KASPERSKY lab

Kaspersky Embedded Systems Security

Guía del administrador

Versión de la aplicación: 2.2.0.605

Estimado usuario:

Gracias por elegir Kaspersky Lab como su proveedor de software de seguridad. Esperamos que este documento le ayude a usar nuestro producto.

Fecha de la revisión del documento: 07.12.2018

https://latam.kaspersky.com/
https://support.kaspersky.com/mx

Contenido

Acerca de esta guía

La Guía del usuario de Kaspersky Embedded Systems Security 2.2.0.605 (en adelante, denominada “Kaspersky Embedded Systems Security 2.2”, “la aplicación”) fue creada para especialistas que instalan y administran Kaspersky Embedded Systems Security 2.2 en todos los dispositivos protegidos, y para especialistas que proporcionan soporte técnico a organizaciones mediante Kaspersky Embedded Systems Security 2.2.

Esta guía contiene información sobre cómo configurar y usar Kaspersky Embedded Systems Security 2.2.

La Guía también lo ayudará a conocer las fuentes de información sobre la aplicación y cómo recibir soporte técnico.

En este capítulo

En este documento

La Guía del administrador de Kaspersky Embedded Systems Security 2.2 contiene las siguientes secciones:

Fuentes de información acerca de Kaspersky Embedded Systems Security 2.2

Esta sección enumera las fuentes de información acerca de la aplicación.

Kaspersky Embedded Systems Security 2.2

Esta sección describe las funciones, los componentes y el kit de distribución de Kaspersky Embedded Systems Security 2.2, además de brindar una lista de requisitos de hardware y software de Kaspersky Embedded Systems Security 2.2.

Instalación y desinstalación de la aplicación

Esta sección proporciona instrucciones paso a paso para instalar y desinstalar Kaspersky Embedded Systems Security 2.2.

Interfaz de la aplicación

Esta sección brinda información sobre los elementos de la interfaz de Kaspersky Embedded Systems Security 2.2.

Licencia de la aplicación

Esta sección brinda información sobre los conceptos principales relacionados con el otorgamiento de una licencia de la aplicación.

Inicio y detención de Kaspersky Embedded Systems Security 2.2

Esta sección contiene la información sobre cómo iniciar y detener el Complemento de administración de Kaspersky Embedded Systems Security 2.2 (en adelante, denominado Complemento de administración) y el servicio de Kaspersky Security.

Acerca de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security 2.2

Esta sección contiene información acerca de los permisos para administrar Kaspersky Embedded Systems Security

2.2 y los servicios de Windows® registrados por la aplicación, e instrucciones sobre cómo configurar estos permisos.

Creación y configuración de directivas

Esta sección contiene información sobre la utilización de las directivas de Kaspersky Security Center para administrar Kaspersky Embedded Systems Security 2.2 en diferentes equipos.

Creación y configuración de tareas con Kaspersky Security Center

Esta sección contiene información sobre tareas de Kaspersky Embedded Systems Security 2.2 y cómo crearlas, configurarlas, iniciarlas y detenerlas.

Administración de las configuraciones de la aplicación

Esta sección contiene información acerca de cómo ajustar las configuraciones generales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center.

Protección del equipo en tiempo real

Esta sección brinda información sobre las tareas de la Protección del equipo en tiempo real: Protección de archivos en tiempo real, uso de KSN; y también la funcionalidad de Prevención de exploits. También brinda instrucciones sobre cómo configurar tareas de protección en tiempo real y cómo administrar la configuración de seguridad de un equipo protegido.

Control de actividad local

Esta sección proporciona información sobre la funcionalidad de Kaspersky Embedded Systems Security 2.2 que controla los inicios de aplicaciones y las conexiones a dispositivos externos mediante USB.

Control de actividad de red

Esta sección contiene la información sobre la tarea de administración de firewall.

Inspección del sistema

Esta sección contiene la información sobre la tarea del Monitor de integridad de archivos y funciones para inspeccionar el registro del sistema operativo.

Integración con sistemas de terceros

Esta sección describe la integración de Kaspersky Embedded Systems Security 2.2 con funciones y tecnologías de terceros.

Cómo utilizar Kaspersky Embedded Systems Security 2.2 desde la línea de comandos

Esta sección describe cómo utilizar Kaspersky Embedded Systems Security 2.2 desde la línea de comandos.

Comunicarse con el soporte técnico

Esta sección describe cómo se puede recibir soporte técnico y las condiciones en las cuales se encuentra disponible.

Glosario

Esta sección contiene la lista de términos que se mencionan en el documento, así como sus definiciones respectivas.

AO Kaspersky Lab

Esta sección proporciona información sobre AO Kaspersky Lab.

Información sobre código de terceros

Esta sección contiene información acerca del código de terceros usado en la aplicación.

Avisos de marcas registradas

Esta sección enumera las marcas comerciales reservadas a propietarios externos que se mencionan en el documento.

Índice

Esta sección le permite encontrar rápidamente la información necesaria en el documento.

Convenciones del documento

Este documento utiliza las siguientes convenciones (consulte la tabla que se encuentra a continuación).

Table 1. Convenciones del documento

Texto de ejemplo	Descripción de la convención del documento
Tenga en cuenta que...	Las advertencias están resaltadas en rojo y destacadas en un cuadro. Las advertencias contienen información sobre las acciones que pueden tener consecuencias no deseadas.
Le recomendamos que use...	Las notas están destacadas en un cuadro. Las notas contienen información complementaria y de referencia.
Por ejemplo: …	Los ejemplos se dan en letras de imprenta, con un fondo azul y debajo del título “Por ejemplo”.
Actualización significa... Se produce el evento Las bases de datos están desactualizadas.	Los siguientes elementos están en cursiva en el texto: • Términos nuevos • Nombres de eventos y estados de las aplicaciones
Presione INTRO. Presione ALT+F4.	Los nombres de las teclas del teclado aparecen en negrita y en mayúsculas. Los nombres de teclas conectados por el signo "+" (más) indican el uso de una combinación de teclas. Esas teclas se deben presionar simultáneamente.
Haga clic en el botón **Habilitar**.	Los nombres de los elementos de la interfaz de la aplicación, por ejemplo, cuadros de texto, elementos de menú y botones, están destacados en negrita.

Texto de ejemplo	Descripción de la convención del documento
► *Para configurar la programación de una tarea:*	Las frases introductorias de las instrucciones están en cursiva y tienen una flecha.
En la línea de comandos, escriba `help` Aparece el siguiente mensaje: Especifique la fecha en el formato `dd:mm:yy`.	Los siguientes tipos de contenido del texto están destacados con una fuente especial: • Texto en la línea de comandos • Texto de los mensajes que la aplicación muestra en la pantalla • Los datos se deben introducir desde el teclado
<Nombre de usuario>	Las variables se ponen entre corchetes angulares. En lugar de una variable, se debe insertar el valor correspondiente y omitir los corchetes angulares.

Fuentes de información acerca de Kaspersky Embedded Systems Security 2.2

Esta sección enumera las fuentes de información acerca de la aplicación.

Puede seleccionar la fuente de información más adecuada, según el nivel de importancia y la urgencia del problema.

En este capítulo

Fuentes para la recuperación de información independiente

Puede usar las siguientes fuentes para buscar información acerca de Kaspersky Embedded Systems Security 2.2:

- Página de Kaspersky Embedded Systems Security 2.2 en el sitio web de Kaspersky Lab.
- Página de Kaspersky Embedded Systems Security 2.2 en el sitio web de soporte técnico (base de conocimientos).
- Manuales.

Si no encontró una solución para su problema, póngase en contacto con el Servicio de soporte técnico de Kaspersky Lab https://support.kaspersky.com/mx.

Se requiere una conexión a Internet para usar las fuentes de información en línea.

Página de Kaspersky Embedded Systems Security 2.2 en el sitio web de Kaspersky Lab

En la página de Kaspersky Embedded Systems Security 2.2 (https://latam.kaspersky.com/enterprise-security/embedded-systems), puede consultar información general acerca de la aplicación, sus funciones y sus características.

La página de Kaspersky Embedded Systems Security 2.2 contiene un vínculo a la tienda en línea. Allí podrá comprar la aplicación o renovar la licencia.

Página de Kaspersky Embedded Systems Security 2.2 en la Base de conocimientos

La Base de conocimientos es una sección del sitio web del Servicio de soporte técnico.

La página de Kaspersky Embedded Systems Security 2.2 en la Base de conocimientos

(https://support.kaspersky.com/mx/kess2) incluye artículos que brindan información útil, recomendaciones y respuestas a las preguntas frecuentes sobre cómo comprar, instalar y usar la aplicación.

Los artículos de la base de conocimientos pueden responder preguntas relacionadas no solo con Kaspersky Embedded Systems Security 2.2, sino también con otras aplicaciones de Kaspersky Lab. Los artículos de la base de conocimientos también pueden incluir noticias de soporte técnico.

Documentación de Kaspersky Embedded Systems Security 2.2

La Guía del administrador de Kaspersky Embedded Systems Security 2.2 contiene información acerca de la instalación, la desinstalación, la configuración y el uso de la aplicación.

Foro sobre aplicaciones de Kaspersky Lab

Si su pregunta no requiere una respuesta inmediata, puede analizarla con los expertos de Kaspersky Lab y otros usuarios en nuestro foro http://forum.kaspersky.com/.

En este foro, puede ver conversaciones existentes, dejar comentarios y crear conversaciones nuevas.

Kaspersky Embedded Systems Security 2.2

Esta sección describe las funciones, los componentes y el kit de distribución de Kaspersky Embedded Systems Security 2.2, además de brindar una lista de requisitos de hardware y software de Kaspersky Embedded Systems Security 2.2.

En este capítulo

Acerca de Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 protege equipos y otros sistemas integrados que ejecutan Microsoft® Windows contra virus y otras amenazas del equipo. Los usuarios de Kaspersky Embedded Systems Security 2.2 son administradores de red corporativos y especialistas a cargo de la protección antivirus de la red corporativa.

Puede instalar Kaspersky Embedded Systems Security 2.2 en diversos sistemas integrados que ejecuten Windows, incluidos los siguientes tipos de dispositivos:

- Cajeros automáticos;
- TPV (terminal de punto de venta).

Kaspersky Embedded Systems Security 2.2 se puede administrar de las siguientes formas:

- Mediante la Consola de la aplicación instalada en el mismo equipo donde está instalado Kaspersky Embedded Systems Security 2.2 o en un equipo diferente.
- Mediante comandos en la línea de comandos.
- Mediante la Consola de administración de Kaspersky Security Center.

La aplicación Kaspersky Security Center también se puede utilizar para la administración centralizada de varios equipos que ejecutan Kaspersky Embedded Systems Security 2.2.

Es posible revisar los contadores de rendimiento de Kaspersky Embedded Systems Security 2.2 para la aplicación "Supervisor del sistema", además de los contadores y las capturas SNMP.

Componentes y funciones de Kaspersky Embedded Systems Security 2.2

La aplicación incluye los siguientes componentes:

- **Protección de archivos en tiempo real**. Kaspersky Embedded Systems Security 2.2 analiza los objetos cuando accede a ellos. Kaspersky Embedded Systems Security 2.2 analiza los siguientes objetos:
  - Archivos
  - Flujos de sistemas de archivos alternativos (flujos NTFS)
  - Registro de inicio maestro y sectores de inicio de los discos duros locales y las unidades extraíbles
- **Análisis a pedido**. Kaspersky Embedded Systems Security 2.2 ejecuta un solo análisis de la zona especificada en busca de virus y otras amenazas de seguridad informática. La aplicación analiza archivos, RAM y objetos de inicio en un equipo protegido.
- **Control de inicio de aplicaciones**. El componente rastrea los intentos de los usuarios de iniciar aplicaciones y controla los inicios de la aplicación en un equipo protegido.
- **Control de dispositivos**. El componente controla el registro y el uso de dispositivos del almacenamiento y unidades de CD/DVD a fin de proteger el equipo contra amenazas de seguridad informática que pueden surgir al intercambiar archivos con unidades flash conectadas mediante USB u otros tipos de dispositivos externos.
- **Administración de firewall**. Este componente proporciona la capacidad de administrar el firewall de Windows: configurar los ajustes y reglas de firewall del sistema operativo, y bloquear toda posibilidad de configuración externa del firewall.
- **Monitor de integridad de archivos**. Kaspersky Embedded Systems Security 2.2 detecta los cambios en los archivos dentro de las áreas de supervisión especificadas en los ajustes de la tarea. Estos cambios pueden indicar una violación de la seguridad en el equipo protegido.
- **Inspección de registros**. Este componente supervisa la integridad del ambiente protegido sobre la base de los resultados de una inspección de los registros de eventos de Windows.

Las siguientes funciones se implementan en la aplicación:

- **Actualización de bases de datos y actualización de módulos del programa.** Kaspersky Embedded Systems Security 2.2 descarga las actualizaciones de las bases de datos y los módulos de la aplicación desde los servidores de actualización FTP o HTTP de Kaspersky Lab, el servidor de administración de Kaspersky Security Center u otros orígenes de actualizaciones.
- **Cuarentena**. Kaspersky Embedded Systems Security 2.2 pone en cuarentena los objetos probablemente infectados pasándolos de su ubicación original a la *Cuarentena*. Por razones de seguridad, los objetos se ponen en Cuarentena en forma cifrada.
- **Copia de seguridad**. Kaspersky Embedded Systems Security 2.2 almacena copias cifradas de los objetos clasificados como *Infectado* o *Probablemente infectado* en *Copia de seguridad* antes de desinfectarlos o eliminarlos.
- **Notificaciones de administrador y usuario**. Se puede configurar la aplicación para notificar al administrador y a los usuarios que tienen acceso al equipo protegido sobre eventos en el funcionamiento de Kaspersky Embedded Systems Security 2.2 y el estado de la protección antivirus en el equipo.
- **Cómo importar y exportar la configuración**. Se puede exportar la configuración de Kaspersky Embedded Systems Security 2.2 a un archivo de configuración XML e importar los parámetros a Kaspersky Embedded Systems Security 2.2 desde el archivo de configuración. Puede guardar todos los ajustes de la aplicación o únicamente los ajustes de componentes individuales en un archivo de configuración.
- **Aplicar plantillas**. Puede configurar manualmente los ajustes de seguridad de un nodo en el árbol o en una lista de recursos del archivo del equipo y guardar los valores de ajuste configurados como plantilla.

Esta plantilla se puede utilizar entonces para configurar las opciones de seguridad de otros nodos en las tareas de análisis y protección de Kaspersky Embedded Systems Security 2.2.

- **Administración de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security**. Puede configurar los derechos de administración de Kaspersky Embedded Systems Security 2.2 y de los servicios de Windows que están registrados por la aplicación, para usuarios y grupos de usuarios.
- **Carga de eventos en el registro de eventos de la aplicación**. Kaspersky Embedded Systems Security 2.2 registra la información sobre la configuración de los componentes del software, el estado actual de las tareas, los eventos que ocurrieron durante su ejecución, los eventos asociados con la administración de Kaspersky Embedded Systems Security 2.2 y la información necesaria para el diagnóstico de fallas en Kaspersky Embedded Systems Security 2.2.
- **Zona de confianza**. Puede generar una lista de objetos que desea excluir de la protección o el área del análisis que Kaspersky Embedded Systems Security 2.2 aplicará durante las tareas de análisis a pedido y protección en tiempo real.
- **Prevención de exploits**. Puede proteger la memoria de proceso de exploits mediante un agente inyectado en el proceso.

Novedades

Kaspersky Embedded Systems Security 2.2 ofrece las siguientes nuevas funciones y mejoras:

- Compatibilidad con nuevas versiones de sistemas operativos Microsoft Windows.

  Mecanismos de autoprotección basados en las tecnologías ELAM y PPL: ahora cuando se instala la aplicación, registra automáticamente un controlador ELAM que hace posible iniciar el servicio de Kaspersky Security (kavfs.exe) con el atributo Luz de proceso protegido. Esto permite reforzar la autoprotección de la aplicación y evitar una amplia gama de ataques.

  La funcionalidad está disponible cuando la aplicación se instala en equipos que ejecutan Microsoft Windows 10 RS2 (número de compilación 15063) y superiores.
- Compatibilidad para comprobar y procesar archivos de la nube almacenados en Microsoft OneDrive.
- Se han mejorado las posibilidades del subsistema de control de distribución de software.

  Ahora puede indicar qué archivos de instalación pueden transferir el atributo del paquete de instalación de confianza para toda la cadena de archivos extraídos de ellos. Esto hace posible aumentar la estabilidad de los procesos de instalación del software en un equipo con Control de inicio de aplicaciones habilitado, pero también amplía el área para un potencial ataque al aumentar el número de inicios de aplicaciones autorizados. Se recomienda usar esta opción durante implementaciones de software complejas, por ejemplo, cuando debe reiniciarse el equipo durante el proceso de distribución del software.
- Integración con herramientas de WMI.

  Ahora, cuando la aplicación se instala, se crea automáticamente un espacio de nombre de Kaspersky Security en el espacio de nombre raíz de WMI en el equipo local. Puede usar soluciones del cliente que admiten consultas de WMI para obtener datos sobre la aplicación y sus componentes.
- El formato para mostrar la información sobre la aplicación y sus componentes se ha ampliado con el comando KAVSHELL OMSINFO: ahora puede obtener la información sobre el estado de la tarea Control de inicio de aplicaciones, y también información sobre las actualizaciones críticas instaladas de módulos de la aplicación.
- Mayores posibilidades para administrar y monitorear el estado de aplicación con la Interfaz de diagnóstico compacto:
  - Ahora puede revisar los contadores de estadísticas de componentes instalados en la ficha Estadísticas

de la Interfaz de diagnóstico compacto.

- No se requiere contraseña al acceder a la interfaz de diagnósticos compacta, ni siquiera cuando la función de protección con contraseña está activada: la aplicación limita el acceso a la información y los elementos de control que están disponibles en la Interfaz de diagnóstico compacto en base únicamente a los permisos del usuario especificados para la administración de la aplicación.

