000
Número máximo de eventos para almacenar	45000000
Número máximo de directivas	2000
Número máximo de tareas	2000
Número total máximo de objetos de Active Directory (unidades organizativas [OU] y cuentas de usuarios, dispositivos y grupos de seguridad)	1000000
Número máximo de perfiles en una directiva	100
Número máximo de Servidores de administración secundarios en un único Servidor de administración principal	500
Número máximo de Servidores de administración virtuales	500
Número máximo de dispositivos que un único punto de distribución puede abarcar (los puntos de distribución pueden abarcar únicamente dispositivos no móviles)	10000
Número máximo de dispositivos que pueden usar una única puerta de enlace de conexión	10 000, incluyendo dispositivos móviles
Número máximo de dispositivos móviles por Servidor de administración	100 000 menos el número de dispositivos fijos administrados

Cálculos de los Servidores de administración

Esta sección proporciona los requisitos de software y hardware para los dispositivos utilizados como Servidores de administración. También se proporcionan recomendaciones para calcular el número y la jerarquía de los Servidores de administración según la configuración de la red de la organización.

Cálculo de recursos de hardware para el Servidor de administración

Esta sección contiene cálculos que proporcionan una guía para planificar recursos de hardware para el Servidor de administración. Se proporciona por separado una recomendación sobre el cálculo del espacio en disco cuando se utiliza la función Administración de vulnerabilidades y parches.

Requisitos de hardware para el DBMS y el Servidor de administración

La siguiente tabla especifica los requisitos mínimos de hardware recomendados para un DBMS y un Servidor de administración obtenidos durante pruebas. Para ver una lista completa de sistemas operativos y DBMS admitidos, consulte la lista de requisitos de software y hardware.

El Servidor de administración y SQL Server están en dispositivos diferentes, la red incluye 50 000 dispositivos

Dirección del dispositivo con el Servidor de administración instalado.

Hardware	Valor
CPU	4 núcleos, 2500 MHz
RAM	8 GB
Disco duro	300 GB, RAID recomendado
Adaptador de red	1 Gbit

Configuración del dispositivo con SQL Server instalado

Hardware	Valor
CPU	4 núcleos, 2500 MHz
RAM	16 GB
Disco duro	200 GB, RAID SATA
Adaptador de red	1 Gbit

El Servidor de administración y SQL Server están en el mismo dispositivo, la red incluye 50 000 dispositivos

La configuración del dispositivo que tiene el Servidor de administración y SQL Server instalados

Hardware	Valor
CPU	8 núcleos, 2500 MHz
RAM	16 GB
Disco duro	500 GB, RAID SATA
Adaptador de red	1 Gbit

El Servidor de administración y SQL Server están en dispositivos diferentes, la red incluye 100 000 dispositivos

Dirección del dispositivo con el Servidor de administración instalado.

Hardware	Valor
CPU	8 núcleos, 2,13 GHz
RAM	8 GB
Disco duro	1 TB con RAID
Adaptador de red	1 Gbit

Configuración del dispositivo con SQL Server instalado

Hardware	Valor
CPU	8 núcleos, 2,53 GHz
RAM	26 GB
Disco duro	500 GB, RAID SATA
Adaptador de red	1 Gbit

Las pruebas se ejecutaron bajo la configuración siguiente:

- La asignación automática de puntos de distribución se activa en el Servidor de administración, o los puntos de distribución se asignan manualmente según la tabla de recomendaciones.
- La tarea de copia de seguridad guarda las copias de seguridad en un recurso de archivo localizado en un servidor dedicado.
- El intervalo de sincronización para los Agentes de red está configurado según lo especificado en la tabla a continuación.

Intervalo de sincronización para Agentes de red

Intervalo de sincronización (min)	Número de dispositivos administrados
15	10000
30	20000
45	30000
60	40000
75	50000
150	100000

Cálculo del espacio de la base de datos

La fórmula siguiente permite calcular de manera aproximada la cantidad de espacio que debe reservarse en la base de datos:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

Donde:

- C es el número de dispositivos.
- E es el número de eventos que almacenar.
- A es el número total de objetos de Active Directory:
  - Cuentas del dispositivo
  - Cuentas de usuario
  - Cuentas de grupos de seguridad
  - Unidades organizativas de Active Directory

Si análisis de Active Directory está desactivado, A se considera igual a cero.

- N es la cantidad promedio de archivos ejecutables que se incluyen en el inventario de un dispositivo de endpoint.
- F es el número de dispositivos de endpoint, donde se incluyen en el inventario los archivos ejecutables.

Si planea habilitar (en la configuración de la directiva de Kaspersky Endpoint Security) la notificación del Servidor de administración en las aplicaciones que ejecuta, necesitará gigabytes (GB) adicionales (0.03 * C) para almacenar en la base de datos la información sobre las aplicaciones que ejecuta.

Si el Servidor de administración distribuye actualizaciones de Windows (es decir, funciona como servidor de Windows Server Update Services), la base de datos necesitará 2,5 GB adicionales.

Durante el funcionamiento, un cierto *espacio no asignado* siempre está presente en la base de datos. Así, el tamaño real del archivo de base de datos (de forma predeterminada, el archivo KAV.MDF si SQL Server se utiliza como DBMS) en general suele ser el doble de la cantidad de espacio ocupado en la base de datos.

No se recomienda limitar explícitamente el tamaño del registro de transacciones (de forma predeterminada, el archivo KAV_log.LDF, si utiliza SQL Server como DBMS). Se recomienda dejar el valor predeterminado del parámetro MAXSIZE. Sin embargo, si tiene que limitar el tamaño de este archivo, tenga en cuenta que el valor necesario habitual del parámetro MAXSIZE para KAV_log.LDF es de 20480 MB.

Cálculo del espacio en disco (usando o sin usar la función Administración de vulnerabilidades y parches)

Cálculo del espacio en disco sin usar la función Administración de vulnerabilidades y parches

El espacio de disco del Servidor de administración requerido para la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit se puede estimar aproximadamente usando la fórmula:

(724 * C + 0.15 * E + 0.17 * A), KB

Donde:

- C es el número de dispositivos.
- E es el número de eventos que almacenar.
- A es el número total de objetos de Active Directory:
  - Cuentas del dispositivo
  - Cuentas de usuario
  - Cuentas de grupos de seguridad
  - Unidades organizativas de Active Directory

Si análisis de Active Directory está desactivado, A se considera igual a cero.

Cálculo del espacio en disco adicional usando la función Administración de vulnerabilidades y parches

- Actualizaciones. La carpeta compartida requiere adicionalmente al menos 4 GB para almacenar actualizaciones.
- Paquetes de instalación. Si algunos paquetes de instalación están almacenados en el Servidor de administración, la carpeta compartida requerirá una cantidad adicional de espacio en disco libre igual al tamaño total de todos los paquetes de instalación disponibles para su instalación.
- Tareas de instalación remota. Si en el Servidor de administración hay tareas de instalación remota, se requerirá una cantidad adicional de espacio en disco libre (en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) equivalente al tamaño total de los paquetes de instalación que se instalarán.
- Parches. Si el Servidor de administración está involucrado en la instalación de parches, se requerirá una cantidad adicional de espacio en el disco:
  - En la carpeta de parches debería haber una cantidad de espacio en disco igual al tamaño total de todos los parches que se han descargado. De forma predeterminada, los parches se almacenan en la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (puede usar la utilidad klsrvswch para especificar una carpeta diferente para almacenar parches). Si el Servidor de administración se utiliza como el servidor WSUS, se le aconseja asignar al menos 100 GB a esta carpeta.
  - En la carpeta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit debe haber una cantidad de espacio en disco igual al tamaño total de los parches a los que hacen referencia las instancias existentes de las tareas de reparación de vulnerabilidades e instalación de actualizaciones (parche).