- A partir de la versión 2.2, la aplicación implementa la capacidad de proporcionar una protección del equipo básica durante el inicio del sistema operativo en modo a prueba de fallos.

  De forma predeterminada, la aplicación no funciona en un equipo que se ejecuta en el modo a prueba de fallos. Para que la aplicación se inicie cuando el sistema operativo se inicia en el modo a prueba de fallos, configure el parámetro LoadInSafeMode con el valor 1 en la siguiente clave del registro de Windows:

  `HKLM\SYSTEM\CurrentControlSet\services\klam\Parameters`

  > Cuando se ejecuta en un equipo iniciado en modo a prueba de fallos, se limitará la funcionalidad de la aplicación.

- Se admiten informes de Kaspersky Security Center: ahora puede revisar informes sobre el estado de los componentes de la aplicación y dos tipos de informes sobre aplicaciones prohibidas.

  Esta funcionalidad se admite solo si usa Kaspersky Security Center 11.

- Los permisos de acceso al usuario para cambiar la carpeta de instalación y modificar ramas del registro críticas de los componentes de la aplicación ahora están limitados.

Kit de distribución

El kit de distribución incluye la aplicación de bienvenida que le permite realizar lo siguiente:

- Iniciar el asistente de instalación de Kaspersky Embedded Systems Security 2.2.
- Iniciar el asistente de instalación de la Consola de Kaspersky Embedded Systems Security 2.2.
- Iniciar el asistente que instalará el Complemento de administración de Kaspersky Embedded Systems Security 2.2 para administrar la aplicación mediante Kaspersky Security Center.
- Leer la Guía del administrador.
- Lea la Guía del usuario.
- Ir a la página de Kaspersky Embedded Systems Security 2.2 en el sitio web de Kaspersky Lab.
- Visitar el sitio web del Servicio de soporte técnico (https://support.kaspersky.com/mx).
- Leer información sobre la versión actual de Kaspersky Embedded Systems Security 2.2.

La carpeta \console contiene archivos para instalar la Consola de la aplicación (el conjunto de componentes de ”Herramientas de administración de Kaspersky Embedded Systems Security 2.2”).

La carpeta \product contiene:

- Archivos para la instalación de los componentes de Kaspersky Embedded Systems Security 2.2 en un equipo que ejecuta un sistema operativo de Microsoft Windows de 32 o 64 bits.
- Archivo para la instalación del Complemento de administración de Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center.
- Archivo que contiene las bases de datos antivirus actuales al momento del lanzamiento de la aplicación.

- Archivo que contiene los términos del Contrato de licencia de usuario final y la Política de privacidad.

La carpeta \product_no_avbases contiene archivos de instalación de los componentes y complementos de Kaspersky Embedded Systems Security 2.2 sin las bases de datos antivirus.

La carpeta \setup contiene los archivos de inicio del programa de bienvenida.

Los archivos del kit de distribución se almacenan en carpetas diferentes según el uso deseado (ver la tabla a continuación).

Table 2. Archivos del kit de distribución de Kaspersky Embedded Systems Security 2.2

Archivo	Objetivo
autorun.inf	Archivo de ejecución automática del asistente de instalación de Kaspersky Embedded Systems Security 2.2 para instalar la aplicación desde medios extraíbles.
ess_admin_guide_es.pdf	Guía del administrador.
ess_user_guide_es.pdf	Guía del usuario.
release_notes.txt	El archivo contiene información sobre la versión.
setup.exe	Archivo de inicio del programa de bienvenida (inicia setup.hta).
\console\esstools_x86(x64).msi	Paquete de instalación de Windows Installer; instala la Consola de la aplicación en el equipo protegido.
\console\setup.exe	El archivo que ejecuta el asistente de configuración para el conjunto de componentes de “Herramientas de administración” (incluida la Consola de la aplicación); inicia el archivo del paquete de instalación esstools.msi con la configuración especificada en el asistente de configuración.
\product\bases.cab	Archivo de almacenamiento que contiene las bases de datos antivirus actuales al momento del lanzamiento de la aplicación.
\product\setup.exe	El archivo que ejecuta el asistente para instalar Kaspersky Embedded Systems Security 2.2 en el equipo protegido; ejecuta el archivo del paquete de instalación ess.msi con la configuración de instalación especificada en el asistente.
\product\ess_x86(x64).msi	Paquete de instalación de Windows Installer; instala Kaspersky Embedded Systems Security 2.2 en el equipo protegido.
\product\ess.kud	Archivo en el formato definición Unicode de Kaspersky con una descripción del paquete de instalación para la instalación remota de Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center.
\product\klcfginst.exe	Instalador de un complemento de administración de Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center. Instale el complemento de administración en cada equipo donde encuentra instalada la Consola de administración de Kaspersky Security Center si planea usarla para administrar Kaspersky Embedded Systems Security 2.2.
\product\license.txt	Texto del Contrato de licencia de usuario final y la Política de privacidad.
\product\migration.txt	El archivo describe la migración desde versiones anteriores de la aplicación.
\setup\setup.hta	Archivo de inicio del programa de bienvenida.

Los archivos del kit de distribución se pueden ejecutar desde el CD de instalación. Si anteriormente copió los archivos del paquete de distribución en la unidad local, asegúrese de que se haya preservado la estructura de los archivos del kit de distribución.

Requisitos de hardware y software

Antes de instalar Kaspersky Embedded Systems Security 2.2, debe desinstalar otras aplicaciones antivirus del equipo.

Requisitos de hardware para el equipo protegido

Requisitos generales:

- Sistemas x86 compatibles con configuraciones simples y multiprocesador.
- Sistemas x64 compatibles con configuraciones simples y multiprocesador.

Volumen del disco:

- Para instalar el componente del Control de inicio de aplicaciones: 50 MB.
- Para instalar todos los componentes de Kaspersky Embedded Systems Security 2.2: 500 MB.

RAM:

- 256 MB para instalar el componente Control de inicio de aplicaciones solo en el equipo con el sistema operativo Microsoft® Windows.
- 512 MB para realizar la instalación completa de todos los componentes del equipo que ejecute el sistema operativo de Microsoft Windows.

Requisitos mínimos del procesador:

- para sistemas operativos Microsoft Windows de 32 bits: Intel® Pentium® III.
- para sistemas operativos Microsoft Windows de 64 bits: Intel Pentium IV.

Requisitos de software para el equipo protegido

Puede instalar Kaspersky Embedded Systems Security 2.2 en un dispositivo que ejecute un sistema operativo Microsoft Windows de 32 o 64 bits.

Se necesita tener Windows Installer 3.1 para una instalación correcta de la aplicación que funcione en un equipo que ejecuta Microsoft Windows XP.

Para instalar y usar Kaspersky Embedded Systems Security 2.2 en los dispositivos con sistemas operativos integrados, se requieren los componentes Administración de filtros y Herramientas de asistencia de administración.

Puede instalar Kaspersky Embedded Systems Security 2.2 en un equipo que ejecute alguno de los siguientes sistemas operativos Microsoft Windows de 32 o 64 bits:

- Windows XP Embedded SP3
- Windows XP Pro SP2/SP3
- Windows Embedded POSReady 2009
- Windows Embedded Standard 7 SP1

- Windows Embedded Enterprise 7 SP1
- Windows Embedded POSReady 7
- Windows 7 Professional / Enterprise SP1
- Windows Embedded 8.1 Industry Professional / Enterprise
- Windows Embedded 8.1 Professional
- Windows Embedded 8.0 Standard
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise
- Windows 10 IoT Enterprise
- Windows 10 Redstone 1 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 2 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 3 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 4 Professional / Enterprise / IoT Enterprise
- Windows 10 Redstone 5 Professional / Enterprise / IoT Enterprise

Instalación y desinstalación de la aplicación

Esta sección proporciona instrucciones paso a paso para instalar y desinstalar Kaspersky Embedded Systems Security 2.2.

En este capítulo

Componentes de software de Kaspersky Embedded Systems Security 2.2 y sus códigos para el servicio Windows Installer

De forma predeterminada, los archivo \server\ess_x86(x64).msi se utilizan para instalar todos los componentes de Kaspersky Embedded Systems Security 2.2. Puede instalar este componente al incluirlo en la instalación personalizada.

Los archivos \client\esstools_x86(x64).msi instalan todos los componentes del software que están incluidos en el conjunto de "Herramientas administrativas".

Las siguientes secciones presentan los códigos de los componentes de Kaspersky Embedded Systems Security 2.2 para el servicio Windows Installer. Estos códigos pueden utilizarse para definir una lista de los componentes que se instalan durante la instalación de Kaspersky Embedded Systems Security 2.2 desde la línea de comandos.

En esta sección

Componentes de software de Kaspersky Embedded Systems Security 2.2

La siguiente tabla contiene los códigos y las descripciones de los componentes de la aplicación Kaspersky Embedded Systems Security 2.2.

Table 3. Descripción de los componentes de la aplicación Kaspersky Embedded Systems Security 2.2

Componente	Código	Funciones realizadas
Funcionalidad básica	Core	Este componente contiene el conjunto de funciones básicas de la aplicación y garantiza su operación.
Control de inicio de aplicaciones	AppCtrl	Este componente supervisa los intentos del usuario de ejecutar aplicaciones y autoriza o rechaza el inicio de estas de acuerdo con las reglas de Control de inicio de aplicaciones. Se implementa en la tarea de Control de inicio de aplicaciones.
Control de dispositivos	DevCtrl	Este componente supervisa los intentos de conectar dispositivos de almacenamiento mediante USB a un equipo protegido y permite o restringe el uso de estos dispositivos según las reglas de control de dispositivos especificadas. El componente se implementa en la tarea de Control de dispositivos.
Protección antivirus	AVProtection	Este componente garantiza la protección antivirus y contiene los siguientes componentes: • Análisis a pedido • Protección de archivos en tiempo real
Análisis a pedido	Ods	Este componente instala los archivos de sistema de Kaspersky Embedded Systems Security 2.2 y las tareas de análisis a pedido (analiza los objetos del equipo protegido a solicitud del usuario). Si se especifican otros componentes de Kaspersky Embedded Systems Security 2.2 durante la instalación de Kaspersky Embedded Systems Security 2.2 desde la línea de comandos, pero no se indica el componente Core, este se instala automáticamente.
Protección de archivos en tiempo real	Oas	Este componente realiza un análisis antivirus de los archivos en el equipo protegido cuando obtiene acceso a estos. Implementa la tarea de Protección de archivos en tiempo real.
Uso de Kaspersky Security Network	Ksn	Este componente brinda protección a partir de las tecnologías en la nube de Kaspersky Lab. Implementa la tarea de Uso de KSN (envío de solicitudes y recepción de conclusiones del servicio de Kaspersky Security Network).

Componente	Código	Funciones realizadas
Monitor de integridad de archivos	Fim	Este componente registra las operaciones realizadas en los archivos con el área de supervisión especificada. El componente implementa la tarea Monitor de integridad de archivos.
Prevención de exploits	AntiExploit	Este componente hace posible administrar la configuración para proteger la memoria usada por procesos en la memoria de un equipo protegido.
Administración de firewall	Firewall	Este componente hace posible administrar el firewall de Windows a través de la interfaz gráfica de usuario de Kaspersky Embedded Systems Security 2.2. El componente implementa la tarea Administración de firewall.
Módulo de integración con el Agente de red de Kaspersky Security Center	AKIntegration	Proporciona una conexión entre Kaspersky Embedded Systems Security 2.2 y el Agente de red de Kaspersky Security Center. Puede instalar este componente en el equipo protegido si desea administrar la aplicación a través de Kaspersky Security Center.
Inspección de registros	LogInspector	Este componente supervisa la integridad del ambiente protegido sobre la base de los resultados de una inspección de los registros de eventos de Windows.
Conjunto de contadores de rendimiento del "Supervisor del sistema"	PerfMonCounters	Este componente instala un conjunto de contadores de rendimiento del Supervisor del sistema. Los contadores de rendimiento permiten medir el rendimiento de Kaspersky Embedded Systems Security 2.2 e identificar posibles cuellos de botella en el equipo cuando Kaspersky Embedded Systems Security 2.2 se utiliza junto con otros programas.
Contadores y capturas SNMP	SnmpSupport	Este componente publica los contadores y las capturas de Kaspersky Embedded Systems Security 2.2 a través del Protocolo simple de administración de redes (SNMP) en Microsoft Windows. Este componente puede instalarse en el equipo protegido únicamente si Microsoft SNMP está instalado en el mismo equipo.
Icono de Kaspersky Embedded Systems Security 2.2 en el área de notificación	TrayApp	Este componente muestra el icono de Kaspersky Embedded Systems Security 2.2 en el área de notificación de la bandeja de tareas del equipo protegido. El icono de Kaspersky Embedded Systems Security 2.2 muestra el estado de protección del equipo y se puede utilizar para abrir la Consola de Kaspersky Embedded Systems Security 2.2 en Microsoft Management Console (si está instalada) y la ventana **Acerca de la aplicación**.
Utilidad de línea de comandos	Shell	Permite controlar Kaspersky Embedded Systems Security 2.2 desde la línea de comandos del equipo protegido.

Conjunto de “Herramientas administrativas” de los componentes de software

La siguiente tabla contiene los códigos y las descripciones del conjunto de “Herramientas de administración” de los componentes de software.

Table 4. Descripción de los componentes de software de las "Herramientas de administración"

Componente	Código	Funciones del componente
Complementos de Kaspersky Embedded Systems Security 2.2	MmcSnapin	Este componente instala el complemento Microsoft Management Console mediante la Consola de Kaspersky Embedded Systems Security 2.2. Si se especifican otros componentes durante la instalación de las "Herramientas de administración" desde la línea de comandos y no se indica el componente MmcSnapin, este se instala automáticamente.
Help	Help	Archivo de ayuda .chm que se guarda en la carpeta junto con los archivos de las Herramientas de administración de Kaspersky Embedded Systems Security 2.2. Puede abrir el archivo de Ayuda a través del menú **Iniciar** o al hacer clic en la tecla **F1** con la ventana de la Consola de la aplicación abierta.
Documentación	Help	Kaspersky Embedded Systems Security 2.2 agrega un acceso directo al recurso web de Kaspersky Lab, donde la Guía del administrador y la Guía del usuario están disponibles en formato PDF. El acceso directo está disponible en el menú Inicio.

Cambios en el sistema después de la instalación de Kaspersky Embedded Systems Security 2.2

Si Kaspersky Embedded Systems Security 2.2 y la Consola de la aplicación (conjunto de “Herramientas de administración”) se instalan juntos, el servicio Windows Installer realizará las siguientes modificaciones en el equipo:

- Se crean las carpetas de Kaspersky Embedded Systems Security 2.2 en el equipo protegido y en el equipo donde se instala la Consola de la aplicación.
- Se registran los servicios de Kaspersky Embedded Systems Security 2.2.
- Se crea un grupo de usuarios de Kaspersky Embedded Systems Security 2.2.
- Se registran las claves de Kaspersky Embedded Systems Security 2.2 en el registro del sistema.

Los cambios se describen en la siguiente tabla.

Carpetas de Kaspersky Embedded Systems Security 2.2

Table 5. Carpetas de Kaspersky Embedded Systems Security 2.2 en un equipo protegido

Carpeta	Archivos de Kaspersky Embedded Systems Security 2.2
Carpeta de instalación predeterminada de Kaspersky Embedded Systems Security 2.2: En la versión de Microsoft Windows de 32 bits: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security\. En la versión de Microsoft Windows de 64 bits: %ProgramFiles(x86)%\Kaspersky Embedded Systems Security\	Archivos ejecutables de Kaspersky Embedded Systems Security 2.2 (carpeta de destino especificada durante la instalación).
Carpeta %Kaspersky Embedded Systems Security%\mibs	Archivos MIB (Management Information Base); estos archivos contienen una descripción de los contadores y los enlaces publicados por Kaspersky Embedded Systems Security 2.2 a través del protocolo SNMP.
Carpeta %Kaspersky Embedded Systems Security%\x64	Las versiones de 64 bits de los archivos ejecutables de Kaspersky Embedded Systems Security 2.2 (la carpeta se crea únicamente durante la instalación de Kaspersky Embedded Systems Security 2.2 para la versión de 64 bits de Microsoft Windows).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Data\ %ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Settings\ %ALLUSERSPROFILE%\Application Data\Kaspersky Embedded Systems Security\2.2\Dskm\	Archivos de servicio de Kaspersky Embedded Systems Security 2.2.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\	Archivos con configuración de orígenes de actualizaciones.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Update\Distribution\	Actualizaciones de bases de datos y módulos del programa descargados mediante la tarea Copia de actualizaciones (la carpeta se crea la primera vez que se descargan actualizaciones con la tarea Copia de actualizaciones).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Reports\	Registros de tareas y registro de auditoría del sistema.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Current\	Conjunto de bases de datos utilizado a la hora actual.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Backup\	Copia de seguridad de bases de datos; se sobrescribe cada vez que se actualizan las bases de datos.

Carpeta	Archivos de Kaspersky Embedded Systems Security 2.2
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Bases\Temp\	Archivos temporales creados durante la ejecución de tareas de actualización.
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Quarantine\	Objetos en cuarentena (carpeta predeterminada).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Backup\	Objetos en copia de seguridad (carpeta predeterminada).
%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored\	Objetos restaurados de la copia de seguridad y la cuarentena (carpeta predeterminada para los objetos restaurados).

Table 6. Carpetas creadas durante la instalación de la Consola de la aplicación

Carpeta	Archivos de la Consola de Kaspersky Embedded Systems Security 2.2
Carpeta de instalación predeterminada de la Consola de la aplicación: • En la versión de Microsoft Windows de 32-bits: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\ • En la versión de Microsoft Windows de 64 bits: %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools\	Archivos de “Herramientas de administración” (carpeta de destino especificada durante la instalación de la Consola de Kaspersky Embedded Systems Security 2.2).