Cálculo del número y configuración de los Servidores de administración

Para reducir la carga en el Servidor de administración principal, puede asignar un Servidor de administración separado a cada grupo de administración. El número de Servidores de administración secundarios no puede exceder 500 para un solo Servidor de administración principal.

Recomendamos que cree la configuración de Servidores de administración en correspondencia con la configuración de la red de su organización.

Cálculos para puntos de distribución y puertas de enlace de conexión

Esta sección proporciona los requisitos de hardware para dispositivos utilizados como puntos de distribución junto con recomendaciones para calcular el número de puntos de distribución y puertas de enlace de conexión, según la configuración de la red corporativa.

Requisitos para un punto de distribución

Para manejar hasta 10 000 dispositivos cliente, un punto de distribución debe cumplir los siguientes requisitos mínimos (la siguiente configuración es la sugerida para un banco de pruebas):

- CPU: Intel® Core™ i7-7700 CPU a 3,60 GHz de 4 núcleos.
- RAM: 8 GB.

- Disco: SSD 120 GB.

Además, un punto de distribución debe tener acceso a Internet y debe estar siempre conectado.

Si en el Servidor de administración hay tareas de instalación remota pendientes, el dispositivo con el punto de distribución también necesitará un espacio libre en disco, equivalente al tamaño total de los paquetes de instalación que se instalarán.

Si en el Servidor de administración están pendientes una o varias instancias de la tarea para la instalación de actualizaciones (parches) y la reparación de vulnerabilidades, el dispositivo con el punto de distribución también necesitará un espacio libre en disco que será el doble del tamaño total de todos los parches que se instalarán.

Cálculo del número y la configuración de los puntos de distribución

Cuantos más dispositivos cliente contenga una red, más puntos de distribución requerirá. Le recomendamos que no desactive la asignación automática de puntos de distribución. Cuando la asignación automática de puntos de distribución está activada, el Servidor de administración asigna puntos de distribución si el número de dispositivos cliente es elevado y define su configuración.

La utilización de puntos de distribución exclusivamente asignados

Si planea usar ciertos dispositivos específicos como puntos de distribución (es decir, servidores asignados exclusivamente), puede optar por no usar la asignación automática de puntos de distribución. En este caso, compruebe que los dispositivos a los que planea hacer puntos de distribución tengan el volumen suficiente de espacio libre en disco, que no se apaguen con frecuencia y que tengan el modo de suspensión desactivado.

Número de puntos de distribución asignados exclusivamente en una red que contiene un único segmento de red, en función del número de dispositivos en red

Número de dispositivos cliente en el segmento de la red	Número de puntos de distribución
Menos de 300	0 (no asigne puntos de distribución)
Más de 300	Aceptable: (N/10,000 + 1), recomendado: (N/5000 + 2), donde N es el número de dispositivos conectados a una red

Número de puntos de distribución asignados exclusivamente en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

Número de dispositivos cliente por segmento de la red	Número de puntos de distribución
Menos de 10	0 (no asigne puntos de distribución)
10-100	1
Más de 100	Aceptable: (N/10,000 + 1), recomendado: (N/5000 + 2), donde N es el número de dispositivos conectados a una red

Uso de dispositivos cliente estándar (estaciones de trabajo) como puntos de distribución

Si planea usar dispositivos cliente estándar (es decir, estaciones de trabajo) como puntos de distribución, le recomendamos que asigne puntos de distribución como se muestra en las siguientes tablas para evitar una carga excesiva en los canales de comunicación y el Servidor de administración:

Número de estaciones de trabajo que funcionan como puntos de distribución en una red que contiene un único segmento de red, en función del número de dispositivos en red

Número de dispositivos cliente en el segmento de la red	Número de puntos de distribución
Menos de 300	0 (no asigne puntos de distribución)
Más de 300	(N/300 + 1), donde N es el número de dispositivos en red, pero debe haber al menos tres puntos de distribución

Número de estaciones de trabajo que funcionan como puntos de distribución en una red que contiene múltiples segmentos de red, en función del número de dispositivos en red

Número de dispositivos cliente por segmento de la red	Número de puntos de distribución
Menos de 10	0 (no asigne puntos de distribución)
10-30	1
31-300	2
Más de 300	(N/300 + 1), donde N es el número de dispositivos en red, pero debe haber al menos tres puntos de distribución

Si un punto de distribución se apaga (o no está disponible por algún otro motivo), los dispositivos administrados en su cobertura pueden acceder al Servidor de administración para obtener actualizaciones.

Cálculo del número de puertas de enlace de conexión

Si planea usar una puerta de enlace de conexión, le recomendamos que designe un dispositivo especial para esta función.

Una puerta de enlace de conexión puede cubrir un máximo de 10 000 dispositivos administrados, incluidos los dispositivos móviles.

Registro de información sobre eventos para tareas y directivas

Esta sección proporciona cálculos asociados con el almacenamiento del evento en la base de datos del Servidor de administración y ofrece recomendaciones sobre cómo minimizar el número de eventos y reducir así la carga en el Servidor de administración.

De forma predeterminada, las propiedades de cada tarea y cada directiva permiten almacenar todos los eventos relacionados con la ejecución de la tarea y la aplicación de la directiva.

Sin embargo, si una tarea se ejecuta con bastante frecuencia (por ejemplo, más de una vez por semana) y en un número bastante grande de dispositivos (por ejemplo, más de 10.000), la cantidad de eventos puede ser demasiado grande y los eventos puede inundar la base de datos. En este caso, se recomienda seleccionar una de dos opciones en la configuración de la tarea:

- **Guardar eventos sobre el progreso de la tarea**. En este caso, la base de datos solo recibe información sobre el inicio, el progreso y la finalización (correcta, con una advertencia o un error) de la tarea de cada dispositivo en el que se ejecuta.
- **Guardar solo los resultados de ejecución de la tarea**. En este caso, la base de datos solo recibe información sobre la finalización (correcta, con una advertencia o un error) de la tarea de cada dispositivo en el que se ejecuta.

Si se ha definido una directiva para un número bastante grande de dispositivos (por ejemplo, más de 10.000), la cantidad de eventos también puede ser grande y los eventos pueden inundar la base de datos. En este caso, se recomienda elegir solo los eventos más críticos en la configuración de la directiva y habilitar su registro. Se recomienda desactivar el registro de todos los demás eventos.

Al hacerlo, reducirá la cantidad de eventos en la base de datos, aumentará la velocidad de ejecución de los escenarios asociados con el análisis de la tabla de eventos en la base de datos y disminuirá el riesgo de que una gran cantidad de eventos que involucren cambios en el estado de las tareas de grupo sobrescriban eventos críticos.

También puede reducir el plazo de almacenamiento para eventos asociados con una tarea o directiva. El período predeterminado es de siete días para eventos relacionados con la tarea y 30 días para eventos relacionados con la directiva. Cuando cambie el plazo de almacenamiento del evento, tenga en cuenta los procedimientos de trabajo establecidos en su organización y la cantidad de tiempo que el administrador del sistema puede dedicar al análisis de cada evento.

Se recomienda modificar la configuración de almacenamiento de eventos en cualquiera de los siguientes casos:

- Los eventos que implican cambios en el estado intermedio de tareas de grupo y eventos de aplicación de directivas representan un gran porcentaje de todos los eventos en la base de datos de Kaspersky Security Center

- El registro de eventos de Kaspersky comienza a mostrar entradas sobre la eliminación automática de eventos cuando se excede el límite establecido en el número total de eventos almacenados en la base de datos

Elija las opciones de registro de eventos en el supuesto de que la cantidad óptima de eventos procedentes de un solo dispositivo por día no debe exceder 20. Puede aumentar este límite ligeramente, si es necesario, pero solo si la cantidad de dispositivos en su red es relativamente pequeña (menos de 10.000).

Consideraciones específicas y configuración óptima de ciertas tareas

Ciertas tareas están sujetas a consideraciones específicas relacionadas con la cantidad de dispositivos en red. Esta sección ofrece recomendaciones sobre la configuración óptima de configuraciones para tales tareas.

La detección de dispositivos, la tarea de copia de seguridad de datos, la tarea de mantenimiento de la base de datos y las tareas de grupo para actualizar Kaspersky Endpoint Security forman parte de las funciones básicas de Kaspersky Security Center.

La tarea de inventario es parte de la función Administración de vulnerabilidades y parches y no está disponible si esta no está activada.

Frecuencia de detección de dispositivos

No es aconsejable aumentar la frecuencia predeterminada de la detección de dispositivos porque esto puede crear una carga excesiva en los controladores de dominio. En cambio, se recomienda programar el sondeo a la frecuencia mínima posible permitida por las necesidades de su organización. Las recomendaciones para calcular la programación óptima se proporcionan en la tabla a continuación.

Programación de detección de dispositivos

Número de dispositivos en red	Frecuencia de detección de dispositivos recomendada
Menos de 10 000	Frecuencia predeterminada o menos
10.000 o mayor	Una vez por día o menos

Tarea de copia de seguridad de datos del Servidor de administración y tarea de mantenimiento de la base de datos

El Servidor de administración deja de funcionar cuando se ejecutan las siguientes tareas:

- Copia de seguridad de los datos del Servidor de administración
- Mantenimiento de bases de datos

Cuando se ejecutan estas tareas, la base de datos no puede recibir ningún dato.

Es posible que tenga que reprogramar estas tareas para que no se ejecuten al mismo tiempo que otras tareas del Servidor de administración.

Tareas de grupo para actualizar Kaspersky Endpoint Security

Si el Servidor de administración actúa como fuente de actualizaciones, la opción de programación recomendada para Kaspersky Endpoint Security 10 y versiones posteriores es **Cuando se descargan nuevas actualizaciones en el repositorio** con la casilla **Utilizar retardo aleatorio automático para el inicio de tareas** seleccionada.

Si se crea una tarea local para descargar actualizaciones de servidores de Kaspersky al repositorio en cada punto de distribución, se recomienda la programación periódica para la tarea de actualización del grupo de Kaspersky Endpoint Security. El valor del período de aleatorización debe ser de una hora en este caso.

Tarea de inventario de software

El número de archivos ejecutables recibidos a través del Servidor de administración de un solo dispositivo no puede ser superior a 150.000. Una vez que Kaspersky Security Center alcanza este límite, no podrá recibir ningún nuevo archivo.

Normalmente, la cantidad de archivos en un dispositivo cliente común no supera los 60.000. La cantidad de archivos ejecutables en un servidor de archivos puede ser mayor e incluso superar el umbral de 150.000.

Las mediciones de prueba han demostrado que la tarea de inventario obtiene los siguientes resultados en un dispositivo que ejecuta el sistema operativo Windows 7 con Kaspersky Endpoint Security 11 instalado y sin aplicaciones de terceros instaladas:

- Con las casillas de verificación **Inventario de módulos DLL** e **Inventario de archivos Script** desactivadas: aproximadamente 3000 archivos.
- Con el **inventario de módulos DLL** y las casillas de verificación de **Inventario de archivos de script** seleccionadas: de 1.0000 a 20.000 archivos, dependiendo de la cantidad de paquetes de servicio del sistema operativo instalados.
- Con solo la casilla de verificación **Inventario de archivos de script** seleccionada: aproximadamente 10.000 archivos.

Detalles de la repartición de carga de red entre el Servidor de administración y los dispositivos protegidos

Esta sección proporciona los resultados de las mediciones de prueba del tráfico de red con una descripción de las condiciones en las que se realizaron dichas mediciones. Puede consultar esta información cuando planifique la infraestructura de red y la capacidad de rendimiento de los canales de red dentro de su organización (o entre el Servidor de administración y otra organización con dispositivos para proteger). Al conocer la capacidad de rendimiento de la red, también puede estimar aproximadamente cuánto tiempo tardarán las diferentes operaciones de transmisión de datos.

Consumo de tráfico en varios escenarios

La siguiente tabla muestra los resultados de las pruebas de medición realizadas en el tráfico entre el Servidor de administración y un dispositivo administrado en diferentes escenarios.

De manera predeterminada, los dispositivos se sincronizan con el Servidor de administración cada 15 minutos o con un intervalo más largo. Sin embargo, si modifica la configuración de una directiva o tarea en el Servidor de administración, se produce una sincronización temprana en los dispositivos a los que se aplica esa directiva/tarea, de modo que la nueva configuración se transmite a los dispositivos.

Tasa de tráfico entre el Servidor de administración y el dispositivo administrado

Escenario	Tráfico del Servidor de administración a cada dispositivo administrado	Tráfico de cada dispositivo administrado al Servidor de administración
Instalación de Kaspersky Endpoint Security 11.7 para Windows con bases de datos actualizadas	390 MB	3,3 MB
Instalación del Agente de red	75 MB	397 KB
Instalación simultánea del Agente de red y de Kaspersky Endpoint Security 11.7 para Windows	459 MB	3,6 MB
Actualización inicial de las bases de datos antivirus sin actualizar las bases de datos en el paquete (si se deshabilita la participación en Kaspersky Security Network)	113 MB	1,8 MB
Actualización diaria de bases de datos antivirus (si se activa la participación en Kaspersky Security Network)	22 MB	373 MB
Sincronización inicial antes de la actualización de las bases de datos en un dispositivo (transferencia de directivas y tareas)	382 KB	446 KB
Sincronización inicial después de la actualización de las bases de datos en un dispositivo	20 KB	157 KB
Sincronización sin cambios en el Servidor de administración (según la planificación)	18 KB	23 KB
Sincronización cuando se cambia un solo ajuste en una directiva de grupo (tan pronto como se modifique la configuración)	19 KB	20 KB

Sincronización cuando se cambia un solo ajuste en una tarea de grupo (tan pronto como se modifique la configuración)	14 KB	11 KB
Forzar sincronización	110 KB	109 KB
Evento **Virus detectado** (1 virus)	44 KB	50 KB
Evento **Virus detectado** (10 virus)	58 KB	77 KB
Tráfico único después de habilitar la lista de registro de aplicaciones	hasta 10 KB	hasta 12 KB
Tráfico diario cuando la lista de registro de aplicaciones está habilitada	hasta 840 KB	hasta 1 MB

Uso promedio de tráfico por 24 horas

El uso promedio de tráfico en 24 horas entre el Servidor de administración y un dispositivo administrado es el siguiente:

- El tráfico del Servidor de administración al dispositivo administrado utiliza 840 KB.
- El tráfico del dispositivo administrado al Servidor de administración utiliza 1 MB.