Servicios de Kaspersky Embedded Systems Security 2.2

Los servicios de Kaspersky Embedded Systems Security 2.2 se inician con la cuenta de sistema local (SYSTEM).

Table 7. Servicios de Kaspersky Embedded Systems Security 2.2

Servicio	Objetivo
Servicio de Kaspersky Security (KAVFS)	Servicio esencial de Kaspersky Embedded Systems Security 2.2 que administra las tareas y el flujo de trabajo de Kaspersky Embedded Systems Security 2.2.
Servicio de Kaspersky Security Management (KAVFSGT)	Este servicio fue diseñado para administrar Kaspersky Embedded Systems Security 2.2 a través de la Consola de la aplicación.

Grupos de Kaspersky Embedded Systems Security 2.2

Table 8. Grupos de Kaspersky Embedded Systems Security 2.2

Grupo	Objetivo

Administradores de ESS	Grupo del equipo protegido cuyos usuarios disponen de acceso absoluto al servicio de Kaspersky Security Management y a todas las funciones de Kaspersky Embedded Systems Security 2.2.

Claves de registro del sistema

Table 9. Claves de registro del sistema

Clave	Objetivo
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFS]	Propiedades del servicio Kaspersky Embedded Systems Security 2.2.
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Kaspersky Security]	Configuración del registro de eventos de Kaspersky Embedded Systems Security 2.2 (registro de eventos de Kaspersky).
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\KAVFSGT]	Propiedades del servicio de administración de Kaspersky Embedded Systems Security 2.2.
En la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security\Performance] En la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kaspersky Security x64\Performance].	Configuración de los contadores de rendimiento.
En la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\SnmpAgent] En la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\SnmpAgent]	Configuración del componente de Compatibilidad con protocolo SNMP.
En la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\CrashDump] En la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\CrashDump]	Configuración de escritura del archivo de volcado.
En la versión de 32 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\ESS\2.2\Trace] En la versión de 64 bits de Microsoft Windows: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Trace]	Configuración del archivo de rastreo.

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\ESS\2.2\Environment]	Configuración de las tareas y las funciones de la aplicación.

Procesos de Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 inicia los procesos que se describen en la siguiente tabla.

Table 10. Procesos de Kaspersky Embedded Systems Security 2.2

Nombre de archivo	Objetivo
kavfswp.exe	Flujo de trabajo de Kaspersky Embedded Systems Security 2.2
kavtray.exe	Proceso para el icono de la bandeja del sistema
kavshell.exe	Proceso de la utilidad de línea de comandos
kavfsrcn.exe	Proceso de administración remota de Kaspersky Embedded Systems Security 2.2
kavfs.exe	Proceso del servicio de Kaspersky Security
kavfsgt.exe	Proceso del servicio de Kaspersky Security Management
kavfswh.exe	Proceso del servicio de prevención de exploits de Kaspersky Security

Configuraciones de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer

Las tablas que aparecen a continuación contienen descripciones de las configuraciones para instalar y desinstalar Kaspersky Embedded Systems Security 2.2, sus valores predeterminados, claves para modificar los valores de la configuración de instalación y sus posibles valores. Estas claves pueden utilizarse junto con claves estándar para el comando msiexec del servicio Windows Installer durante la instalación de Kaspersky Embedded Systems Security 2.2 desde la línea de comandos.

Table 11. Parámetros de instalación y opciones de la línea de comandos de Windows Installer

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado	Descripción
Aceptación de los términos del Contrato de licencia de usuario final	EULA=<valor> 0: rechaza los términos del Contrato de licencia de usuario final. 1: acepta los términos del Contrato de licencia de usuario final.	0	Debe aceptar los términos del Contrato de licencia de usuario final para proceder con la instalación de Kaspersky Embedded Systems Security 2.2.

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado	Descripción
Aceptación de los términos de la Política de privacidad	PRIVACYPOLICY=<valor> 0: rechaza los términos de la Política de privacidad. 1: acepta los términos de la Política de privacidad.	0	Debe aceptar los términos de la Política de privacidad para instalar Kaspersky Embedded Systems Security 2.2.
Carpeta de destino	INSTALLDIR=<ruta completa de la carpeta>	Kaspersky Embedded Systems Security 2.2: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Herramientas de administración: %ProgramFiles%\Kaspersky Lab\Kaspersky Embedded Systems Security Admins Tools En la versión de 64 bits de Microsoft Windows: %ProgramFiles(x86)%.	Carpeta en la que se guardan los archivos de Kaspersky Embedded Systems Security 2.2 durante la instalación. Puede especificar otra carpeta.
Al iniciar Kaspersky Embedded Systems Security 2.2, se activa la Protección de archivos en tiempo real (**Habilitar la protección en tiempo real después de la instalación**)	RUNRTP=<valor> 1: iniciar; 0: no iniciar.	1	Active esta configuración para iniciar la Protección de archivos en tiempo real al iniciar Kaspersky Embedded Systems Security 2.2 (recomendado).

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado	Descripción
Exclusiones del análisis según recomendaciones de Microsoft Corporation (**Agregar archivos recomendados por Microsoft a la lista de exclusiones**)	ADDMSEXCLUSION=<valor> 1: excluir; 0: no excluir.	1	En la tarea Protección de archivos en tiempo real, excluya del alcance de la protección a los objetos del equipo que Microsoft Corporation recomiende excluir. Es posible que algunas aplicaciones instaladas en el equipo se vuelvan inestables si la aplicación antivirus intercepta o modifica archivos utilizados por estas aplicaciones. Por ejemplo, Microsoft Corporation incluye algunas aplicaciones del controlador de dominio en la lista de tales objetos.
Objetos excluidos del área del análisis de acuerdo con las recomendaciones de Kaspersky Lab (**Agregar archivos recomendados por Kaspersky Lab a la lista de exclusiones**)	ADDKLEXCLUSION=<valor> 1: excluir; 0: no excluir.	1	En la tarea Protección de archivos en tiempo real, excluya del alcance de la protección a los objetos del equipo que Kaspersky Lab recomiende excluir.

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado	Descripción
Permite la conexión remota con la Consola de la aplicación.	ALLOWREMOTECON=<valor> 1: permitir; 0: denegar.	0	De forma predeterminada, no se permite la conexión remota para la Consola de la aplicación instalada en el equipo protegido. Durante la instalación, puede habilitar la conexión. Kaspersky Embedded Systems Security 2.2 crea reglas de autorización para el proceso kavfsgt.exe mediante la utilización del protocolo de TCP para todos los puertos.
Ruta del archivo de clave (**Clave**)	LICENSEKEYPATH=<nombre de archivo de clave>	Directorio \product ubicado en el kit de distribución	De forma predeterminada, el instalador intenta buscar el archivo con la extensión .key en la carpeta \product del kit de distribución. Si la carpeta \product contiene varios archivos de clave, el instalador seleccionará el que tenga la fecha de caducidad más alejada. Los archivos de clave pueden guardarse de antemano en la carpeta \product o especificando otra ruta con la opción de configuración **Agregar clave**.

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado	Descripción
			Para agregar una clave después de la instalación de Kaspersky Embedded Systems Security 2.2, utilice la herramienta de administración que prefiera (por ejemplo, la Consola de la aplicación). Si no agrega una clave durante la instalación de la aplicación, Kaspersky Embedded Systems Security 2.2 no funcionará.
Ruta al archivo de configuración	CONFIGPATH=<nombre del archivo de configuración>	Sin especificar	Kaspersky Embedded Systems Security 2.2 importa la configuración desde el archivo de configuración especificado que se creó en la aplicación. Kaspersky Embedded Systems Security 2.2 no importa contraseñas del archivo de configuración (por ejemplo, contraseñas de cuenta para iniciar tareas ni contraseñas para establecer conexión con un servidor proxy). Una vez que se hayan importado las configuraciones, deberá introducir todas las contraseñas de forma manual. Si no ha especificado ningún archivo de configuración, la aplicación empleará los valores predeterminados tras la instalación.

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado	Descripción
Cómo habilitar conexiones de red para la consola	ADDWFEXCLUSION=<valor> **1**: permitir; **0**: denegar.	0	Use esta opción para instalar Kaspersky Embedded Systems Security 2.2 en otro equipo. Puede administrar de forma remota la protección de un equipo desde otro dispositivo con la Consola de Kaspersky Embedded Systems Security 2.2 instalada. Se abre el puerto 135 (TCP) en el firewall de Microsoft Windows, se habilitan las conexiones de red del archivo ejecutable kavfsrcn.exe para la administración remota de Kaspersky Embedded Systems Security 2.2 y se otorga acceso a aplicaciones DCOM. Una vez finalizada la instalación, agregue los usuarios al grupo de administración de ESS para que puedan administrar la aplicación de forma remota y autorizar las conexiones de red para el servicio de Kaspersky Security Management (kavfsgt.exe file) en el equipo. Puede leer más sobre la configuración adicional cuando la Consola de Kaspersky Embedded Systems Security 2.2 se instala en otro equipo (consulte la sección

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado	Descripción
			"Configuración avanzada después de instalar la Consola de la aplicación en otro equipo", en la página 45).
Deshabilitación de la verificación de software incompatible	SKIPINCOMPATIBLESW = <valor> 0: se realiza la verificación de software incompatible 1: no se realiza la verificación de software incompatible	0	Use este parámetro para habilitar o deshabilitar la verificación de software incompatible durante la instalación de fondo de la aplicación en el dispositivo. Independientemente del valor de este parámetro, durante la instalación de Kaspersky Embedded Systems Security 2.2, la aplicación siempre advierte sobre otras versiones de la aplicación instaladas en el dispositivo.

Table 12. Configuración de desinstalación y opciones de la línea de comandos en Windows Installer

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado
Restauración de objetos en cuarentena	RESTOREQTN=<valor> **0**: eliminar el contenido de la cuarentena; **1**: restaurar el contenido puesto en cuarentena en la carpeta especificada por el parámetro RESTOREPATH en la subcarpeta \Quarantine.	0: eliminar
Restauración del contenido de la copia de seguridad	RESTOREBCK=<valor> **0**: eliminar el contenido de la copia de seguridad; **1**: restaurar el contenido de la copia de seguridad en la carpeta especificada por el parámetro RESTOREPATH en la subcarpeta \Backup.	0: eliminar
Ingrese la contraseña actual para confirmar la eliminación (si la protección con contraseña se habilita).	UNLOCK_PASSWORD=<contraseña especificada>	Sin especificar

Configuración	Opciones de la línea de comandos de Windows Installer y sus valores posibles	Valor predeterminado
Carpeta de objetos restaurados	RESTOREPATH=<ruta completa de la carpeta> Los objetos restaurados se almacenan en la carpeta especificada.	%ALLUSERSPROFILE%\Application Data\Kaspersky Lab\Kaspersky Embedded Systems Security\2.2\Restored

Registro de instalación y desinstalación de Kaspersky Embedded Systems Security 2.2

Si Kaspersky Embedded Systems Security 2.2 se instala o desinstala con la ayuda del asistente de instalación (o desinstalación), el servicio Windows Installer crea un registro de instalación (o desinstalación). El archivo de registro ess_install_<uid>.log (donde <uid> representa a un identificador de registro único de 8 caracteres) se guarda en una carpeta %temp% del usuario con cuya cuenta se ejecutó el archivo setup.exe.

Si se ejecuta la opción **Modificar o eliminar** para la Consola de la aplicación o Kaspersky Embedded Systems Security 2.2 en el menú **Iniciar**, se crea automáticamente el archivo ess_2.2_maintenance.log en la carpeta %temp%.

Si Kaspersky Embedded Systems Security 2.2 se instala o desinstala desde la línea de comandos, el archivo de registro de instalación no se crea de manera predeterminada.

► *Para instalar Kaspersky Embedded Systems Security 2.2 con el archivo de registro creado en el disco C:\:*

- `msiexec /i ess_x86.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`
- `msiexec /i ess_x64.msi /l*v C:\ess.log /qn EULA=1 PRIVACYPOLICY=1`

Planificación de la instalación

Esta sección contiene información sobre el conjunto de herramientas de administración de Kaspersky Embedded Systems Security 2.2 y aspectos especiales de la instalación y desinstalación de Kaspersky Embedded Systems Security 2.2 con el asistente (consulte la sección “Instalación y desinstalación de la aplicación con el asistente”, en la página 41), desde la línea de comandos (consulte la sección “Instalación y desinstalación de la aplicación desde la línea de comandos”, en la página 53), mediante Kaspersky Security Center (consulte la sección “Instalación y desinstalación de la aplicación mediante Kaspersky Security Center”, en la página 58) y mediante la directiva de grupos de Active Directory® (consulte la sección “Instalación y desinstalación de la aplicación mediante directivas de grupos de Active Directory” en la página 62).

Antes de iniciar la instalación de Kaspersky Embedded Systems Security 2.2, planifique las etapas más importantes.

1. Defina qué herramientas de administración utilizará para configurar y administrar Kaspersky Embedded Systems Security 2.2.
2. Seleccione los componentes de la aplicación necesarios para la instalación (consulte la sección “Componentes de software de Kaspersky Embedded Systems Security 2.2 y sus códigos para el

servicio de Windows Installer", en la página 24).

3. Elija un método de instalación.

En esta sección

Selección de herramientas de administración

Defina las herramientas de administración que utilizará para configurar y administrar Kaspersky Embedded Systems Security 2.2. Kaspersky Embedded Systems Security 2.2 se puede administrar desde la Consola de la aplicación, la utilidad de línea de comandos y la Consola de administración de Kaspersky Security Center.

Consola de Kaspersky Embedded Systems Security 2.2

La Consola de Kaspersky Embedded Systems Security 2.2 es un complemento aislado agregado a Microsoft Management Console. Kaspersky Embedded Systems Security 2.2 se puede administrar mediante la Consola de la aplicación instalada en el equipo protegido o en cualquier otro equipo de la red corporativa.

Es posible agregar varios complementos de Kaspersky Embedded Systems Security 2.2 a una Microsoft Management Console abierta en el modo de creación, a fin de usarla para administrar la protección de varios equipos en los que está instalado Kaspersky Embedded Systems Security 2.2.

La Consola de la aplicación se incluye en el conjunto de componentes de la aplicación "Herramientas de la administración".

Utilidad de línea de comandos

Puede administrar Kaspersky Embedded Systems Security 2.2 desde la línea de comandos del equipo protegido.

La utilidad de línea de comandos está incluida en el grupo de componentes de la aplicación Kaspersky Embedded Systems Security 2.2.

Kaspersky Security Center

Si su empresa utiliza la aplicación Kaspersky Security Center para administrar de forma centralizada la protección antivirus, puede gestionar Kaspersky Embedded Systems Security 2.2 a través de la Consola de administración de Kaspersky Security Center.

Deben instalarse los siguientes componentes:

- **Módulo de integración con el Agente de red de Kaspersky Security Center**. Este componente está incluido en el grupo de componentes de la aplicación Kaspersky Embedded Systems Security 2.2. Garantiza la comunicación entre Kaspersky Embedded Systems Security 2.2 y el Agente de red. Instale el módulo de integración con el Agente de red de Kaspersky Security Center en el equipo protegido.
- **Agente de red de Kaspersky Security Center**. Instale este componente en todos los equipos protegidos. Este componente admite la interacción entre la instancia de Kaspersky Embedded Systems Security 2.2 instalada en el equipo y la Consola de administración de Kaspersky Security Center. El archivo de instalación del Agente de red se encuentra en la carpeta del kit de distribución de Kaspersky Security Center.
- **Complemento de administración de Kaspersky Embedded Systems Security 2.2**. Además, puede

instalar el complemento de administración para gestionar Kaspersky Embedded Systems Security 2.2 a través de la Consola de administración en el equipo donde se instaló el servidor de administración de Kaspersky Security Center. Esto implementará la interfaz de administración de la aplicación a través de Kaspersky Security Center. El archivo de instalación del complemento de administración, \product\klcfginst.exe, está incluido en el kit de distribución de Kaspersky Embedded Systems Security 2.2.

Selección del tipo de instalación

Después de especificar los componentes de software para la instalación de Kaspersky Embedded Systems Security 2.2 (consulte la sección “Componentes de software de Kaspersky Embedded Systems Security 2.2 y sus códigos para el servicio de Windows Installer”, en la página 24), deberá seleccionar el método de instalación de la aplicación.

Seleccione el método de instalación en función de la arquitectura de la red y de las siguientes condiciones:

- Si deben configurarse las opciones de instalación de Kaspersky Embedded Systems Security 2.2, o si se utilizarán las opciones de instalación recomendadas (consulte la sección “Configuración de instalación y desinstalación y opciones de línea de comandos para el servicio de Windows Installer”en la página 31).
- Si la configuración de instalación será la misma para todos los equipos o específica para cada equipo.

Se puede instalar Kaspersky Embedded Systems Security 2.2 de forma interactiva con el asistente de instalación o en modo silencioso sin la participación del usuario, e invocarse mediante la ejecución del archivo del paquete de instalación con las opciones de configuración desde la línea de comandos. Se puede instalar Kaspersky Embedded Systems Security 2.2 de forma remota y centralizada mediante las directivas de grupo de Active Directory o ejecutando la tarea de instalación remota de Kaspersky Security Center.

Se puede instalar Kaspersky Embedded Systems Security 2.2 en un solo equipo, configurar su funcionamiento y guardar sus valores de configuración en un archivo de configuración; en el futuro puede usar el archivo creado para instalar Kaspersky Embedded Systems Security 2.2 en otro equipo (esta posibilidad no es aplicable si la aplicación se instala con directivas de grupo de Active Directory).

Inicio del asistente de instalación

El asistente de instalación puede instalar los siguientes elementos:

- Componentes de Kaspersky Embedded Systems Security 2.2 (consulte la sección “Componentes de software de Kaspersky Embedded Systems Security 2.2”, en la página 25) en un equipo protegido desde un archivo \product\setup.exe incluido en el kit de distribución.
- La Consola de Kaspersky Embedded Systems Security 2.2 (consulte la sección “Instalación de la Consola de Kaspersky Embedded Systems Security 2.2”, en la página 44) desde el archivo \client\setup.exe del kit de distribución en el equipo protegido u otro host LAN.

Ejecución del archivo del paquete de instalación desde la línea de comandos con la configuración de instalación requerida

Si el archivo del paquete de instalación se inicia sin opciones de línea de comandos, Kaspersky Embedded Systems Security 2.2 se instalará con la configuración predeterminada. Las opciones de Kaspersky Embedded Systems Security 2.2 pueden utilizarse para modificar la configuración de instalación.

La Consola de la aplicación puede instalarse en el equipo protegido o en la estación de trabajo del administrador.

También puede utilizar comandos de ejemplo para la instalación de Kaspersky Embedded Systems Security 2.2 y la Consola de la aplicación (consulte la Sección “Instalación y desinstalación de la aplicación desde la línea de comandos”en la página 53).

Instalación centralizada mediante Kaspersky Security Center

Si su red utiliza Kaspersky Security Center para administrar la protección antivirus de los equipos en red, Kaspersky Embedded Systems Security 2.2 puede instalarse en varios equipos ejecutando la tarea de instalación remota de Kaspersky Security Center.

Los equipos en los que desee instalar Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center (consulte la sección “Instalación y desinstalación de la aplicación mediante Kaspersky Security Center”, en la página 58) pueden encontrarse en el mismo dominio que Kaspersky Security Center, pertenecer a otro dominio, o no pertenecer a ninguno.

Instalación centralizada a partir de directivas de grupo de Active Directory

Las directivas de grupo de Active Directory pueden utilizarse para instalar Kaspersky Embedded Systems Security 2.2 en un equipo protegido. La Consola de la aplicación puede instalarse en el equipo protegido o en la estación de trabajo del administrador.

Kaspersky Embedded Systems Security 2.2 puede instalarse utilizando solo la configuración de instalación recomendada.

Los equipos en los cuales se instala Kaspersky Embedded Systems Security 2.2 mediante directivas de grupo de Active Directory (consulte la sección “Instalación y desinstalación mediante directivas de grupo de Active Directory”, en la página 62) deben estar ubicados en el mismo dominio y en la misma unidad organizacional. La instalación se lleva a cabo al iniciar el equipo, antes de iniciar sesión en Microsoft Windows.

Instalación y desinstalación de la aplicación mediante un asistente

Esta sección contiene información sobre los procesos de instalación y desinstalación de Kaspersky Embedded Systems Security 2.2 y la Consola de la aplicación mediante el asistente de instalación, así como información sobre configuraciones adicionales y acciones que deben ejecutarse tras la instalación de Kaspersky Embedded Systems Security 2.2.

En esta sección

Instalación mediante el asistente de instalación

Las siguientes secciones contienen información sobre la instalación de Kaspersky Embedded Systems Security 2.2 y la Consola de la aplicación.

► *Para instalar y utilizar Kaspersky Embedded Systems Security 2.2, siga estos pasos:*

1. Instale Kaspersky Embedded Systems Security 2.2 en un equipo protegido.
2. Instale la Consola de la aplicación en los equipos desde los que administrará Kaspersky Embedded Systems Security 2.2.
3. Si la Consola de la aplicación se instaló en un equipo de la red, además de en el equipo protegido, deberá

definir determinados parámetros de la configuración para permitir que los usuarios de la Consola de la aplicación administren Kaspersky Embedded Systems Security 2.2 de forma remota.

4. Realice acciones después de la instalación de Kaspersky Embedded Systems Security 2.2.

En esta sección

Instalación de Kaspersky Embedded Systems Security 2.2

Antes de instalar Kaspersky Embedded Systems Security 2.2, siga estos pasos:

- Asegúrese de que no haya otros programas antivirus instalados en el equipo.
- Asegúrese de que la cuenta que utilizará para iniciar el asistente de instalación esté registrada en el grupo de administradores del equipo protegido.

Después de completar las acciones descritas anteriormente, continúe con el procedimiento de instalación. Siga las indicaciones del asistente de instalación, especifique la configuración para la instalación de Kaspersky Embedded Systems Security 2.2. Puede detener el proceso de instalación de Kaspersky Embedded Systems Security 2.2 en cualquier paso del asistente de instalación. Para ello, presione el botón **Cancelar** que se encuentra en la ventana del asistente de instalación.

Puede leer más sobre la configuración de instalación (y desinstalación) (consulte la sección “Configuración de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer”, en la página 31).

► *Para instalar Kaspersky Embedded Systems Security 2.2 mediante el asistente de instalación:*

1. Inicie el archivo setup.exe de bienvenida en el equipo.
2. En la ventana que se abre, en la sección **Instalación**, haga clic en el vínculo **Instalar Kaspersky Embedded Systems Security 2.2**.
3. En la pantalla bienvenida del Asistente de instalación de Kaspersky Embedded Systems Security 2.2, haga clic en el botón **Siguiente**.

   Se abre la ventana **Contrato de licencia de usuario final y Política de privacidad**.
4. Revise los términos de Contrato de licencia y la Política de privacidad.
5. Si acepta los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, seleccione las casillas **los términos y condiciones de este Contrato de licencia de usuario final** y **Política de privacidad que describe el manejo de datos** a fin de continuar con la instalación.

   Si no acepta el Contrato de licencia de usuario final y/o la Política de privacidad, la instalación se cancelará.
6. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Instalación personalizada**.
7. Seleccione los componentes que quiera instalar.

   De forma predeterminada, todos los componentes de Kaspersky Embedded Systems Security 2.2 se incluyen en el conjunto de instalación recomendado, excepto el componente de Administración de firewall.

El componente de compatibilidad con el protocolo SNMP de Kaspersky Embedded Systems Security 2.2 solo aparece en la lista de componentes que se sugiere instalar si el servicio Microsoft Windows SNMP está instalado en el equipo.

8. Para cancelar todos los cambios, presione el botón **Restablecer** en la ventana **Instalación personalizada**. Haga clic en el botón **Siguiente**.
9. En la ventana **Seleccione una carpeta de destino**:
   - Si es necesario, especifique una carpeta en la cual se copiarán los archivos de Kaspersky Embedded Systems Security 2.2.
   - Si fuera necesario, puede hacer clic en el botón **Disco** para revisar la información sobre el espacio disponible en las unidades locales.

   Haga clic en el botón **Siguiente**.
10. En la ventana **Configuración avanzada de instalación**, configure las siguientes opciones de instalación:
    - **Habilitar la protección en tiempo real después de la instalación**.
    - **Agregar archivos recomendados por Microsoft a la lista de exclusiones**.
    - **Agregar archivos recomendados por Kaspersky Lab a la lista de exclusiones**.

      Haga clic en el botón **Siguiente**.
11. En la ventana **Importar opciones de configuración del archivo de configuración**:
    a. Especifique el archivo de configuración para importar Kaspersky Embedded Systems Security 2.2 de un archivo de configuración existente creado en cualquier versión anterior de la aplicación.
    b. Presione el botón **Siguiente**.
12. En la ventana **Activación de la aplicación**, realice una de las siguientes acciones:
    - Si desea activar la aplicación, especifique un archivo de clave de Kaspersky Embedded Systems Security 2.2.
    - Si desea activar la aplicación más adelante, pulse el botón **Siguiente**.
    - Si ya se ha guardado un archivo de clave en la carpeta \server del kit de distribución, el nombre del archivo aparecerá en el campo **Clave**.

      Para agregar la clave usando un archivo de clave guardado en otra carpeta, especifique el archivo.

      Una vez que se agrega el archivo de clave, la información sobre la licencia se mostrará en la ventana. Kaspersky Embedded Systems Security 2.2 mostrará la fecha calculada de la caducidad de la licencia. El periodo de la licencia entra en vigor en el momento en que se agrega una clave y caduca antes de la fecha de caducidad del archivo de clave.

      Haga clic en el botón **Siguiente** para ingresar la clave en la aplicación.
13. En la ventana **Listo para instalar**, presione el botón **Instalar**. El asistente comenzará con la instalación de los componentes de Kaspersky Embedded Systems Security 2.2.
14. Una vez que termine la instalación, se abrirá la ventana **Instalación finalizada**.
15. Seleccione la casilla de verificación **Ver las Notas de la versión** para ver información sobre la versión después de que el asistente de instalación finalice.
16. Haga clic en **Aceptar**.

Se cierra la ventana del asistente de instalación. Una vez finalizada la instalación, ya podrá utilizar Kaspersky

Embedded Systems Security 2.2 si ha agregado la clave de activación.

Instalación de la Consola de Kaspersky Embedded Systems Security 2.2

Siga las instrucciones del asistente de instalación para ajustar las opciones de instalación para la instalación de la Consola de la aplicación. Puede detener el proceso de instalación de Virus en cualquier paso del asistente de instalación. Para ello, haga clic en el botón **Cancelar** que se encuentra en la ventana del asistente de instalación.

► *Para instalar la Consola de la aplicación, siga estos pasos:*

1. Asegúrese de que la cuenta con la que ejecute el asistente de instalación esté incluida en el grupo de administradores del equipo.
2. Ejecute el archivo de bienvenida setup.exe en el equipo.

   Se abre la ventana de bienvenida.
3. Haga clic en el vínculo **Instalar la Consola de Kaspersky Embedded Systems Security 2.2**.

   Se abre la ventana de bienvenida del asistente de instalación. Haga clic en el botón **Siguiente**.
4. Revise los términos del Contrato de licencia de usuario final y la Política de privacidad en la ventana abierta, y seleccione **los términos y condiciones de este Contrato de licencia de usuario final** y **Política de privacidad que describe el manejo de datos** para continuar con la instalación. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración avanzada de instalación**.
5. En la ventana **Configuración avanzada de instalación**:
   - Si tiene pensado utilizar la Consola de la aplicación para administrar una instancia de Kaspersky Embedded Systems Security 2.2 instalada en un equipo remoto, marque la casilla de verificación **Permitir el acceso remoto**.
   - Para abrir la **Instalación personalizada** y seleccionar componentes:
     a. Haga clic en el botón **Avanzado**.

        Se abre la ventana **Instalación personalizada**.
     b. Seleccione los componentes del conjunto “Herramientas de administración” de una lista.

        De forma predeterminada, se instalan todos los componentes.
     c. Haga clic en el botón **Siguiente**.

   > Puede encontrar más información sobre los componentes de Kaspersky Embedded Systems Security 2.2 (consulte la sección “Componentes de software de Kaspersky Embedded Systems Security 2.2 y sus códigos para el servicio de Windows Installer”, en la página 24).
6. En la ventana **Seleccione una carpeta de destino**:
   a. Si lo necesita, puede indicar otra carpeta en la que se guardarán los archivos de instalación.
   b. Haga clic en el botón **Siguiente**.
7. En la ventana **Listo para instalar**, presione el botón **Instalar**.

   El asistente comenzará a instalar los componentes seleccionados.
8. Haga clic en **Aceptar**.

Se cierra la ventana del asistente de instalación. La Consola de la aplicación se instalará en un

equipo protegido.

Si el conjunto de “Herramientas de administración” se instaló en un equipo de la red además del equipo protegido, ajuste la configuración avanzada (consulte la sección “Configuración avanzada después de la instalación de la Consola de la aplicación en otro equipo”, en la página 45).

Configuración avanzada después de la instalación de la Consola de la aplicación en otro equipo

Si la Consola de la aplicación se ha instalado en algún equipo en la red, además del equipo protegido, realice las acciones descritas a continuación para que los usuarios pueden administrar Kaspersky Embedded Systems Security 2.2 de forma remota:

- Agregar usuarios de Kaspersky Embedded Systems Security 2.2 al grupo de administración de ESS en el equipo protegido.
- Permita conexiones de red para el servicio de Kaspersky Security Management (kavfsgt.exe) (consulte la sección “Acerca de los permisos para el servicio de Kaspersky Security Management”, en la página 83) si el equipo protegido utiliza el firewall de Windows u otro firewall.
- Si no se seleccionó la casilla **Permitir el acceso remoto** durante la instalación de la Consola de la aplicación en un equipo que ejecuta Microsoft Windows, debe permitir manualmente conexiones de red para la Consola de la aplicación mediante el firewall del equipo.

Cómo permitir conexiones de red para la Consola de la aplicación

Los nombres de las opciones pueden variar según el sistema operativo Windows instalado.

La Consola de la aplicación en el equipo remoto utiliza el protocolo DCOM para recibir información sobre eventos de Kaspersky Embedded Systems Security 2.2 (objetos analizados, tareas finalizadas, etc.) del servicio de Kaspersky Security Management en el equipo protegido. Debe permitir conexiones de red para la Consola de la aplicación en la configuración de firewall de Windows para establecer conexiones entre la Consola de la aplicación y el servicio de Kaspersky Security Management.

En el equipo remoto donde está instalada la Consola de la aplicación, haga lo siguiente:

- Asegúrese de que esté permitido el acceso remoto anónimo a las aplicaciones COM (pero no el inicio y la activación remotos de las aplicaciones COM).
- En el firewall de Windows, abra el puerto TCP 135 y permita las conexiones de red para el archivo ejecutable del proceso de administración remota de Kaspersky Embedded Systems Security 2.2, kavfsrcn.exe.

  El equipo cliente en el que está instalada la Consola de la aplicación utiliza el puerto TCP 135 para acceder al equipo protegido y recibir una respuesta.
- Configure la regla saliente del firewall de Windows para permitir la conexión.

  A diferencia de los servicios de TCP/IP y UDP/IP tradicionales, donde un único protocolo tiene un puerto fijo, DCOM asigna dinámicamente puertos para los objetos COM a los que accede remotamente. Si existe un firewall entre el cliente (donde está instalada la Consola de la aplicación) y el terminal DCOM (el servidor protegido), debe abrirse un intervalo grande de puertos.

Los mismos pasos deben aplicarse para configurar cualquier otro firewall de software o hardware.

Si la Consola de la aplicación se abrió mientras estaba configurando la conexión entre el equipo protegido y el equipo en el cual se encuentra instalada la consola, cierre la Consola de la aplicación, espere hasta que finalice el proceso de administración remota kavfsrcn.exe de Kaspersky Embedded Systems Security 2.2 y reinicie la Consola de la aplicación. Se aplica la nueva configuración de conexión.

► *Para permitir el acceso remoto anónimo a las aplicaciones COM, siga estos pasos:*

1. En el equipo remoto donde se encuentra instalado de la Consola de Kaspersky Embedded Systems Security 2.2, abra la consola de Servicios de componentes.
2. Seleccione **Iniciar** > **Ejecutar**.
3. Escriba el comando `dcomcnfg`.
4. Haga clic en **Aceptar**.
5. Amplíe el nodo **Equipos** en la consola de **Servicios de componentes** en su equipo.
6. Abra el menú contextual en el nodo **Mi equipo**.
7. Seleccione **Propiedades**.
8. En la pestaña **Seguridad COM** de la ventana **Propiedades**, haga clic en el botón **Editar límites** ubicado en el grupo de opciones de configuración **Permisos de acceso**.
9. Asegúrese de que la casilla de verificación **Permitir el acceso remoto** esté activada para el usuario con INICIO DE SESIÓN ANÓNIMO en la ventana **Permitir el acceso remoto**.
10. Haga clic en **Aceptar**.

► *Para abrir el puerto TCP 135 en el firewall de Windows y permitir conexiones de red para el archivo ejecutable del proceso de administración remota de Kaspersky Embedded Systems Security 2.2:*

1. Cierre la Consola de Kaspersky Embedded Systems Security 2.2 en el equipo remoto.
2. Realice uno de los siguientes pasos:
   - En Microsoft Windows XP o Microsoft Windows Vista®:
     a. En Microsoft Windows XP SP2 o superior, seleccione **Iniciar** > **Firewall de Windows**.

        En Microsoft Windows Vista, seleccione **Inicio** > **Panel de control** > **Firewall de Windows** y en la ventana **Firewall de Windows** seleccione el comando **Cambiar configuración**.
     b. En la ventana Firewall de Windows (o Configuración de Firewall de Windows), haga clic en el botón **Agregar puerto** en la pestaña **Exclusiones**.
     c. En el campo **Nombre**, especifique el nombre del puerto RPC (TCP/135) o introduzca otro nombre, por ejemplo, DCOM de Kaspersky Embedded Systems Security 2.2, y especifique el número de puerto (135) en el campo **Nombre de puerto**.
     d. Seleccione el protocolo **TCP**.
     e. Haga clic en **Aceptar**.
     f. Presione el botón **Agregar** en la pestaña **Exclusiones**.
   - En Microsoft Windows 7 o una versión posterior:
     a. Seleccione **Inicio** > **Panel de control** > **Firewall de Windows**.
     b. En la ventana **Firewall de Windows**, seleccione **Permitir un programa o una característica a**

través de Firewall de Windows**.

c. En la ventana **Permitir que programas se comuniquen a través de Firewall de Windows**, haga clic en el botón **Permitir otro programa...**.

3. Especifique el archivo kavfsrcn.exe en la ventana **Agregar programa**. Está ubicado en la carpeta especificada como carpeta de destino durante la instalación de la Consola de Kaspersky Embedded Systems Security 2.2 mediante Microsoft Management Console.
4. Haga clic en **Aceptar**.
5. Haga clic en el botón **Aceptar** en la ventana Firewall de Windows (**Configuración de Firewall de Windows**).

► *Añadir la regla saliente del firewall de Windows:*

1. Seleccione **Inicio** > **Panel de control** > **Firewall de Windows**.
2. En la ventana **Firewall de Windows**, haga clic en el vínculo **Configuración avanzada**.