El tráfico se ha medido en las siguientes condiciones:

- Dispositivo administrado con Agente de red y Kaspersky Endpoint Security 11.6 para Windows instalados.
- Ningún punto de distribución asignado al dispositivo.
- Administración de vulnerabilidades y parches desactivada.
- Frecuencia de sincronización con el Servidor de administración: 15 minutos.

Contactar con el Servicio de Soporte Técnico

Esta sección describe cómo obtener soporte técnico y las condiciones en que está disponible.

Cómo obtener soporte técnico

Si no encuentra una solución a su problema en la documentación de Kaspersky Security Center o en alguna de las fuentes de información sobre Kaspersky Security Center, póngase en contacto con el Servicio de soporte técnico. Los especialistas del Servicio de soporte técnico responderán a todas sus preguntas sobre la instalación y el uso de Kaspersky Security Center.

Kaspersky proporciona asistencia a Kaspersky Security Center durante su ciclo de vida (consulte la página del ciclo de vida de soporte del producto). Antes de ponerse en contacto con el Servicio de Soporte Técnico lea las reglas de asistencia.

Puede ponerse en contacto con el Servicio de soporte técnico de una de las siguientes formas:

- Visitando el sitio web del Servicio de soporte técnico
- Mediante una solicitud al Servicio de Soporte Técnico, desde el portal Kaspersky CompanyAccount.

Servicio de soporte técnico a través de Kaspersky CompanyAccount

Kaspersky CompanyAccount es un portal para las empresas que utilizan las aplicaciones Kaspersky. El portal Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los especialista de Kaspersky mediante solicitudes en línea. Puede usar Kaspersky CompanyAccount para rastrear el estado de sus solicitudes en línea y también almacenar un historial de ellas.

Puede registrar a todos los empleados de su organización en una única cuenta de Kaspersky CompanyAccount. Esta cuenta única le permite administrar de forma centralizada las solicitudes electrónicas que envían los empleados registrados a Kaspersky, además de administrar los privilegios de estos empleados mediante Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los idiomas siguientes:

- Inglés
- Español
- Italiano
- Alemán
- Polaco
- Portugués
- Ruso

- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el sitio web del Servicio de Soporte Técnico.

Fuentes de información sobre la aplicación

Página de Kaspersky Security Center en el sitio web de Kaspersky

En la página de Kaspersky Security Center en el sitio web de Kaspersky, puede ver información general sobre la aplicación, sus funciones y características.

La página de Kaspersky Security Center en la Base de conocimientos

La *Base de conocimientos* es una sección en el sitio web del Servicio de soporte técnico de Kaspersky.

En la página de Kaspersky Security Center en la Base de conocimientos, puede leer artículos que proporcionan información útil, recomendaciones, y respuestas a las preguntas más frecuentes sobre cómo comprar, instalar, y utilizar la aplicación.

Los artículos en la Base de conocimiento pueden proporcionar respuestas a preguntas relacionadas tanto con Kaspersky Security Center como con otras aplicaciones de Kaspersky. Los artículos en la base de conocimiento también pueden contener noticias del Servicio de soporte técnico.

Discuta sobre las aplicaciones de Kaspersky con la comunidad

Si su pregunta no requiere una respuesta inmediata, puede tratarla con expertos de Kaspersky y otros usuarios en nuestro Foro.

En el Foro puede ver los temas de debate, publicar sus comentarios y crear nuevos temas de debate.

> Se requiere una conexión a Internet para acceder a los recursos del sitio web.

Si no puede encontrar una solución a su problema, comuníquese con el Servicio de soporte técnico.

Glosario

Actualización

Procedimiento de sustitución o adición de nuevos archivos (bases de datos o módulos de la aplicación), recibidos desde los servidores de actualización de Kaspersky.

Actualización disponible

Conjunto de actualizaciones para los módulos de aplicación de Kaspersky, incluidas las actualizaciones críticas acumuladas durante cierto período de tiempo y los cambios en la arquitectura de la aplicación.

Administración de aplicaciones centralizada

Administración de aplicaciones remota usando los servicios de administración proporcionados en Kaspersky Security Center.

Administración de identidades y acceso (IAM)

El servicio AWS que permite la administración del acceso de usuario a otros servicios y recursos AWS.

Administración directa de aplicaciones

Administración de aplicaciones a través de una interfaz local.

Administrador de clientes

Empleado de una organización cliente que es responsable de supervisar el estado de la protección antivirus.

Administrador de Kaspersky Security Center

La persona que administra las operaciones de la aplicación a través del sistema de administración centralizada remota de Kaspersky Security Center.

Administrador del proveedor de servicio

Integrante del personal de un proveedor de servicio de protección antivirus. Este administrador realiza trabajos de instalación y mantenimiento de sistemas de protección antivirus basados en productos antivirus de Kaspersky y presta soporte técnico a los clientes.

Agente de autenticación

Interfaz que le permite completar la autenticación para acceder a los discos duros cifrados y cargar el sistema operativo después de que el disco duro de arranque se haya cifrado.

Agente de red

Componente de Kaspersky Security Center que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky que se instalan en un nodo de red específico (estación de trabajo o servidor). Este componente es común para todas las aplicaciones de empresa para Microsoft® Windows®. Existen versiones independientes del Agente de red para las aplicaciones Kaspersky desarrolladas para sistemas operativos tipo Unix y macOS.

Aplicación incompatible

Aplicación antivirus de un desarrollador externo o una aplicación Kaspersky que no admite la administración a través de Kaspersky Security Center.

Archivo clave

Un archivo con el formato xxxxxxxx.key que permite utilizar una aplicación Kaspersky según las disposiciones de una licencia comercial o de prueba.

Bases de datos antivirus

Bases de datos que contienen información sobre las amenazas de seguridad informática conocidas por Kaspersky desde el momento en que se lanzan las bases de datos antivirus. Las entradas en las bases de datos antivirus permiten detectar códigos maliciosos en objetos analizados. Las bases de datos antivirus las crean especialistas de Kaspersky y se actualizan cada hora.

Brote de virus

Serie de intentos deliberados de infectar un dispositivo con un virus.

Carpeta de copia de seguridad

Carpeta especial para el almacenamiento de copias de datos del Servidor de administración creados mediante la utilidad de copia de seguridad.

Certificado compartido

Certificado diseñado para identificar el dispositivo móvil del usuario.

Certificado del Servidor de administración

El certificado que utiliza el Servidor de administración para la autenticación en las Consolas de administración y para el intercambio de datos con los dispositivos cliente. El certificado se crea automáticamente cuando instala el Servidor de administración y luego se almacena en el Servidor de administración.

Clave activa

Una clave que la aplicación está utilizando actualmente.