   Se abre la ventana **Firewall de Windows con seguridad avanzada**.
3. Seleccione el nodo secundario **Reglas salientes**.
4. Haga clic en la opción **Nueva regla** en el panel **Acciones**.
5. En la ventana **Nuevo asistente de regla saliente** que se abre, seleccione la opción **Puerto** y haga clic en **Siguiente**.
6. Seleccione el protocolo **TCP**.
7. En el campo **Puertos remotos específicos**, especifique el siguiente intervalo de puertos para permitir conexiones salientes: 1024-65535.
8. En la ventana **Acción**, seleccione la opción **Permitir la conexión**.
9. Guarde la nueva regla y cierre la ventana **Firewall de Windows con seguridad avanzada**.

Ahora el firewall de Windows permitirá conexiones de red entre la Consola de la aplicación y el servicio de Kaspersky Security Management.

Acciones a realizar después de la instalación de Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 inicia la protección y las tareas de análisis inmediatamente después de la instalación si ha activado la aplicación. Si se seleccionó **Habilitar la protección en tiempo real después de la instalación** (opción predeterminada) durante la instalación de Kaspersky Embedded Systems Security 2.2, la aplicación analizará los objetos del sistema de archivos del equipo cuando acceda a ellos. Kaspersky Embedded Systems Security 2.2 ejecutará la tarea Análisis de áreas críticas todos los viernes a las 20:00.

Le recomendamos seguir estos pasos después de instalar Kaspersky Embedded Systems Security 2.2:

- Inicie la tarea de actualización de bases de datos de la aplicación. Después de la instalación, Kaspersky Embedded Systems Security 2.2 analizará los objetos con la base de datos incluida en el kit de distribución de la aplicación.

  Recomendamos actualizar las bases de datos de Kaspersky Embedded Systems Security 2.2 inmediatamente, ya que pueden estar desactualizadas.

  La aplicación actualizará la base de datos a cada hora, de acuerdo con la programación predeterminada de

la tarea.

- Realice un análisis de áreas críticas del equipo si no había ningún software antivirus con protección de archivos en tiempo real instalado en el equipo protegido antes de instalar Kaspersky Embedded Systems Security 2.2.
- Configure las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security 2.2.

En esta sección

Inicio y configuración de la tarea de actualización de bases de datos de Kaspersky Embedded Systems Security 2.2

► *Para actualizar la base de datos de la aplicación después de la instalación, haga lo siguiente:*

1. En la configuración de la tarea Actualización de bases de datos, configure una conexión con el origen de actualizaciones a través de los servidores de actualización FTP o HTTP de Kaspersky Lab.
2. Inicie la tarea Actualización de bases de datos.

► *Para configurar la conexión con los servidores de actualización de Kaspersky Lab, en la tarea Actualización de bases de datos:*

1. Inicie la Consola de la aplicación de una de las siguientes maneras:
   - Abra la Consola de la aplicación en el equipo protegido. Para ello, seleccione **Iniciar** > **Todos los programas** > **Kaspersky Embedded Systems Security 2.2** > **Herramientas de administración** > **Consola de Kaspersky Embedded Systems Security 2.2**.
   - Si la Consola de la aplicación se ha iniciado en un equipo no protegido, conéctela al equipo protegido:
     a. Abra el menú contextual del nodo **Kaspersky Embedded Systems Security** en el árbol de la Consola de la aplicación.
     b. Seleccione el elemento **Conectarse a otro equipo**.
     c. En la ventana **Seleccionar equipo**, seleccione **Otro equipo**, e indique el nombre de la red del equipo protegido en el campo de texto.

     Si la cuenta que usaba para iniciar sesión en Microsoft Windows no tiene permisos de acceso para el servicio de Kaspersky Security Management (consulte la sección “Acerca de los permisos de acceso al servicio de Kaspersky Security Management”Acerca de los permisos de acceso al servicio de Kaspersky Security Management”, en la página 83), indique una cuenta que tenga estos permisos.

   Se abre la ventana Consola de la aplicación.
2. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
3. Seleccione el nodo secundario **Actualización de bases de datos**.

4. Haga clic en el vínculo **Propiedades** del panel de detalles.
5. En la ventana **Configuración de tareas** que se abre, abra la pestaña **Configuración de conexión**.
6. Haga lo siguiente:
   a. Si el protocolo de detección automática de proxy web (WPAD) no está configurado en la red para detectar automáticamente las configuraciones del servidor proxy en la red LAN, especifique la configuración del servidor proxy: en la sección de **Configuración del servidor proxy**, seleccione la casilla de verificación **Usar la configuración especificada del servidor proxy** y escriba la dirección en el campo **Dirección** y el número de puerto del servidor proxy en el campo **Puerto**.
   b. Si la red requiere autenticación al acceder al servidor proxy, seleccione el método de autenticación correspondiente en la lista desplegable de la sección**Configuración de autenticación del servidor proxy**:
      - **Usar autenticación NTLM** si el servidor proxy admite la autenticación NTLM integrada en Microsoft Windows. Kaspersky Embedded Systems Security 2.2 usará la cuenta de usuario especificada en las configuraciones de la tarea para acceder al servidor proxy (de forma predeterminada, la tarea se ejecuta con la cuenta de usuario **Sistema local** [**SYSTEM**]).
      - **Usar autenticación NTLM con nombre de usuario y contraseña** si el servidor proxy admite la autenticación NTLM integrada en Microsoft Windows. Kaspersky Embedded Systems Security 2.2 utilizará la cuenta especificada para acceder al servidor proxy. Introduzca un nombre de usuario y contraseña o seleccione un usuario de la lista.
      - **Aplicar nombre de usuario y contraseña** para seleccionar la autenticación básica. Introduzca un nombre de usuario y contraseña o seleccione un usuario de la lista.
7. Haga clic en **Aceptar** en la ventana **Configuración de tareas**.

Se guardará la configuración para establecer conexión con el origen de actualizaciones en la tarea Actualización de bases de datos.

► *Para ejecutar la tarea de Actualización de bases de datos:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Actualización**.
2. En el menú contextual del nodo secundario **Actualización de bases de datos**, seleccione el elemento **Iniciar**.

Iniciará la tarea Actualización de bases de datos.

Una vez que la tarea haya finalizado correctamente, podrá ver la fecha de lanzamiento de las últimas actualizaciones de bases de datos instaladas en el panel de detalles del nodo **Kaspersky Embedded Systems Security**.

Análisis de áreas críticas

Después de actualizar las bases de datos de Kaspersky Embedded Systems Security 2.2, analice el equipo en busca de malware con la tarea Análisis de áreas críticas.

► *Para ejecutar la tarea de análisis de áreas críticas, siga estos pasos:*

1. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
2. En el menú contextual del nodo secundario **Análisis de áreas críticas**, seleccione el comando **Iniciar**.

Cuando inicie la tarea, el espacio de trabajo mostrará el estado de tarea **En ejecución**.

► *Para ver el registro de tareas,*

en el panel de detalles del nodo **Análisis de áreas críticas**, haga clic en el vínculo **Abrir registro**.

Modificación del conjunto de componentes y recuperación de Kaspersky Embedded Systems Security 2.2

Puede agregar o quitar los componentes de Kaspersky Embedded Systems Security 2.2. Debe detener la tarea de Protección de archivos en tiempo real antes de poder eliminar el componente de Protección de archivos en tiempo real. En otros casos, no es necesario detener la protección de archivos en tiempo real ni el servicio de Kaspersky Security.

Si el acceso de la administración de aplicación está protegida con contraseña, Kaspersky Embedded Systems Security 2.2 solicita esta cuando intenta suprimir o modificar el conjunto de componentes en el paso adicional del Asistente de instalación.

► *Para modificar el conjunto de componentes de Kaspersky Embedded Systems Security 2.2:*

1. En el menú **Iniciar**, seleccione **Todos los programas > Kaspersky Embedded Systems Security 2.2 > Modificar o Eliminar**.

   Se abre la ventana **Modificar, reparar o eliminar la instalación** del asistente de instalación.

2. Seleccione **Modificar conjunto de componentes**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Instalación personalizada**.

3. En la ventana de **Instalación personalizada**, en la lista de componentes disponibles, seleccione los componentes que desea agregar o quitar de Kaspersky Embedded Systems Security 2.2. Para ello, realice las siguientes acciones:

   - Para cambiar el conjunto de componentes, haga clic en el botón situado junto al nombre del componente seleccionado, y en el menú contextual seleccione:
     - **El componente se instalará en el disco duro local** si desea instalar un componente;
     - **El componente y sus subcomponentes se instalarán en el disco duro local** si desea instalar un grupo de componentes.
   - Para eliminar componentes anteriormente instalados, haga clic en el botón situado junto al nombre del componente seleccionado, y seleccione **El componente no estará disponible** en el menú contextual.

   Haga clic en el botón **Instalar**.

4. En la ventana **Listo para instalar**, confirme los cambios en el conjunto de componentes haciendo clic en el botón Instalar.

5. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la instalación.

El conjunto de componentes de Kaspersky Embedded Systems Security 2.2 se modificará según la configuración especificada.

Si el funcionamiento de Kaspersky Embedded Systems Security 2.2 presenta problemas (Kaspersky Embedded Systems Security 2.2 deja de funcionar; las tareas dejan de funcionar o no se inician), puede intentar restaurar Kaspersky Embedded Systems Security 2.2. Puede realizar una restauración y guardar la configuración actual de Kaspersky Embedded Systems Security 2.2, o puede seleccionar una opción para restablecer toda la configuración

de Kaspersky Embedded Systems Security 2.2 a sus valores predeterminados.

► *Para recuperar Kaspersky Embedded Systems Security 2.2 después de que la aplicación o una tarea deje de funcionar, siga estos pasos:*

1. En el menú **Iniciar**, seleccione **Todos los programas > Kaspersky Embedded Systems Security 2.2 > Modificar o Eliminar**.

   Se abre la ventana **Modificar, reparar o eliminar** del asistente de instalación.

2. Seleccione **Reparar componentes instalados**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Reparar componentes instalados**.

3. En la ventana **Reparar componentes instalados**, seleccione la casilla de verificación **Restaurar la configuración recomendada de la aplicación** si desea restablecer las opciones de la aplicación configurada y restaurar Kaspersky Embedded Systems Security 2.2 con su configuración predeterminada. Haga clic en el botón **Instalar**.

4. En la ventana **Listo para reparar**, confirme la operación de reparación haciendo clic en el botón **Instalar**.

5. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la operación de reparación.

Kaspersky Embedded Systems Security 2.2 se restaurará según la configuración especificada.

Desinstalación mediante el asistente de instalación

Esta sección contiene instrucciones sobre cómo desinstalar Kaspersky Embedded Systems Security 2.2 y la Consola de la aplicación de un equipo protegido con el Asistente de instalación.

Desinstalación de Kaspersky Embedded Systems Security 2.2

Los nombres de configuración pueden variar en los diferentes sistemas operativos Windows.

Kaspersky Embedded Systems Security 2.2 puede desinstalarse del equipo protegido con el asistente de instalación/desinstalación.

Después de la desinstalar Kaspersky Embedded Systems Security 2.2 de un equipo protegido, es posible que se requiera reiniciarlo. Puede reiniciar el equipo más adelante.

Las opciones de desinstalación, recuperación e instalación de la aplicación mediante el panel de control de Windows no están disponibles si el sistema operativo usa la función de UAC (Control de la cuenta de usuario) o el acceso a la aplicación está protegido por contraseña.

Si el acceso de la administración de aplicación está protegida con contraseña, Kaspersky Embedded Systems Security 2.2 solicita esta cuando intenta suprimir o modificar el conjunto de componentes en el paso adicional del Asistente de instalación.

► *Para desinstalar Kaspersky Embedded Systems Security 2.2:*

1. En el menú **Iniciar**, seleccione **Todos los programas > Kaspersky Embedded Systems Security 2.2 > Modificar o Eliminar**.

   Se abre la ventana **Modificar, reparar o eliminar la instalación** del asistente de instalación.

2. Seleccione **Eliminar componentes de software**. Haga clic en el botón **Siguiente**.

   Se abre la ventana **Configuración avanzada de desinstalación de la aplicación**.

3. Si es necesario, en la ventana **Configuración avanzada de desinstalación de la aplicación**:

   a. Seleccione la casilla de verificación **Exportar objetos de Cuarentena** para exportar los objetos en cuarentena de Kaspersky Embedded Systems Security 2.2. De forma predeterminada, la casilla está desactivada.

   b. Seleccione la casilla de verificación **Exportar objetos de Copia de seguridad** para exportar los objetos en cuarentena de Kaspersky Embedded Systems Security 2.2. De forma predeterminada, la casilla está desactivada.

   c. Haga clic en el botón **Guardar en** y seleccione la carpeta a la cual desea exportar los objetos restaurados. De forma predeterminada, los objetos se exportarán a %ProgramData%\Kaspersky Lab\Kaspersky Embedded Systems Security 2.2\Uninstall.

      Haga clic en el botón **Siguiente**.

4. En la ventana **Listo para desinstalar**, confirme la desinstalación haciendo clic en el botón **Desinstalar**.
5. Haga clic en el botón **Aceptar** en la ventana que se abre una vez completada la desinstalación.

Kaspersky Embedded Systems Security 2.2 se desinstalará de un equipo protegido.

Desinstalación de la Consola de Kaspersky Embedded Systems Security 2.2

Los nombres de configuración pueden variar en los diferentes sistemas operativos Windows.

Puede desinstalar la Consola de la aplicación de el equipo con el asistente de instalación/desinstalación.

Después de haber desinstalado la Consola de la aplicación, no es necesario reiniciar el equipo.

► *Para desinstalar la Consola de la aplicación:*

1. En el menú **Iniciar**, seleccione **Todos los programas > Kaspersky Embedded Systems Security > Herramientas de administración > Modificar o eliminar**.
2. Se abrirá la ventana **Modificar, reparar o eliminar** del asistente.

   Seleccione **Eliminar componentes de software** y haga clic en el botón **Siguiente**.

3. Se abre la ventana **Listo para desinstalar**. Haga clic en el botón **Eliminar**.

   Se abre la ventana **Desinstalación finalizada**.

4. Haga clic en **Aceptar**.

Una vez que termine la desinstalación, la ventana del asistente de instalación se cerrará.

Instalación y desinstalación de la aplicación desde la línea de comandos

Esta sección indica cómo instalar y desinstalar Kaspersky Embedded Systems Security 2.2 desde la línea de comandos y contiene ejemplos de comandos para realizar dichas acciones, así como ejemplos de comandos para agregar y quitar componentes de Kaspersky Embedded Systems Security 2.2 desde la línea de comandos.

En esta sección

Acerca de la instalación y desinstalación de Kaspersky Embedded Systems Security 2.2 desde la línea de comandos

Puede instalar o desinstalar Kaspersky Embedded Systems Security 2.2 y agregar o quitar componentes al ejecutar los archivos del paquete de instalación llamado \ \product\ess_x86(x64).msi desde la línea de comandos después de haber especificado la configuración de instalación con claves.

El conjunto de "Herramientas de administración" puede instalarse en el equipo protegido o en otro equipo de la red y hacer que trabaje con la Consola de la aplicación de forma local o remota. Para ello, utilice el paquete de instalación \client\esstools.msi.

Lleve a cabo la instalación usando los derechos de una cuenta incluida en el grupo de administradores del equipo en el que se instalará la aplicación.

Si ejecuta uno de los archivos \product\ess_x86(x64).msi en el equipo protegido sin claves adicionales, Kaspersky Embedded Systems Security 2.2 se instalará con la configuración de instalación recomendada.

Puede asignar el conjunto de componentes que se instalará con la opción de la línea de comandos ADDLOCAL; para ello, enumere los códigos de los componentes o conjuntos de componentes seleccionados.

Comandos de ejemplo para la instalación de Kaspersky Embedded Systems Security 2.2

Esta sección presenta ejemplos de comandos utilizados para instalar Kaspersky Embedded Systems Security 2.2.

En equipos con Microsoft Windows de 32 bits, ejecute los archivos con el sufijo x86 del kit de distribución. En equipos con Microsoft Windows de 64 bits, ejecute los archivos con el sufijo x64 del kit de distribución.

La información detallada sobre el uso de comandos estándares de Windows Installer y opciones de la línea de comandos se proporciona en la documentación suministrada por Microsoft.