Clave de acceso de AWS IAM

Combinación que consiste en el id. de clave (similar a "AKIAIOSFODNN7EXAMPLE") y la clave secreta (similar a "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Este par pertenece al usuario de IAM y se usa para obtener el acceso a servicios AWS.

Clave de suscripción adicional

Clave que certifica el derecho a usar la aplicación, pero que no se utiliza actualmente.

Cliente del Servidor de administración (dispositivo cliente)

Dispositivo, servidor o estación de trabajo donde el Agente de red está instalado y se ejecutan las aplicaciones administradas por Kaspersky.

Complemento de administración

Componente especializado que proporciona la interfaz para la administración de aplicaciones, a través de la Consola de administración. Cada aplicación tiene su propio complemento. Se incluye en todas las aplicaciones de Kaspersky que se pueden administrar mediante Kaspersky Security Center.

Configuración de programa

La configuración de la aplicación que es común a todos los tipos de tareas y rige el funcionamiento general de la aplicación, como la configuración de rendimiento de la aplicación, la configuración de informes y la configuración de la copia de seguridad.

Configuración de tarea

Configuraciones de aplicación que son específicas para cada tipo de tarea.

Consola de administración

Componente de Kaspersky Security Center que ofrece una interfaz de usuario para los servicios administrativos del Servidor de administración y del Agente de red.

Consola de administración de AWS

Interfaz web para ver y administrar los recursos de AWS. La consola de administración de AWS está disponible en la web en https://aws.amazon.com/es/console

Copia de seguridad de datos del Servidor de administración

Copia de los datos del Servidor de administración para la copia de seguridad y restauración posterior realizada usando la utilidad de copia de seguridad. La utilidad puede guardar lo siguiente:

- Base de datos del Servidor de administración (directivas, tareas, parámetros de la aplicación, eventos guardados en el Servidor de administración)
- Información de configuración de la estructura de los grupos de administración y los dispositivos cliente
- Repositorio de los archivos de instalación para la instalación remota de aplicaciones (contenido de las carpetas: paquetes y actualizaciones sin instalar)
- Certificado del Servidor de administración

Derechos de administrador

Nivel de derechos y privilegios de usuario necesario para la administración de objetos Exchange de una organización Exchange.

Directiva

Una directiva determina la configuración de una aplicación y administra la capacidad de configurar esa aplicación en equipos en un plazo de un grupo de administración. Se debe crear una directiva individual para cada aplicación. Puede crear múltiples directivas para las aplicaciones instaladas en los equipos en cada grupo de administración, pero solo puede aplicarse una directiva a la vez a cada aplicación dentro de un grupo de administración.

Dispositivo con protección de UEFI

Dispositivo con Kaspersky Anti-Virus para UEFI integrado al nivel de BIOS. La protección integrada garantiza la seguridad del dispositivo a partir del momento en que se inicia el sistema, mientras la protección en dispositivos sin el software integrado solo comienza a funcionar después de que se inicie la aplicación de seguridad.

Dispositivo EAS

Dispositivo móvil conectado al Servidor de administración mediante el protocolo Exchange ActiveSync. Los dispositivos con sistemas operativos iOS, Android y Windows Phone® se pueden conectar y administrar mediante el protocolo de Exchange ActiveSync.

Dispositivo KES

Dispositivo móvil que se conecta al Servidor de administración y se administra mediante Kaspersky Endpoint Security for Android.

Dispositivo MDM con iOS

Dispositivo móvil conectado al Servidor de MDM para iOS mediante el protocolo de MDM de iOS. Los dispositivos en los que se utiliza el sistema operativo iOS se pueden conectar y administrar mediante el protocolo de MDM de iOS.

Dispositivos administrados

Dispositivos de red corporativos incluidos en un grupo de administración.

Dominio de difusión

Área lógica de una red en que todos los nodos pueden intercambiar datos a través de un canal de difusión en OSI (modelo de referencia básico de interconexión de sistemas abiertos).

Entorno de nube

Máquinas virtuales y otros recursos virtuales ubicados en una plataforma de nube y organizados en redes.

Estación de trabajo del administrador

Un dispositivo con la Consola de administración instalada. Este componente proporciona una interfaz de administración de Kaspersky Security Center.

La estación de trabajo del administrador se utiliza para configurar y administrar el lado del servidor de Kaspersky Security Center. Utilizando la estación de trabajo del administrador, el administrador crea y administra un sistema de protección antivirus centralizado para una LAN corporativa basada en las aplicaciones de Kaspersky.

Estado de la protección

Estado actual de la protección, que define el nivel de seguridad del equipo.

Estado de la protección de la red

Estado de la protección en un momento dado que define la seguridad de los dispositivos de red corporativos. El estado de la protección de la red incluye factores como las aplicaciones de seguridad instaladas, el uso de claves de licencia y la cantidad y los tipos de amenazas detectadas.

Función de IAM

Conjunto de derechos para realizar solicitudes a servicios basadosen AWS. Las funciones de IAM no están vinculadas a un usuario o grupo específico, ya que facilitan derechos de acceso sin las claves de acceso de AWS IAM. Puede asignar una función de IAM a usuarios de IAM, instancias EC2 y aplicaciones o servicios basados en AWS.

Gravedad del evento

Una propiedad de un evento encontrado durante el funcionamiento de una aplicación de Kaspersky. Podemos encontrar los siguientes niveles de gravedad:

- Evento crítico
- Fallo operativo
- Advertencia
- Información

Los eventos del mismo tipo pueden tener diferentes niveles de gravedad, en función de la situación en la que se hayan producido.

Grupo de administración

Conjunto de dispositivos agrupados por función y por las aplicaciones de Kaspersky instaladas. Los dispositivos están agrupados como una sola entidad para facilitar su administración. Un grupo puede incluir otros grupos. Se pueden crear directivas de grupo y tareas de grupo para cada aplicación instalada en el grupo.

Grupo de aplicaciones con licencia

Grupo de aplicaciones creadas según los criterios que estableció un administrador (por ejemplo, el proveedor) para las que se mantienen las estadísticas de instalaciones realizadas en los dispositivos cliente.

Grupo de funciones

Grupo de usuarios de dispositivos móviles de Exchange ActiveSync a quienes se ha concedido derechos de administrador idénticos.

HTTPS

Protocolo de seguridad para la transferencia de datos, que utiliza cifrado, entre un navegador y un servidor web. HTTPS se utiliza para tener acceso a información restringida, como datos corporativos o financieros.

Imagen de máquina de Amazon (AMI)

La plantilla que contiene la configuración del software necesaria para ejecutar la máquina virtual. Varias instancias se pueden crear según una única AMI.

Instalación forzada

Método para la instalación remota de aplicaciones de Kaspersky que permite instalar software en dispositivos cliente específicos. Para realizar la instalación forzada con éxito, la cuenta utilizada para la tarea deberá contar con los derechos suficientes para la ejecución remota de aplicaciones en dispositivos cliente. Este método se recomienda para instalar aplicaciones en dispositivos que ejecutan sistemas operativos Microsoft Windows y admiten esta funcionalidad.

Instalación local

La instalación de una aplicación de seguridad en un dispositivo de una red corporativa que presupone el inicio de instalación manual desde el paquete de distribución de la aplicación de seguridad o el inicio manual de un paquete de instalación publicado previamente descargado en el dispositivo.