Ejemplos para la instalación de Kaspersky Embedded Systems Security 2.2 desde el archivo setup.exe

► *Para instalar Kaspersky Embedded Systems Security 2.2 con la configuración de instalación recomendada sin interacción con el usuario, ejecute el siguiente comando:*

```
\product\setup.exe /s/p EULA=1 PRIVACYPOLICY=1
```

► *Para instalar Kaspersky Embedded Systems Security 2.2 con la siguiente configuración:*

- instalar solo los componentes Protección de archivos en tiempo real y Análisis a pedido;
- no ejecutar la función de protección en tiempo real al iniciar Kaspersky Embedded Systems Security 2.2;
- no excluir de los archivos de análisis que Microsoft Corporation recomienda excluir;

ejecute el siguiente comando:

```
\product\setup.exe /p "ADDLOCAL=Oas RUNRTP=0 ADDMSEXCLUSION=0"
```

Ejemplos de comandos que se utilizan en la instalación: ejecutar el archivo .msi del paquete de instalación

► *Para instalar Kaspersky Embedded Systems Security 2.2 con la configuración de instalación recomendada sin interacción con el usuario, ejecute el siguiente comando:*

```
msiexec /i ess.msi /qn EULA=1 PRIVACYPOLICY=1
```

► *Para instalar Kaspersky Embedded Systems Security 2.2 con la configuración de instalación recomendada, muestre la interfaz de instalación y ejecute el siguiente comando:*

```
msiexec /i ess.msi /qf EULA=1 PRIVACYPOLICY=1
```

► *Para instalar Kaspersky Embedded Systems Security 2.2 y activarlo con el archivo de clave C:\0000000A.key:*

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key /qn EULA=1
PRIVACYPOLICY=1
```

► *Para instalar Kaspersky Embedded Systems Security 2.2 con un análisis preliminar de los procesos activos y los sectores de inicio de los discos locales, ejecute el siguiente comando:*

```
msiexec /i ess.msi PRESCAN=1 /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar Kaspersky Embedded Systems Security 2.2 y guardar sus archivos en la carpeta de destino C:\ESS, ejecute el siguiente comando:*

```
msiexec /i ess.msi INSTALLDIR=C:\ESS /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar Kaspersky Embedded Systems Security 2.2: guarde el archivo de registro de instalación con el nombre ess.log en la carpeta en la que se encuentre el archivo msi del paquete de instalación de Kaspersky Embedded Systems Security 2.2 y ejecute el siguiente comando:*

```
msiexec /i ess.msi /l*v ess.log /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar la Consola de Kaspersky Embedded Systems Security 2.2, ejecute el siguiente comando:*

```
msiexec /i esstools.msi /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar Kaspersky Embedded Systems Security 2.2 y activarlo con el archivo de clave C:\0000000A.key: configure Kaspersky Embedded Systems Security 2.2 según la configuración descrita en el archivo de configuración C:\settings.xml y ejecute el siguiente comando:*

```
msiexec /i ess.msi LICENSEKEYPATH=C:\0000000A.key
CONFIGPATH=C:\settings.xml /qn EULA=1 PRIVACYPOLICY=1
```

- *Para instalar el parche de la aplicación cuando Kaspersky Embedded Systems Security 2.2 está protegido con contraseña, ejecute el siguiente comando:*

```
msiexec /p "<msp file name with path>" UNLOCK_PASSWORD=<password>
```

Acciones a realizar después de la instalación de Kaspersky Embedded Systems Security 2.2

Kaspersky Embedded Systems Security 2.2 inicia la protección y las tareas de análisis inmediatamente después de la instalación si ha activado la aplicación. Si seleccionó **Habilitar la protección en tiempo real después de la instalación** durante la instalación de Kaspersky Embedded Systems Security 2.2, la aplicación analizará los objetos del sistema de archivos del equipo cuando acceda a ellos. Kaspersky Embedded Systems Security 2.2 ejecutará la tarea Análisis de áreas críticas todos los viernes a las 8 p.m.

Le recomendamos seguir estos pasos después de instalar Kaspersky Embedded Systems Security 2.2:

- Inicie la tarea de actualización de bases de datos de Kaspersky Embedded Systems Security 2.2. Después de la instalación, Kaspersky Embedded Systems Security 2.2 analizará los objetos con la base de datos incluida en el kit de distribución. Le recomendamos actualizar la base de datos de Kaspersky Embedded Systems Security 2.2 de inmediato. Para ello, debe ejecutar la tarea de Actualización de bases de datos. La base de datos se actualizará cada hora de acuerdo con la programación predeterminada.

  Por ejemplo, puede ejecutar la tarea de Actualización de bases de datos de la aplicación con el siguiente comando:

  KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1 /PROXYUSER:inetuser /PROXYPWD:123456

  En este caso, las actualizaciones de bases de datos de Kaspersky Embedded Systems Security 2.2 se

descargan desde los servidores de actualización de Kaspersky Lab. La conexión con el origen de actualizaciones se realiza a través de un servidor proxy (la dirección del servidor proxy es: proxy.company.com, puerto: 8080); para acceder al servidor, utilice la autenticación NTLM integrada en Windows y acceda con una cuenta (nombre de usuario: inetuser, contraseña: 123456).

- Realice un análisis de áreas críticas del equipo si no había ningún software antivirus con protección de archivos en tiempo real instalado en el equipo protegido antes de instalar Kaspersky Embedded Systems Security 2.2.

► *Para iniciar la tarea de Análisis de áreas críticas a través de la línea de comandos:*

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Este comando guarda el registro de tareas en el archivo scancritical.log disponible en la carpeta actual.

- Configure las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security 2.2.

Cómo agregar o eliminar componentes. Comandos de ejemplo

El componente Control de inicio de aplicaciones se instala automáticamente. No es necesario especificarlo en la lista de valores clave de ADDLOCAL agregando ni eliminando componentes de Kaspersky Embedded Systems Security 2.2.

► *Para agregar el componente Análisis a pedido a los componentes ya instalados, ejecute el siguiente comando:*

```
msiexec /i ess.msi ADDLOCAL=Oas,Ods /qn
```

o

```
\server\setup.exe /s /p "ADDLOCAL=Oas,Ods"
```

Si enumera los componentes que desea instalar junto con los componentes ya instalados, Kaspersky Embedded Systems Security 2.2 instalará de nuevo los componentes existentes.

► *Para eliminar los componentes instalados, ejecute el siguiente comando:*

```
msiexec /i ess.msi "ADDLOCAL=Oas,AppCntrl,Ksn,AntiExploit,DevCtrl,Firewall,
LogInspector,AKIntegration,PerfMonCounters,SnmpSupport,Shell,TrayApp,AVPro
tection,RamDisk REMOVE=Ods,Fim" /qn
```

Desinstalación de Kaspersky Embedded Systems Security 2.2. Comandos de ejemplo

► *Para desinstalar Kaspersky Embedded Systems Security 2.2 del equipo protegido, ejecute el siguiente comando:*

```
msiexec /x ess.msi /qn
```

o

- Para sistemas operativos de 32 bits:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} /qn
```

- Para sistemas operativos de 64 bits:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} /qn
```

► *Para desinstalar la Consola de Kaspersky Embedded Systems Security 2.2, ejecute el siguiente comando:*

```
msiexec /x esstools.msi /qn
```

o

- Para sistemas operativos de 32 bits:

```
msiexec /x {A727008F-F8CC-4B35-848A-1AECEEF22178} /qn
```

- Para sistemas operativos de 64 bits:

```
msiexec /x {D978C311-2D2D-41A3-8158-BDF97149CCD4} /qn
```

► *Para desinstalar Kaspersky Embedded Systems Security 2.2 de un equipo protegido donde esté habilitada la protección con contraseña, ejecute el siguiente comando:*

- Para sistemas operativos de 32 bits:

```
msiexec /x {D8279E25-E44F-4164-8651-10123E2E30EA} UNLOCK_PASSWORD=*** /qn
```

- Para sistemas operativos de 64 bits:

```
msiexec /x {E8584EDC-0675-4784-96E5-FD10C26A613E} UNLOCK_PASSWORD=*** /qn
```

Códigos de devolución

La siguiente tabla contiene una lista de códigos de devolución de la línea de comandos.

Table 13. Códigos de devolución

Código	Descripción
1324	El nombre de la carpeta de destino contiene caracteres no válidos.
25001	Derechos insuficientes para instalar Kaspersky Embedded Systems Security 2.2. Para instalar la aplicación, inicie el asistente de instalación con derechos del administrador local.
25003	Kaspersky Embedded Systems Security 2.2 no se puede instalar en equipos que ejecutan esta versión de Microsoft Windows. Inicie el asistente de instalación para versiones de 64 bits de Microsoft Windows.
25004	Se ha detectado un software incompatible. Para continuar la instalación, desinstale el siguiente software: <lista de softwares incompatibles>.
25010	La ruta indicada no se puede usar para guardar objetos puestos en cuarentena.
25011	El nombre de la carpeta para guardar objetos en cuarentena contiene caracteres no válidos.
26251	No es posible descargar DLL de contadores de rendimiento.
26252	No es posible descargar DLL de contadores de rendimiento.

Código	Descripción
27300	El controlador no se puede instalar.
27301	El controlador no se puede desinstalar.
27302	El componente de la red no se puede instalar. Se alcanzó la cantidad máxima admitida de dispositivos filtrados.
27303	Bases de datos antivirus no encontradas.

Instalación y desinstalación de la aplicación mediante Kaspersky Security Center

Esta sección contiene información general acerca de la instalación de Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center. Asimismo, describe cómo instalar y desinstalar Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center y otras tareas que deben realizarse tras la instalación de Kaspersky Embedded Systems Security 2.2.

En esta sección

Información general sobre la instalación mediante Kaspersky Security Center

Puede instalar Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center con la tarea de instalación remota.

Una vez finalizada la tarea de instalación remota, Kaspersky Embedded Systems Security 2.2 se instalará con la misma configuración en varios equipos.

Todos los equipos pueden combinarse en un solo grupo de administración y puede crearse una tarea de grupo que instale Kaspersky Embedded Systems Security 2.2 en los equipos del grupo.

Puede crear una tarea que instale Kaspersky Embedded Systems Security 2.2 de forma remota en un grupo de equipos que no pertenecen al mismo grupo de administración. Al crear esta tarea, debe generar una lista de los equipos individuales en los que se debe instalar Kaspersky Embedded Systems Security 2.2.

La información detallada acerca de la tarea de instalación remota está disponible en la *Ayuda de Kaspersky Security Center*.

Derechos para instalar o desinstalar Kaspersky Embedded Systems Security 2.2

La cuenta especificada en la tarea de instalación/desinstalación remota debe pertenecer al grupo de administradores en cada uno de los equipos protegidos en todos los casos, excepto en los descritos a continuación:

- Si el Agente de red de Kaspersky Security Center ya está instalado en los equipos en los que se instalará Kaspersky Embedded Systems Security 2.2 (no importa en qué dominio estén los equipos o si pertenecen a alguno).

  Si el Agente de red todavía no está instalado en los equipos, se puede instalar junto con Kaspersky Embedded Systems Security 2.2 mediante una tarea de instalación remota. Antes de instalar el Agente de red, asegúrese de que la cuenta que indique en la tarea esté incluida en el grupo de administradores de cada uno de los equipos.

- Todos los equipos en los que desea instalar Kaspersky Embedded Systems Security 2.2 pertenecen al mismo dominio como servidores de administración y el Servidor de administración está registrado con la cuenta **Administrador de dominio** (si esta cuenta dispone de derechos de administrador local en los equipos incluidos en el dominio).

De manera predeterminada, al usar el método **Instalación forzada**, la tarea de instalación remota se inicia desde la cuenta con la que se ejecuta el servidor de administración.

Al trabajar con tareas de grupo o con tareas para grupos de equipos en el modo de instalación/desinstalación forzada, la cuenta debe disponer de los siguientes derechos en un equipo cliente:

- Derecho de ejecutar aplicaciones remotamente.
- Derechos sobre el recurso **Admin$**.
- Derecho **Inicio de sesión como servicio**.

Procedimiento de instalación de Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center

La información detallada sobre la generación de un paquete de instalación y la creación de una tarea de instalación remota está disponible en la Guía de implementación de Kaspersky Security Center.

Si tiene pensado administrar Kaspersky Embedded Systems Security 2.2 desde Kaspersky Security Center en el futuro, asegúrese de que se cumplan las siguientes condiciones:

- El equipo en el que está instalado el Servidor de administración de Kaspersky Security Center también tiene el Complemento de administración instalado (archivo \product\klcfginst.exe del kit de distribución de Kaspersky Embedded Systems Security 2.2).
- El Agente de red de Kaspersky Security Center está instalado en los equipos protegidos. Si el Agente de red de Kaspersky Security Center no está instalado en los equipos protegidos, puede instalarlo junto con Kaspersky Embedded Systems Security 2.2 mediante una tarea de ejecución remota.

Los equipos también pueden combinarse en un grupo de administración de forma previa para luego administrar la configuración de protección a través de las directivas y tareas de grupo de Kaspersky Security Center.

► *Para instalar Kaspersky Embedded Systems Security 2.2 con la ayuda de la tarea de instalación remota:*

1. Inicie la Consola de administración de Kaspersky Security Center.
2. En Kaspersky Security Center, expanda el nodo **Instalación remota** y, en el nodo secundario **Paquetes de instalación**, seleccione **Crear paquete de instalación para una aplicación de Kaspersky Lab**.
3. Ingrese el nombre del paquete de instalación.
4. Especifique el archivo ess.kud del kit de distribución de Kaspersky Embedded Systems Security 2.2 como el archivo del paquete de instalación.

   Se abre la ventana **Contrato de licencia de usuario final y Política de privacidad**.
5. Si acepta los términos y condiciones del Contrato de licencia de usuario final y la Política de privacidad, seleccione las casillas **los términos y condiciones de este Contrato de licencia de usuario final** y **Política de privacidad que describe el manejo de datos** a fin de continuar con la instalación.

   Debe aceptar el Contrato de licencia y la Política de privacidad para continuar.
6. Para cambiar el conjunto de componentes de Kaspersky Embedded Systems Security 2.2 que se instalarán (consulte la sección “Modificación del conjunto de componentes y recuperación de Kaspersky Embedded Systems Security 2.2”, en la página 50) y las opciones de instalación predeterminadas (consulte la sección “Configuración de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer”, en la página 31) en el paquete de instalación:
   a. En Kaspersky Security Center, expanda el nodo **Instalación remota**.
   b. En el espacio de trabajo del nodo secundario **Paquetes de instalación**, abra el menú contextual del paquete de instalación Kaspersky Embedded Systems Security 2.2 creado y seleccione **Propiedades**.
   c. En la ventana **Propiedades: <nombre del paquete de instalación>** ubicada en la sección **Configuración**, haga lo siguiente:
      a. En el grupo de opciones de configuración **Componentes a instalar**, seleccione las casillas situadas junto a los nombres de los componentes de Kaspersky Embedded Systems Security 2.2 que desea instalar.
      b. Para indicar una carpeta de destino que no sea la predeterminada, especifique el nombre y la ruta de la carpeta en el campo **Carpeta de destino**.

         La ruta de acceso a la carpeta de destino puede contener variables de entorno del sistema. Si la carpeta no existe en el equipo, se creará.
      c. En el grupo **Configuración avanzada de instalación**, configure los siguientes parámetros:
         - Analizar el equipo en busca de virus antes de la instalación.
         - Habilitar la protección en tiempo real después de la instalación.
         - Agregar archivos recomendados por Microsoft a la lista de exclusiones.
      d. Agregar archivos recomendados por Kaspersky Lab a la lista de exclusiones.
   d. En la ventana **Propiedades: <nombre del paquete de instalación>**, haga clic en **Aceptar**.
7. En el nodo **Paquetes de instalación**, cree una tarea para instalar la Consola de Kaspersky Embedded Systems Security 2.2 de forma remota en los equipos seleccionados (grupo de administración). Configure los parámetros de la tarea.

   Para saber más sobre creación y configuración de tareas de instalación remotas, consulte la *Ayuda de*

Kaspersky Security Center.

8. Ejecute la tarea de instalación remota de Kaspersky Embedded Systems Security 2.2.

Kaspersky Embedded Systems Security 2.2 se instalará en los equipos especificados en la tarea.

Acciones a realizar después de la instalación de Kaspersky Embedded Systems Security 2.2

Una vez instalado Kaspersky Embedded Systems Security 2.2, recomendamos actualizar las bases de datos de Kaspersky Embedded Systems Security 2.2 en los equipos y realizar un análisis de áreas críticas del equipo, en caso de que los equipos no hayan tenido instaladas aplicaciones antivirus con una función habilitada de Protección en tiempo real antes de la instalación de Kaspersky Embedded Systems Security 2.2.

Si los equipos en los que se instaló Kaspersky Embedded Systems Security 2.2 están unificados en un único grupo de administración en Kaspersky Security Center, puede llevar a cabo estas tareas de la siguiente manera:

1. Cree tareas de Actualización de bases de datos para los grupos de equipos en los que se instaló Kaspersky Embedded Systems Security 2.2. Establezca el servidor de administración de Kaspersky Security Center como origen de actualizaciones.
2. Cree una tarea de grupo Análisis a pedido con el estado de tarea Análisis de áreas críticas. Kaspersky Security Center evalúa el estado de seguridad de cada uno de los equipos del grupo de acuerdo con los resultados de la ejecución de esta tarea, no en función de los resultados la tarea Análisis de áreas críticas.
3. Cree una directiva para el grupo de equipos. En las propiedades de la directiva creada, en la pestaña **Tareas del sistema**, desactive el inicio programado de las tareas de análisis del sistema, según sea necesario, y las tareas de actualización de bases de datos en los equipos del grupo de administración.

También puede configurar las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security 2.2.

Instalación de la Consola de la aplicación mediante Kaspersky Security Center

La información detallada sobre la creación de un paquete de instalación y la tarea de instalación remota está disponible en la *Guía de implementación de Kaspersky Security Center*.

► *Para instalar la Consola de la aplicación mediante una tarea de instalación:*

1. En la Consola de administración de Kaspersky Security Center, expanda el nodo **Instalación remota** y, en el nodo secundario **Paquetes de instalación**, cree un nuevo paquete de instalación a partir del archivo client\setup.exe. Al crear un paquete de instalación:
   - En la ventana **Seleccione el paquete de distribución para la instalación**, seleccione el archivo client\setup.exe de la carpeta del kit de distribución de Kaspersky Embedded Systems Security 2.2 y seleccione la casilla de verificación **Copiar carpeta al paquete de instalación**.
   - Si es necesario, use la opción de la línea de comandos ADDLOCAL para modificar el conjunto de componentes que desea instalar en el campo **Configuración de inicio del archivo ejecutable** (opcional) y cambie la carpeta de destino.

Por ejemplo, para instalar únicamente la Consola de la aplicación en la carpeta C:\KasperskyConsole sin instalar el archivo de ayuda ni la documentación, proceda de la siguiente forma:

```
/s /p "ADDLOCAL=MmcSnapin INSTALLDIR=C:\KasperskyConsole EULA=1
PRIVACYPOLICY=1"
```

2. En el nodo **Paquetes de instalación**, cree una tarea para instalar la Consola de la aplicación de forma remota en los equipos seleccionados (grupo de administración). Configure los parámetros de la tarea.

Para saber más sobre creación y configuración de tareas de instalación remotas, consulte la *Ayuda de Kaspersky Security Center*.

3. Ejecute la tarea de instalación remota creada.

La Consola de la aplicación se instalará en los equipos especificados en la tarea.

Desinstalación de Kaspersky Embedded Systems Security 2.2 a través de Kaspersky Security Center

Si el acceso de la administración de Kaspersky Embedded Systems Security 2.2 en equipos de la red está protegido por contraseña, escriba la contraseña al crear una tarea de desinstalación de varias aplicaciones. Si la protección por contraseña no está administrada centralmente por la aplicación se desinstalará correctamente desde los equipos con acceso protegido en los cuales la contraseña introducida se corresponda con el valor establecido. Kaspersky Embedded Systems Security 2.2 no se desinstalará del resto de los equipos.

► *Para desinstalar Kaspersky Embedded Systems Security 2.2, siga los siguientes pasos en la Consola de administración de Kaspersky Security Center:*

1. En la Consola de administración de Kaspersky Security Center, cree e inicie la tarea de desinstalación de la aplicación.
2. En la tarea, seleccione el método de desinstalación (similar a la selección del método de instalación; consulte la sección anterior) y especifique una cuenta cuyos derechos del Servidor de administración usará para dirigirse a los equipos. Kaspersky Embedded Systems Security 2.2 solo puede desinstalarse con la configuración de desinstalación predeterminada (consulte la sección “Configuración de instalación y desinstalación y opciones de la línea de comandos para el servicio de Windows Installer”, en la página 31).

Instalación y desinstalación a través de directivas de grupo de Active Directory

Esta sección describe cómo instalar y desinstalar Kaspersky Embedded Systems Security 2.2 mediante directivas de grupo de Active Directory. También contiene información sobre las tareas que deben realizarse tras la instalación de Kaspersky Embedded Systems Security 2.2 a través de las directivas de grupo.

En esta sección

Instalación de Kaspersky Embedded Systems Security 2.2 mediante directivas de grupo de Active Directory

Puede instalar Kaspersky Embedded Systems Security 2.2 en varios equipos a través de la directiva de grupo de Active Directory. Puede instalar la Consola de la aplicación del mismo modo.

Los equipos donde desea instalar Kaspersky Embedded Systems Security 2.2 o la Consola de la aplicación deben pertenecer a un único dominio y a una única unidad organizada.

Los sistemas operativos de los equipos en los que instale Kaspersky Embedded Systems Security 2.2 con la ayuda de directivas deben tener la misma versión (32 bits o 64 bits).

Usted debe disponer de derechos de administrador de dominio.

Para instalar Kaspersky Embedded Systems Security 2.2, use los paquetes de instalación de ess_x86(x64).msi. Para instalar la Consola de la aplicación, use los paquetes de instalación de esstools.msi.

Se ofrece información detallada sobre el uso de las directivas de grupo de Active Directory en la documentación provista por Microsoft.

► *Para instalar Kaspersky Embedded Systems Security 2.2 (o la Consola de la aplicación):*

1. Guarde el archivo msi del paquete de instalación que corresponda al tamaño de palabra (32 bits o 64 bits) según la versión instalada del sistema operativo Microsoft Windows, en la carpeta pública del controlador de dominio.
2. En el controlador de dominio, cree una nueva directiva para el grupo al que pertenezcan los equipos.
3. Utilice el **Editor de objetos de directiva de grupo** para crear un nuevo paquete de instalación en el nodo **Configuración del equipo**. Escriba la ruta del archivo msi del paquete de instalación de Kaspersky Embedded Systems Security 2.2 (o la Consola de la aplicación) en el formato UNC (convención de nomenclatura universal).
4. Seleccione **Instalar siempre con privilegios elevados** en el servicio Windows Installer, tanto en el nodo **Configuración del equipo** como en el nodo **Configuración del usuario** del grupo seleccionado.
5. Aplique los cambios con el comando `gpupdate / force`.

Kaspersky Embedded Systems Security 2.2 se instalará en los equipos del grupo después de que se hayan reiniciado y antes de iniciar sesión en Microsoft Windows.

Acciones a realizar después de la instalación de Kaspersky Embedded Systems Security 2.2

Luego de instalar Kaspersky Embedded Systems Security 2.2 en los equipos protegidos, se recomienda actualizar inmediatamente las bases de datos de la aplicación y ejecutar un Análisis de áreas críticas. Puede realizar estas acciones (consulte la sección “Acciones a realizar después de la instalación de Kaspersky Embedded Systems Security 2.2”, en la página 47) desde la Consola de la aplicación.

También puede configurar las notificaciones del administrador sobre eventos de Kaspersky Embedded Systems Security 2.2.

Desinstalación de Kaspersky Embedded Systems Security 2.2 mediante directivas de grupo de Active Directory

Si instaló Kaspersky Embedded Systems Security 2.2 (o la Consola de la aplicación) en los equipos del grupo a través de la directiva de grupo de Active Directory, también puede utilizarla para desinstalar Kaspersky Embedded Systems Security 2.2 (o la Consola de la aplicación).

La aplicación puede desinstalarse únicamente con los parámetros de desinstalación predeterminados.

Se ofrece información detallada sobre el uso de las directivas de grupo de Active Directory en la documentación provista por Microsoft.

Si el acceso a la administración de la aplicación está protegido por contraseña, la desinstalación de Kaspersky Embedded Systems Security 2.2 mediante directivas de grupo de Active Directory no está disponible.

► *Para desinstalar Kaspersky Embedded Systems Security 2.2 (o la Consola de la aplicación):*

1. Seleccione la unidad organizativa en el controlador de dominio de los equipos en los que desea desinstalar Kaspersky Embedded Systems Security 2.2 o la Consola de la aplicación.
2. Seleccione la directiva creada para la instalación de Kaspersky Embedded Systems Security 2.2, y en el **Editor de objetos de directivas de grupo**, en el nodo **Instalación de software** (**Configuración del equipo** > **Configuración de software** > **Instalación de software**), abra el menú contextual del paquete de instalación de Kaspersky Embedded Systems Security 2.2 (o la Consola de la aplicación) y seleccione el comando **Todas las tareas > Eliminar**.
3. Seleccione el método de eliminación **Desinstalar inmediatamente el software de usuarios y equipos**.
4. Aplique los cambios con el comando `gpupdate / force`.

Verificación de funciones de Kaspersky Embedded Systems Security 2.2. Uso del virus de prueba EICAR

Esta sección describe el virus de prueba EICAR y cómo debe utilizarse para comprobar las funciones Protección en tiempo real y Análisis a pedido de Kaspersky Embedded Systems Security 2.2.

En esta sección

Acerca del virus de prueba EICAR

El virus de prueba fue diseñado para comprobar el funcionamiento de las aplicaciones antivirus. Fue desarrollado

por el Instituto Europeo para la Investigación de los Antivirus Informáticos (EICAR).

El virus de prueba no es un virus y no contiene código de programa en su equipo, aunque las aplicaciones antivirus de la mayoría de los proveedores lo detectan como una amenaza.

El archivo contiene el virus de prueba llamado eicar.com. Se puede descargar desde el sitio web de EICAR, http://www.eicar.org/anti_virus_test_file.htm.

Antes de guardar el archivo en una carpeta en el disco duro de su equipo, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada en esa unidad.

El archivo eicar.com contiene una línea de texto. Cuando se analiza el archivo, Kaspersky Embedded Systems Security 2.2 detecta una amenaza de prueba en esta línea de texto, le asigna el estado **Infectado** al archivo y lo elimina. La información acerca de la amenaza detectada en el archivo aparecerá en la Consola de la aplicación y en el registro de tareas.

Puede utilizar el archivo eicar.com para comprobar cómo Kaspersky Embedded Systems Security 2.2 desinfecta los objetos infectados y cómo detecta objetos probablemente infectados. Para hacerlo, abra el archivo mediante un editor de texto, agregue uno de los prefijos enumerados en la tabla a continuación al principio de la línea de texto en el archivo y guarde el archivo con un nombre nuevo; por ejemplo, eicar_cure.com.

Para asegurarse de que Kaspersky Embedded Systems Security 2.2 procese el archivo eicar.com con un prefijo, en la sección **Protección de objetos** de la configuración de seguridad, establezca el valor **Todos los objetos** en las tareas de Protección de archivos en tiempo real y Análisis a pedido de Kaspersky Embedded Systems Security 2.2.

Table 14. Prefijos de archivos EICAR

Prefijo	Estado del archivo después del análisis y la acción tomada por Kaspersky Embedded Systems Security 2.2
Sin prefijo	Kaspersky Embedded Systems Security 2.2 le asigna el estado **Infectado** al objeto y lo elimina.
SUSP–	Kaspersky Embedded Systems Security 2.2 le asigna el estado **Probablemente infectado** al objeto (detectado por el analizador heurístico) y lo elimina (los objetos probablemente infectados no se desinfectan).
WARN–	Kaspersky Embedded Systems Security 2.2 le asigna el estado **Probablemente infectado** al objeto (el código del objeto coincide en parte con el código de una amenaza conocida) y lo elimina (los objetos probablemente infectados no se desinfectan).
CURE–	Kaspersky Embedded Systems Security 2.2 le asigna el estado **Infectado** al objeto y lo desinfecta. Si la desinfección se realiza correctamente, la totalidad del texto del archivo se reemplaza con la palabra "CURE".

Prueba de Protección en tiempo real y Análisis a pedido

Después de instalar Kaspersky Embedded Systems Security 2.2, puede confirmarle a Kaspersky Embedded Systems Security 2.2 que encuentre objetos que contengan código malicioso. Para comprobarlo, puede usar el

virus de prueba de EICAR (consulte la sección “Acerca del virus de prueba EICAR”, en la página 64).

► *Para comprobar la función Protección en tiempo real, siga estos pasos:*

1. Descargue el archivo eicar.com en el sitio web de EICAR, http://www.eicar.org/anti_virus_test_file.htm. Guárdelo en una carpeta pública en el disco local de cualquiera de los equipos de la red.

   Antes de guardar el archivo en la carpeta, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada en la carpeta.

2. Si desea comprobar el funcionamiento de las notificaciones de red al usuario, asegúrese de que el servicio Windows Messenger de Microsoft esté habilitado tanto en el equipo protegido como en el equipo en el que guardó el archivo eicar.com.
3. Abra la Consola de la aplicación.
4. Copie el archivo eicar.com guardado en el disco local del equipo protegido mediante alguno de los siguientes métodos:
   - Para probar las notificaciones a través de la ventana Terminal Services, copie el archivo eicar.com en el equipo después de conectarlo al equipo mediante la utilidad Conexión remota a escritorio.
   - Para probar notificaciones a través del servicio Windows Messenger de Microsoft, use los sitios de la red del equipo para copiar el archivo eicar.com del equipo donde lo guardó.

La protección de archivos en tiempo real funciona correctamente si se cumplen las siguientes condiciones:

- El archivo eicar.com se ha eliminado del equipo protegido.
- En la Consola de la aplicación, se le asigna el estado **Crítico** al registro de tareas. Apareció una línea en el registro con información sobre una amenaza en el archivo eicar.com. (Para ver el registro de tareas, en el árbol de la Consola de la aplicación, expanda el nodo **Protección del equipo en tiempo real**, seleccione la tarea Protección de archivos en tiempo real y finalmente, en el panel de información, haga clic en el vínculo **Abrir registro**).
  - Aparece el siguiente mensaje del servicio Windows Messenger de Microsoft en el equipo desde el que copió el archivo: `Kaspersky Embedded Systems Security 2.2 bloqueó el acceso a <ruta del archivo en el equipo>\eicar.com en el equipo <nombre de red del equipo> a las <hora del evento>. Motivo: Amenaza detectada. Virus: EICAR-Test-File. Nombre de usuario: <nombre de usuario>. Nombre del equipo: <nombre de red del equipo desde el que se copió el archivo>.`

  Asegúrese de que el servicio Windows Messenger de Microsoft esté en funcionamiento en el equipo desde el que se copió el archivo eicar.com.

► *Para comprobar la función Análisis a pedido, siga estos pasos:*

1. Descargue el archivo eicar.com en el sitio web de EICAR, http://www.eicar.org/anti_virus_test_file.htm. Guárdelo en una carpeta pública en el disco local de cualquiera de los equipos de la red.

   Antes de guardar el archivo en la carpeta, asegúrese de que la Protección de archivos en tiempo real esté deshabilitada en la carpeta.

2. Abra la Consola de la aplicación.
3. Haga lo siguiente:
    a. Expanda el nodo **Análisis a pedido** en el árbol de la Consola de la aplicación.
    b. Seleccione el nodo secundario **Análisis de áreas críticas**.
    c. En la pestaña **Configuración del área de análisis**, abra el menú contextual del nodo **Red** y seleccione **Agregar archivo de red**.
    d. Introduzca la ruta de acceso de red al archivo eicar.com en el equipo remoto con el formato UNC (convención de nomenclatura universal).
    e. Seleccione la casilla para incluir la ruta de acceso de red agregada en el área del análisis.
    f. Ejecute la tarea Análisis de áreas críticas.

El Análisis a pedido funciona correctamente si se cumplen las siguientes condiciones:

- El archivo eicar.com se eliminó del disco duro del equipo.

En la Consola de la aplicación, se le asigna el estado **Crítico** al registro de tareas; en el registro de la tarea Análisis de áreas críticas aparece una línea con información acerca de una amenaza en el archivo eicar.com. (Para ver el registro de tareas, en el árbol de la Consola de la aplicación, expanda el nodo de aplicaciones **Análisis a pedido**, seleccione la tarea Análisis de áreas críticas y finalmente, en el panel de información, haga clic en el vínculo **Abrir registro**).

Interfaz de la aplicación

Puede controlar Kaspersky Embedded Systems Security 2.2 a través del Complemento de administración y la Consola de la aplicación local. Las acciones que pueden llevarse a cabo con la Consola de la aplicación local se describen en la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*. La interfaz de la Consola de administración de Kaspersky Security Center se usa para realizar acciones con el Complemento de administración. Consulte información detallada sobre la interfaz de Kaspersky Security Center en la *Ayuda de Kaspersky Security Center*.

Licencia de la aplicación

Esta sección brinda información sobre los conceptos principales relacionados con el otorgamiento de una licencia de la aplicación.

En este capítulo

Acerca del Contrato de licencia de usuario final

El *Contrato de licencia de usuario final* es un acuerdo vinculante entre usted y AO Kaspersky Lab en el que se estipulan los términos que rigen el uso de la aplicación.

Recomendamos revisar detenidamente los términos del Contrato de licencia de usuario final antes de comenzar a usar la aplicación.

Puede revisar los términos del Contrato de licencia de usuario final de las siguientes formas:

- Durante la instalación de Kaspersky Embedded Systems Security 2.2
- Leyendo el archivo license.txt. Este documento está incluido en el kit de distribución de la aplicación.

Al confirmar que acepta el Contrato de licencia de usuario final al instalar la aplicación, debe indicar su aceptación de los términos del Contrato de licencia de usuario final. Si no acepta los términos del Contrato de licencia de usuario final, debe anular la instalación de la aplicación y no debe usarla.

Acerca de la licencia

Una licencia es un derecho con límite de tiempo para usar la aplicación que se le otorga de acuerdo con el Contrato de licencia de usuario final.

Una licencia válida le da derecho a recibir los siguientes servicios:

- Uso de la aplicación de acuerdo con los términos del Contrato de licencia de usuario final
- Soporte técnico

El área del servicio y el plazo del uso de la aplicación dependen del tipo de licencia con la cual se activó la aplicación.

La aplicación se activa usando un archivo de clave para una licencia comercial comprada.

Una licencia comercial es una licencia paga otorgada con la compra de la aplicación.

Kaspersky Embedded Systems Security 2.2 ofrece dos tipos de licencias comerciales:

- Licencia estándar de Kaspersky Embedded Systems Security
- Licencia extendida de Kaspersky Embedded Systems Security Compliance Edition, que incluye dos componentes de inspección adicionales del sistema: Monitor de integridad de archivos e inspección de registros.

Cuando expira una licencia comercial, la aplicación sigue ejecutándose, pero algunas de sus funciones dejan de estar disponibles (por ejemplo, las bases de datos de Kaspersky Embedded Systems Security 2.2 no se pueden actualizar). Para seguir usando todas las funciones de Kaspersky Embedded Systems Security 2.2, debe renovar su licencia comercial.

Para garantizar la máxima protección de su equipo contra amenazas a la seguridad, recomendamos renovar la licencia antes de que expire.

Asegúrese de que la clave adicional que agrega tenga una fecha de caducidad posterior que la activa.

Acerca del certificado de licencia

Un *certificado de licencia* es un documento que se le entrega junto con un archivo de clave o un código de activación (si corresponde).

Un certificado de licencia contiene la siguiente información sobre la licencia proporcionada:

- Número de pedido
- Información acerca del usuario a quien se le ha otorgado la licencia
- Información acerca de la aplicación que puede activarse con la licencia proporcionada
- Límite del número de unidades de licencia (es decir, dispositivos en los cuales puede usarse la aplicación con la licencia proporcionada)
- Fecha de inicio de validez de la licencia
- Fecha de caducidad de la licencia o término de la licencia
- Tipo de licencia

Acerca del código de activación

Un *código de activación* es una secuencia única de 20 letras y números. Debe introducir un código de activación para poder agregar una clave de activación de Kaspersky Embedded Systems Security 2.2. Recibirá el código de activación en la dirección de correo electrónico que proporcionó al comprar Kaspersky Embedded Systems Security 2.2.

Para activar la aplicación con un código de activación, necesita acceso a Internet a fin de conectarse con los servidores de activación de Kaspersky Lab.

Si ha perdido su código de activación después de instalar la aplicación, puede recuperarlo. Es posible que necesite el código de activación para registrar Kaspersky CompanyAccount, por ejemplo. Para recuperar su código de activación, póngase en contacto con el Servicio de soporte técnico de Kaspersky Lab.

Acerca de la clave

Una *clave* es una secuencia de bits con la cual puede activar y posteriormente usar la aplicación de acuerdo con los términos del Contrato de licencia de usuario final. Kaspersky Lab genera una clave.

Para agregar una clave a la aplicación, use un archivo de clave. Luego de agregar una clave a la aplicación, esta aparece en la interfaz de la aplicación como una secuencia alfanumérica exclusiva.