Instalación manual

Instalación de una aplicación de seguridad en un dispositivo de una red corporativa desde el paquete de distribución. La instalación manual requiere la participación de un administrador u otro especialista de TI. Por lo general, la instalación manual se lleva a cabo si la instalación remota se completa con un error.

Instalación remota

Instalación de aplicaciones Kaspersky mediante servicios facilitados por Kaspersky Security Center.

Instancia de Amazon EC2

Máquina virtual creada según una imagen AMI mediante servicios web de Amazon.

Interfaz de programación de aplicaciones de AWS (API de AWS)

Interfaz para programas de aplicación de la plataforma AWS que utiliza Kaspersky Security Center. Específicamente, las herramientas de API de AWS se utilizan para sondear el segmento de la nube e instalar el Agente de red en instancias.

JavaScript

Lenguaje de programación que amplía el rendimiento de las páginas web. Las páginas web creadas mediante JavaScript pueden realizar funciones (por ejemplo, cambiar la vista de elementos de la interfaz o abrir ventanas adicionales) sin tener que actualizar la página con nuevos datos del servidor web. Para ver páginas creadas usando JavaScript, active la compatibilidad con JavaScript en la configuración de su navegador.

Kaspersky Private Security Network (KSN privada)

Kaspersky Private Security Network es una solución que ofrece acceso a las bases de datos de reputación de Kaspersky Security Network y otros datos estadísticos a los usuarios de dispositivos con aplicaciones instaladas de Kaspersky acceso a las bases de datos de reputación de Kaspersky Security Network y otros datos estadísticos sin enviar datos desde sus dispositivos a Kaspersky Security Network. Kaspersky Private Security Network está diseñado para clientes corporativos que no pueden participar en Kaspersky Security Network por alguna de las siguientes razones:

- Los dispositivos del usuario no están conectados a Internet.
- La transmisión de datos fuera del país o de la LAN corporativa está prohibida por ley o por las directivas de seguridad corporativas.

Kaspersky Security Network (KSN)

Una infraestructura de servicios en la nube que proporciona acceso a la base de datos de Kaspersky con información actualizada constantemente sobre la reputación de los archivos, recursos web y software. Kaspersky Security Network garantiza respuestas más rápidas de las aplicaciones Kaspersky a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsos positivos.

Nivel de importancia del parche

Atributo del parche. Hay cinco niveles de importancia para parches de Microsoft y parches de terceros:

- Crítico
- Alta
- Media
- Mínimo

- Desconocido

El nivel de importancia de un parche de terceros o parche de Microsoft está determinado por el nivel de gravedad más alto entre las vulnerabilidades que los parches deben solucionar.

Operador de Kaspersky Security Center

Usuario que supervisa el estado y la operación de un sistema de protección administrada con Kaspersky Security Center.

Paquete de instalación

Un conjunto de archivos creados para la instalación remota de una aplicación de Kaspersky mediante el sistema de administración remota de Kaspersky Security Center. El paquete de instalación contiene un intervalo de configuraciones necesarias para instalar la aplicación y ejecutarla inmediatamente después. La configuración corresponde a la configuración predeterminada de las aplicaciones. El paquete de instalación consta de archivos con extensiones .kpd y .kud que se incluyen en el kit de distribución de la aplicación.

Perfil

Conjunto de opciones de configuración de dispositivos móviles Exchange que define su comportamiento cuando están conectados a un servidor Exchange de Microsoft.

Perfil de aprovisionamiento

Conjunto de parámetros de configuración para el funcionamiento de las aplicaciones en dispositivos móviles de iOS. Un perfil de aprovisionamiento contiene información sobre la licencia y está vinculado a una aplicación específica.

Perfil de configuración

Directiva que incluye un conjunto de parámetros y restricciones para un dispositivo móvil con MDM de iOS.

Perfil de MDM para iOS

Conjunto de parámetros de configuración para conectar dispositivos móviles de iOS al Servidor de administración. El usuario instala un perfil de MDM para iOS a un dispositivo móvil y, a continuación, conecta este dispositivo móvil al Servidor de administración.

Periodo de vigencia de la licencia

El periodo de licencia es el tiempo durante el que tiene acceso a las funciones de la aplicación y a los derechos para usar servicios adicionales. Los servicios que se pueden utilizar dependerán del tipo de licencia.

Propietario del dispositivo

El propietario del dispositivo es un usuario que el administrador puede comunicarse cuando es necesario efectuar determinadas operaciones con un dispositivo cliente.

Protección antivirus de la red

Conjunto de medidas técnicas y organizativas que disminuyen el riesgo de que entren virus y spam a la red de una organización, y evitan ataques, phishing y otras amenazas contra la red. La seguridad de la red aumenta cuando usa aplicaciones de seguridad y servicios y cuando aplica y se adhiere a la directiva de seguridad de los datos corporativos.

Protección antivirus: proveedor de servicio

Organización que proporciona a una organización cliente servicios de protección antivirus sobre la base de soluciones de Kaspersky.

Puerta de enlace de conexión

Una *puerta de enlace de conexión* es un Agente de red que actúa en un modo especial. Una puerta de enlace de conexión acepta conexiones de otros Agentes de red y las conecta al Servidor de administración a través de su propia conexión con el Servidor. A diferencia de un Agente de red normal, una puerta de enlace de conexión espera las conexiones del Servidor de administración en lugar de establecer conexiones con el Servidor de administración.

Punto de distribución

Equipo que tiene Agente de red instalado y se utiliza para la distribución de actualizaciones, la instalación remota de aplicaciones, la obtención de información sobre equipos en un grupo de administración o dominio de difusión. Los puntos de distribución se han diseñado para reducir la carga del Servidor de administración durante la distribución de actualizaciones y para optimizar el tráfico de red. Los puntos de distribución se pueden asignar de forma automática mediante el Servidor de administración o bien de forma manual por parte del administrador. El punto de distribución se conocía previamente como el agente de actualización.

Repositorio de eventos

Una parte de la base de datos del Servidor de administración dedicada al almacenamiento de información sobre eventos que ocurren en Kaspersky Security Center.

Restauración

Reubicación del objeto original de la Cuarentena o Copia de seguridad a su carpeta original donde el objeto había sido almacenado antes de su puesta en cuarentena, desinfección o eliminación, o en una carpeta definida por un usuario.

Restauración de los datos del Servidor de administración

Restauración de los datos del Servidor de administración a partir de la información guardada en la copia de seguridad mediante la utilidad de copia de seguridad. La utilidad puede restaurar lo siguiente:

- Base de datos del Servidor de administración (directivas, tareas, parámetros de la aplicación, eventos guardados en el Servidor de administración)
- Información de configuración de la estructura de los grupos de administración y los equipos de cliente
- Repositorio de los archivos de instalación para la instalación remota de aplicaciones (contenido de las carpetas: paquetes y actualizaciones sin instalar)
- Certificado del Servidor de administración

Servidor de administración

Componente de Kaspersky Security Center que almacena de forma centralizada la información sobre todas las aplicaciones Kaspersky que estén instaladas en la red de la empresa. También puede utilizarse para administrar estas aplicaciones.

Servidor de administración principal

El Servidor de administración principal es el Servidor de administración que se especificó durante la instalación del Agente de red. El Servidor de administración principal se puede utilizar en la configuración de perfiles de conexión del Agente de red.

Servidor de administración virtual

Componente de Kaspersky Security Center diseñado para la administración del sistema de protección de la red de la organización cliente.

El Servidor de administración virtual es un tipo concreto de Servidor de administración secundario y, en comparación con un Servidor de administración físico, tiene las siguientes restricciones:

- El Servidor de administración virtual solo se puede crear en un Servidor de administración principal.
- Durante su funcionamiento, el Servidor de administración Virtual utiliza la base de datos del Servidor de administración principal. Las tareas de copia de seguridad y restauración de datos, así como las tareas de exploración y descarga de actualizaciones, no son compatibles con un Servidor de administración virtual.
- El Servidor virtual no permite la creación de Servidores de administración secundarios (incluidos los Servidores virtuales).

Servidor de dispositivos móviles

Componente de Kaspersky Security Center que proporciona acceso a dispositivos móviles y permite administrarlos con la Consola de administración.

Servidor de dispositivos móviles de Exchange

Componente de Kaspersky Security Center que le permite conectar dispositivos móviles de Exchange ActiveSync al Servidor de administración.

Servidor de MDM para iOS

Componente de Kaspersky Security Center instalado en un dispositivo cliente y que permite que los dispositivos móviles de iOS se conecten al Servidor de administración. También hace posible gestionar dispositivos móviles iOS mediante Apple Push Notifications (APNs).

Servidor web de Kaspersky Security Center

Un componente de Kaspersky Security Center que se instala junto con el Servidor de administración. El Servidor web está diseñado para publicar paquetes de instalación independientes, perfiles de MDM de iOS y archivos de una carpeta compartida a través de una red.

Servidores de actualización de Kaspersky

Servidores HTTP(S) de Kaspersky desde los que las aplicaciones Kaspersky descargan las actualizaciones para las bases de datos y los módulos de la aplicación.

SSL

Protocolo de cifrado de datos usado en Internet y redes locales. El protocolo SSL (capa de conexión segura) se utiliza en aplicaciones web para crear una conexión segura entre un cliente y servidor.

System Health Validator (SHV) de Kaspersky Security Center

Un componente de Kaspersky Security Center diseñado para comprobar la capacidad de funcionamiento del sistema operativo en caso de la operación simultánea de Kaspersky Security Center y de Microsoft NAP.

Tarea

Las funciones realizadas por la aplicación Kaspersky se implementan como tareas, como: protección de archivos en tiempo real, análisis completo del equipo y actualización de las bases de datos.

Tarea de grupo

Tarea definida para un grupo de administración y ejecutada en todos los dispositivos cliente incluidos en ese grupo de administración.

Tarea local

Una tarea definida y ejecutada en un único equipo de cliente.

Tarea para dispositivos específicos

Tarea asignada a un conjunto de dispositivos cliente de grupos de administración arbitrarios y realizados en dichos dispositivos.

Tienda de aplicaciones

Componente de Kaspersky Security Center. La Tienda de aplicaciones se utiliza para instalar aplicaciones en dispositivos Android que pertenecen a los usuarios. La Tienda de aplicaciones le permite publicar los archivos APK de aplicaciones y enlaces a aplicaciones en Google Play.

Umbral de la actividad de virus

Número máximo de eventos permitidos de un tipo específico en un intervalo de tiempo limitado. Cuando se supera, se interpreta como un aumento de la actividad de virus y una amenaza de brote de virus. Esta propiedad es importante durante los periodos de brotes de virus, puesto que permite que los administradores reaccionen a tiempo cuando se producen amenazas de ataque de virus.

Usuario de IAM

El usuario de servicios AWS. Un usuario de IAM puede tener los derechos de realizar el sondeo de segmento de la nube.

Usuarios internos

Las cuentas de los usuarios internos se utilizan para trabajar con Servidores de administración virtuales. Kaspersky Security Center otorga los derechos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo en Kaspersky Security Center. No se transfiere ningún dato de los usuarios internos al sistema operativo. Kaspersky Security Center autentifica los usuarios internos.

Vulnerabilidad

Defecto de un sistema operativo o una aplicación que puede ser explotado por desarrolladores de malware para introducirse en ellos y dañar su integridad. La presencia de una gran cantidad de vulnerabilidades en un sistema operativo lo hace poco fiable, ya que los virus que se introducen en el sistema operativo pueden causar interrupciones en su funcionamiento y en las aplicaciones instaladas.

Windows Server Update Services (WSUS)

Aplicación que se usa para distribuir las actualizaciones de aplicaciones de Microsoft en los equipos de usuarios que se encuentren conectados a la red de una organización.

Zona desmilitarizada (DMZ)

La zona desmilitarizada es un segmento de una red local que contiene servidores que responden a las solicitudes de la Web global. Para garantizar la seguridad de la red local de una organización, el acceso a la LAN desde la zona desmilitarizada se protege mediante un firewall.

Información sobre el código de terceros

La información sobre el código de terceros se encuentra en el archivo legal_notices.txt, en la carpeta de instalación de la aplicación.

Avisos de marcas comerciales

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos dueños.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista, y Windows Azure son marcas comerciales del grupo de compañías Microsoft.

Adobe, Acrobat, Flash, Shockwave y PostScript son marcas comerciales registradas o marcas comerciales de Adobe en los Estados Unidos y/o en otros países.

AirPlay, AirDrop, AirPrint, App Store, Apple, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime, y Touch ID son marcas comerciales de Apple Inc., registradas en los EE. UU. y en otros países y regiones.

AMD, AMD64 son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace son marcas comerciales de Amazon.com, Inc. o sus filiales en los Estados Unidos y/o en otros países.

Android, Chrome, Chromium, Dalvik, Firebase, Google, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts y YouTube son marcas comerciales de Google LLC.

Apache y el logotipo de la pluma de Apache son marcas comerciales de Apache Software Foundation.

BlackBerry pertenece a Research In Motion Limited y está registrada en los Estados Unidos y puede estar registrada o pendiente de registro en otros países.

La palabra Bluetooth, su marca y sus logotipos de Bluetooth SIG, Inc.

Chef es una marca comercial o marca comercial registrada de Progress Software Corporation y/o una de sus subsidiarias o filiales en los Estados Unidos y/o en otros países.

Cisco, Cisco Systems, Cisco Jabber, iOS son marcas registradas o marcas comerciales de Cisco Systems, Inc. y sus filiales en los Estados Unidos y en otros países.

CVE es una marca registrada de The MITRE Corporation.

Citrix, XenServer son marcas comerciales de Citrix Systems, Inc. y/o una o más de sus subsidiarias, y pueden estar registradas en la Oficina de Marcas y Patentes de los Estados Unidos y en otros países.

Corel es una marca comercial o una marca registrada de Corel Corporation y/o sus subsidiarias en Canadá, los Estados Unidos y/o en otros países.

Debian es una marca comercial registrada de Software in the Public Interest, Inc.

Dropbox es una marca comercial de Dropbox, Inc.

FusionCompute, FusionSphere son marcas comerciales de Huawei Technologies Co., Ltd registradas en China y otros países.

Firebird es una marca comercial registrada de Firebird Foundation.

Foxit es una marca registrada de Foxit Corporation.

Firefox, Mozilla, Thunderbird son marcas registradas de Mozilla Foundation.

FreeBSD es una marca comercial registrada de FreeBSD Foundation.

Oracle, Java, JavaScript y TouchDown son marcas registradas de Oracle y/o sus filiales.

OpenAPI es una marca comercial de The Linux Foundation.

QRadar, IBM son marcas comerciales de International Business Machines Corporation, registrada en muchas jurisdicciones en todo el mundo.

Intel, Core, Xeon son marcas comerciales de Intel Corporation en los EE. UU. y/o en otros países.

CentOS es una marca registrada de Red Hat, Inc.

Ansible, Fedora, Red Hat y Red Hat Enterprise Linux son marcas comerciales o marcas comerciales registradas de Red Hat Inc. o sus subsidiarias en los Estados Unidos y otros países.

Linux es la marca registrada de Linus Torvalds en EE. UU. y otros países.

Logitech es una marca comercial registrada o una marca comercial de Logitech en los Estados Unidos y/o en otros países.

Micro Focus es una marca comercial o una marca comercial registrada de Micro Focus (IP) Limited o sus subsidiarias en el Reino Unido, Estados Unidos y otros países.

Node.js es una marca comercial de Joyent, Inc.

Novell y Netware son marcas registradas de Novell Inc. en Estados Unidos y otros países.

Parallels y el logotipo de Parallels son marcas comerciales o marcas comerciales registradas de Parallels International GmbH en Canadá, Estados Unidos u otros lugares.

Puppet es una marca comercial o marca comercial registrada de Puppet, Inc.

Python es una marca comercial o una marca comercial registrada de Python Software Foundation.

Radmin es una marca comercial registrada de Famatech.

Samsung es una marca comercial de SAMSUNG en los Estados Unidos u otros países.

SPL, Splunk son marcas comerciales y marcas comerciales registradas de Splunk Inc. en Estados Unidos y otros países.

Symbian es una marca comercial que pertenece a Symbian Foundation Ltd.

SUSE es una marca registrada de SUSE LLC en Estados Unidos y otros países.

Ubuntu es una marca registrada de Canonical Ltd.

UNIX es una marca registrada en Estados Unidos y otros países, con licencia exclusiva a través de X/Open Company Limited.

Zabbix es una marca registrada de Zabbix SIA.

VMware, VMware vSphere y VMware Workstation son marcas comerciales registradas o marcas comerciales de VMware, Inc. en Estados Unidos y/o en otras jurisdicciones.

Problemas conocidos

Kaspersky Security Center 14 Web Console tiene una serie de limitaciones que no son críticas para el funcionamiento de la aplicación:

- Al iniciar sesión en Kaspersky Security Center 14 Web Console, si utiliza la autenticación de dominio y especifica un Servidor de administración virtual para conectarse, cierra la sesión y luego intenta iniciar sesión en el Servidor de administración principal, Kaspersky Security Center 14 Web Console se conecta al Servidor de administración virtual. Para conectarse al Servidor de administración principal, vuelva a abrir el navegador.

- Si especifica la configuración del servidor proxy en las propiedades del Servidor de administración y luego habilita la opción **No usar servidor proxy** en la tarea *Descargar actualizaciones en el repositorio del Servidor de administración*, esta opción se ignora y la conexión se establece a través del servidor proxy.

- Si abre Kaspersky Security Center 14 Web Console en diferentes navegadores y descarga el archivo de certificado del Servidor de administración en la ventana de propiedades del Servidor de administración, los archivos descargados tienen nombres diferentes.

- Se produce un error cuando intenta restaurar un objeto desde el repositorio **COPIA DE SEGURIDAD** (**OPERACIONES → REPOSITORIOS → COPIA DE SEGURIDAD**) o enviar el objeto a Kaspersky.

- Un dispositivo administrado que tiene más de un adaptador de red envía información al Servidor de administración sobre la dirección MAC del adaptador de red que no se usa para conectarse al Servidor de administración.

- La configuración bloqueada en una directiva de nivel superior de Kaspersky Endpoint Security for Linux se hereda, pero no se bloquea en las directivas secundarias.

- Después de actualizar a Kaspersky Security Center 14, si cambia de un Servidor de administración principal a uno secundario, luego vuelve al principal y luego intenta volver al secundario, Kaspersky Security Center 14 Web Console no puede abrir el Servidor secundario. Este problema solo se reproduce si está instalado el complemento web para Kaspersky Endpoint Security para Windows versión 11.9.

- En la Consola de administración basada en MMC, cuando crea una directiva para Kaspersky Industrial CyberSecurity for Linux Nodes 1.0, Kaspersky Security Center muestra un mensaje de error sobre la creación de un volcado de diagnóstico. Sin embargo, la directiva se crea correctamente.

- Puede eliminar una categoría de aplicaciones que haya añadido a la función Control de aplicaciones en la directiva de Kaspersky Endpoint Security for Linux.

- En un widget de gráfico circular en el tablero, no se cambia el color del texto a claro después de cambiar el tema de la consola a oscuro.

- Es posible que se muestre un estado incorrecto de una tarea local en la lista de tareas de las propiedades del dispositivo.

- Al añadir más de 200 exclusiones a una regla de Control de anomalías adaptativo, se muestra un mensaje de error en lugar de un mensaje de advertencia.

- En la sección **Categorías de aplicaciones**, si se muestra la columna **Utilizado en políticas**, no se puede ocultar.

- En la configuración de la tarea del *Servidor de administración de Cambios*, algunas opciones están mal colocadas.

- En la directiva del Agente de red, la sección **Programa de conexión** tiene un título incorrecto.

- El sondeo de la red de Windows rápido o completo devuelve un resultado vacío.

- Si utiliza la utilidad sysrep.exe para capturar la imagen del sistema operativo y añadir la configuración necesaria, el sistema operativo capturado se despliega sin esta configuración.

- Si instala Kaspersky Security Center 14 Web Console con Identity and Access Manager y luego cambia el Servidor de administración para Kaspersky Security Center 14 Web Console, Identity and Access Manager no obtiene la información sobre el nuevo Servidor de administración.

- Los botones **Restaurar** y **Enviar a Kaspersky** en la sección **OPERACIONES → REPOSITORIOS → COPIA DE SEGURIDAD** no funcionan.

- Al añadir un certificado en la sección **Certificados** de la ventana de propiedades del Servidor de administración, por ejemplo, un certificado de Servidor web, el botón **Cerrar** ("X") oculta el campo **Tipo de certificado** y se muestra un botón **Mostrar** innecesario.

- Recargar el servicio del Servidor de administración en un Servidor de administración secundario provoca la desconexión entre Kaspersky Security Center 14 Web Console y el Servidor de administración principal.

- Los mensajes de error de presuntos ataques de Zip Slip y Zip Bomb se muestran solo en inglés.

- La ventana de propiedades de una función no puede abrirse desde la lista de funciones asignadas al usuario.

- Las notificaciones no se pueden ordenar por fecha.

- En las propiedades de las actualizaciones de Microsoft, en la sección **Dispositivos**, la búsqueda por "Estado de instalación" y "Dirección IP" no está disponible.

- No se admite el despliegue de Windows 10, versión 2004, a través del Entorno de ejecución de prearranque (PXE).

- En las selecciones de eventos, los filtros nuevos no reemplazan a los filtros antiguos. Para evitar esto, puede eliminar manualmente los filtros antiguos.