Kaspersky Lab puede incluir una clave en una lista negra si se producen infracciones del Contrato de licencia. Si se bloquea su clave, se debe agregar una clave diferente para que funcione la aplicación.

Una clave puede ser una "clave activa" o una "clave adicional".

Una *clave activa* es la clave que usa la aplicación actualmente para funcionar. Se puede agregar una clave para una licencia comercial como clave activa. La aplicación no puede tener más de una clave activa.

Una *clave adicional* es una clave que confirma el derecho de usar la aplicación pero que actualmente no se encuentra en uso. La clave adicional se activa automáticamente cuando expira la licencia asociada con la clave actual activa. Se puede agregar una clave adicional solo si hay una clave activa.

Acerca del archivo de clave

Un *archivo de clave* es un archivo con la extensión .key que le proporciona Kaspersky Lab. Los archivos de clave están diseñados para activar la aplicación mediante la adición de una clave.

Recibirá un archivo de clave en la dirección de correo electrónico que proporcionó al comprar Kaspersky Embedded Systems Security 2.2.

No necesita conectarse con los servidores de activación de Kaspersky Lab a fin de activar la aplicación con un archivo de clave.

Puede recuperar un archivo de clave si lo elimina accidentalmente. Es posible que necesite un archivo de clave para registrarse en Kaspersky CompanyAccount.

Para recuperar un archivo de clave, debe realizar una de las siguientes acciones:

- Ponerse en contacto con el Servicio de soporte técnico https://support.kaspersky.com/mx.
- Obtener un archivo de clave en el sitio web de Kaspersky Lab según el código de activación que ya tenga.

Sobre la provisión de datos

El Contrato de licencia para Kaspersky Embedded Systems Security 2.2, específicamente la sección titulada "Términos del procesamiento de datos", especifica los términos, la responsabilidad legal y el procedimiento para enviar y procesar los datos indicados en esta Guía. Antes de aceptar el Contrato de licencia, revise detenidamente sus términos, además de todos los documentos vinculados con el Contrato de licencia.

Los datos que Kaspersky Lab recibe cuando usted utiliza la aplicación se protegen y se procesan de acuerdo con la Política de privacidad, disponible en http://www.kaspersky.com/products-and-services-privacy-policy.

Al aceptar los términos del Contrato de licencia, acepta enviar automáticamente los siguientes datos a Kaspersky Lab:

- Admitir el mecanismo para recibir actualizaciones; información sobre la aplicación instalada y su activación: el identificador de la aplicación instalada y su versión completa, incluido el número de compilación, el tipo, y el identificador de licencia, el identificador de instalación y el identificador de tarea de actualización único.
- Usar la capacidad de explorar artículos de la Base de conocimientos cuando se produzcan errores en la aplicación (servicio de Redirección); información sobre la aplicación y el tipo del vínculo, específicamente: el nombre, la configuración regional y el número de versión completo de la aplicación,el tipo de vínculo de redirección y el identificador del error.
- Administrar confirmaciones para el procesamiento de datos; información sobre el estado de aceptación de contratos de licencia y otros documentos que estipulan términos de transferencia de datos: el identificador y la versión del Contrato de licencia u otro documento, como parte de los cuales se aceptan o se rechazan los términos de procesamiento de datos; un atributo, indicando la acción del usuario (confirmación o retiro de la aceptación de los términos); la fecha y la hora de los cambios de estado de la aceptación de los términos de procesamiento de datos.

Puede revisar los términos del Contrato de licencia de usuario final de las siguientes formas:

- Durante la instalación de la aplicación Kaspersky Embedded Systems Security 2.2, el asistente de instalación muestra el texto completo del Contrato de licencia en un paso donde se requiere la aceptación de sus términos.
- En cualquier momento en el archivo .TXT (license.txt), que contiene el texto completo del Contrato de licencia. El archivo se incluye en el kit de distribución de Kaspersky Embedded Systems Security 2.2, junto con los archivos de instalación de la aplicación.

Procesamiento de datos local

Al ejecutar las funciones principales de la aplicación descritas en esta Guía, Kaspersky Embedded Systems Security 2.2 procesa y almacena localmente una secuencia de tipos de datos en el equipo protegido:

- Información sobre archivos analizados y objetos detectados, por ejemplo, nombres y atributos de archivos procesados y rutas completas de los archivos en los medios analizados, acciones realizadas en archivos analizados, cuentas de usuarios que realizan cualquier acción en la red protegida o el equipo protegido, nombres y datos de los dispositivos analizados, información sobre procesos que se ejecutan en el sistema.
- Información sobre la actividad y la configuración del sistema operativo, por ejemplo, la configuración del Firewall de Windows, entradas del registro de eventos de Windows, nombres de cuentas de usuario, inicios de archivos ejecutables, sus sumas de comprobación y atributos.

Kaspersky Embedded Systems Security 2.2 procesa y almacena datos como parte de la funcionalidad básica de la aplicación, particularmente para registrar eventos de aplicaciones y recibir datos de diagnóstico. Los datos procesados localmente están protegidos según las opciones configuradas y aplicadas.

Kaspersky Embedded Systems Security 2.2 le permite configurar el nivel de la protección para los datos procesados localmente: puede cambiar los privilegios del usuario para acceder a datos de proceso, cambiar periodos de retención para tales datos, deshabilitar de manera parcial o total la funcionalidad que involucra el registro de datos, y cambiar la ruta y los atributos de la carpeta en el medio donde se registran los datos.

La información detallada sobre la configuración de la funcionalidad de la aplicación que involucra el procesamiento de la información y la configuración predeterminada de almacenamiento de los datos procesados puede encontrarse en las secciones correspondientes de esta Guía.

De forma predeterminada, todos los datos almacenados en un equipo local se eliminan después de la desinstalación de Kaspersky Embedded Systems Security 2.2, excepto los archivos con información de diagnóstico (archivos de rastreo y de volcado) y los registros de la actividad de la aplicación del registro de eventos de Windows. Debe eliminar manualmente estos archivos. Puede encontrar información detallada sobre la configuración de procesos de diagnóstico en las secciones correspondientes de esta Guía.

Al desinstalar la aplicación puede guardar el contenido de los depósitos de copia de seguridad y de cuarentena.

Activación de la aplicación con una clave

Puede activar Kaspersky Embedded Systems Security 2.2 aplicando una clave.

Si ya se ha agregado una clave activa para Kaspersky Embedded Systems Security 2.2 y se agrega otra clave como clave activa, la nueva clave sustituye a la clave agregada previamente. La clave activa instalada anteriormente se elimina.

Si ya se ha agregado una clave adicional para Kaspersky Embedded Systems Security 2.2 y se agrega otra clave como adicional, la nueva clave sustituye a la clave agregada previamente. La clave adicional instalada anteriormente se elimina.

Si ya se han agregado una clave activa y una clave adicional para Kaspersky Embedded Systems Security 2.2 y se agrega una nueva clave como clave activa, la nueva clave sustituye a la clave activa agregada anteriormente y la clave adicional no se elimina.

► *Para activar Kaspersky Embedded Systems Security 2.2:*

1. En el árbol de la Consola de la aplicación, expanda el nodo **Licencia**.
2. En el panel de detalles del nodo **Licencia**, haga clic en el vínculo **Agregar clave**.
3. En la ventana que se abre, haga clic en el botón **Examinar** y seleccione un archivo de clave con la extensión .key.

   También puede agregar una clave como un adicional. Para agregar una clave adicional, seleccione la casilla de verificación **Usar como clave adicional**.

4. Haga clic en **Aceptar**.

Se aplicará la clave seleccionada. La información sobre la clave agregada estará disponible en el nodo **Licencia**.

Visualización de información acerca de la licencia actual

Visualización de la información de la licencia

La información sobre la licencia actual se muestra en el panel de detalles del nodo **Kaspersky Embedded Systems Security** de la Consola de la aplicación. El estado de la clave puede tener los siguientes valores:

- **Verificando el estado de la clave**: Kaspersky Embedded Systems Security 2.2 está comprobando el archivo de clave agregado o código de activación aplicado y espera una respuesta sobre el estado de la clave actual.
- **Fecha de caducidad de la licencia**: Kaspersky Embedded Systems Security 2.2 se ha activado hasta la fecha y la hora especificadas. El estado de la clave se resalta en amarillo en los siguientes casos:
  - La licencia caducará en 14 días y no se ha agregado ninguna clave adicional ni código de activación.
  - La clave agregada se ha colocado en una lista negra y se bloqueará.
- **Aplicación no activada**: Kaspersky Embedded Systems Security 2.2 no se activa porque la clave no se ha agregado o el código de activación no se ha aplicado. El estado se resalta en rojo.
- **La licencia ha caducado**: Kaspersky Embedded Systems Security 2.2 no está activado porque la licencia caducó. El estado se resalta en rojo.
- **Infracción del Contrato de licencia de usuario final**: Kaspersky Embedded Systems Security 2.2 no se activa porque se han infringido los términos del Contrato de licencia de usuario final (consulte la sección “Acerca del Contrato de licencia de usuario final”, en la página 68). El estado se resalta en rojo.
- **La clave está en la lista negra**: el archivo de clave agregado se ha bloqueado y ha sido puesto en una lista negra por Kaspersky Lab, por ejemplo, si la clave ha sido utilizada por terceros para activar la aplicación ilegalmente. El estado se resalta en rojo.

Visualización de información acerca de la licencia actual

► *Para consultar la información acerca de la licencia actual,*

en el árbol de la Consola de la aplicación, expanda el nodo **Licencia**.

La información general acerca de la licencia actual se muestra en el panel de detalles del nodo **Licencia** (consulte la tabla a continuación).

Table 15. Información general acerca de la licencia en el nodo Licencia

Campo	Descripción
Código de activación	Número de código de activación. Este campo se completa si activa la aplicación con un código de activación.
Estado de activación	Información sobre el estado de la activación de la aplicación. La información en la columna Estado de activación en el panel de control del nodo Licencia puede tener los siguientes valores: • **Aplicada**: si ha activado la aplicación con un código o clave de activación. • **Activación**: si ha aplicado un código de activación para activar la aplicación, pero el proceso de activación aún no ha finalizado. El valor de estado cambia a Aplicada después de que la activación de la aplicación se ha completado y el contenido del panel de detalles del nodo se ha actualizado. • **Error de activación**: si se produjo un error en la activación de la aplicación. Puede ver la causa del error en la activación en el registro de tareas.

Campo	Descripción
Clave	El número de la clave que utilizó para activar la aplicación.
Tipo de licencia	Tipo de licencia: comercial.
Fecha de caducidad	La fecha y la hora de caducidad de la licencia asociada con una clave activa.
Estado del código de activación o estado de la clave	Estado del código de activación o estado de la clave: Activo o adicional.

► *Para consultar información detallada acerca de la licencia,*

en el nodo **Licencia**, abra el menú contextual en la cadena con los datos de la licencia que desea ampliar y seleccione **Propiedades**. En la ventana **Propiedades: <estado del código de activación o estado de la clave>** de la pestaña **General** se muestra información detallada acerca de la licencia actual, y en la pestaña **Avanzado** está disponible información sobre el cliente e información de contacto de Kaspersky Lab o el distribuidor donde compró Kaspersky Embedded Systems Security 2.2 (consulte la tabla a continuación).

Table 16. Información detallada de la licencia en la ventana Propiedades: <estado del código de activación o estado de la clave>

Campo	Descripción
Ficha General	
Clave	El número de la clave que utilizó para activar la aplicación.
Fecha de adición de clave	Fecha en la que se agregó la clave a la aplicación.
Tipo de licencia	Tipo de licencia: comercial.
Días hasta la fecha de caducidad	Cantidad de días restantes hasta la expiración de la licencia asociada con la clave activa.
Fecha de caducidad	La fecha y la hora de caducidad de la licencia asociada con una clave activa. Si activa la aplicación con una suscripción ilimitada, el valor del campo es *Ilimitada*. Si Kaspersky Embedded Systems Security 2.2 no puede determinar la fecha de caducidad de la licencia, el valor del campo se configura como *Desconocido*.
Aplicación	El nombre de la aplicación que se activó con la clave o con un código de activación agregado.
Restricción de uso de clave	Restricción en el uso de la clave (si existe alguna).
Brinda acceso a soporte técnico	Información sobre si Kaspersky Lab o uno de nuestros socios proporcionará soporte técnico a los clientes según los términos de la licencia.
Ficha Adicional	
Información sobre la licencia	Número y tipo de licencia actual.
Información de soporte	Información de contacto de Kaspersky Lab o de su socio que proporciona el Servicio de soporte técnico. Este campo puede estar vacío si no se proporciona el Servicio de soporte técnico.
Información del propietario	Información sobre el cliente de la licencia: el nombre del cliente y el nombre de la organización para la cual la licencia se adquirió.

Limitaciones funcionales tras el vencimiento de la licencia

Cuando la licencia actual expira, se aplican las siguientes limitaciones en el trabajo de los componentes funcionales:

- Todas las tareas se detienen, excepto las tareas de Protección de archivos en tiempo real, Análisis a pedido y Control de integridad de la aplicación.
- Se rechaza el inicio de todas las tareas, excepto las de Protección en tiempo real, Análisis a pedido y Control de integridad de la aplicación. Estas tareas continúan ejecutándose usando las bases de datos antivirus viejas.
- Se limita la funcionalidad de Prevención de exploits:
  - Los procesos se protegen hasta que se reinician.
  - Los procesos nuevos no se pueden agregar al alcance de la protección.

Otras funciones (almacenamiento, registros, información de diagnóstico) seguirán estando disponibles.

Renovación de la licencia

De forma predeterminada, cuando la licencia tiene 14 días restantes antes de su expiración, Kaspersky Embedded Systems Security 2.2 se lo notifica. En este caso, el estado **Fecha de caducidad de la licencia** en el panel de detalles del nodo **Kaspersky Embedded Systems Security** se resalta en amarillo.

Puede renovar la fecha de caducidad de la licencia antes de que finalice con una clave adicional o un código de activación. Esto garantiza que el servidor permanezca protegido después de la expiración de la licencia existente y antes de que active la aplicación con una licencia nueva.

► *Para renovar una licencia, siga estos pasos:*

1. Compre un nuevo código de activación o un archivo de clave.
2. En el árbol de la Consola de la aplicación, abra el nodo **Licencia**.
3. En el panel de detalles del nodo **Licencia**, realice una de las siguientes acciones:
   - Si desea renovar una licencia con una clave adicional:
     a. Haga clic en el vínculo **Agregar clave**.
     b. En la ventana que se abre, haga clic en el botón **Examinar** y seleccione un nuevo archivo de clave con la extensión .key.
     c. Seleccione la casilla de verificación **Usar como clave adicional**.
   - Si desea renovar una licencia con un código de activación:
     a. Haga clic en el vínculo **Agregar código de activación**.
     b. Escriba el código de activación comprado en la ventana que se abre.
     c. Seleccione la casilla de verificación **Usar como clave adicional**.

   Se requiere una conexión a Internet para aplicar el código de activación.
4. Haga clic en **Aceptar**.

   La clave adicional o el código de activación se agregarán y se aplicarán automáticamente cuando expire la licencia actual de Kaspersky Embedded Systems Security 2.2.

Eliminación de la clave

Se puede eliminar la clave agregada.

Si se ha agregado una clave adicional a Kaspersky Embedded Systems Security 2.2 y la clave activa se elimina, la clave adicional se convierte automáticamente en la clave activa.

Si se elimina una clave adicional, se puede restaurar volviendo a aplicar el archivo de clave.

► *Para eliminar una clave que se ha agregado:*

1. En el árbol de la Consola de la aplicación, seleccione el nodo **Licencia**.
2. En el panel de detalles del nodo **Licencia**, en la tabla que contiene información sobre claves agregadas, seleccione la clave que desea eliminar.
3. En el menú contextual de la línea que contiene información sobre la clave seleccionada, seleccione **Eliminar**.
4. Haga clic en el botón **Sí** de la ventana de confirmación para confirmar que desea eliminar la clave.

Se eliminará la clave seleccionada.

Inicio y detención del complemento de Kaspersky Embedded Systems Security 2.2

Esta sección contiene información sobre cómo iniciar y detener el Complemento de administración de Kaspersky Embedded Systems Security 2.2 y el servicio de Kaspersky Security.

En este capítulo

Inicio del complemento de administración de Kaspersky Embedded Systems Security 2.2

No se requiere ninguna acción avanzada para iniciar el complemento de administración de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center. Después de que el complemento se instala en el equipo del administrador, se inicia simultáneamente con Kaspersky Security Center. La información detallada sobre Kaspersky Security Center inicial se puede encontrar en la *Ayuda de Kaspersky Security Center*.

Inicio y detención del servicio de Kaspersky Security

De forma predeterminada, el servicio de Kaspersky Security se inicia automáticamente cuando se inicia el sistema operativo. El servicio de Kaspersky Security administra procesos de trabajo en los que se ejecutan tareas de actualización, Protección del equipo en tiempo real, Control de actividad local y Análisis a pedido.

De forma predeterminada, cuando se inicia el servicio de Kaspersky Embedded Systems Security 2.2, se inician las tareas de Protección de archivos en tiempo real y Análisis al inicio del sistema operativo, así como otras tareas que están programadas para iniciarse **Al inicio de la aplicación**.

Si se detiene el servicio de Kaspersky Security, todas las tareas en ejecución se detienen. Después de reiniciar el servicio de Kaspersky Security, la aplicación inicia automáticamente solo aquellas tareas cuya programación tienen la frecuencia de inicio configurada en **Al inicio de la aplicación**, mientras que las otras tareas se deben iniciar manualmente.

Puede iniciar y detener el servicio de Kaspersky Security con el menú contextual del nodo **Kaspersky Embedded Systems Security** o con el complemento **Servicios** de Microsoft Windows.

Puede iniciar y detener la aplicación si es miembro del grupo Administradores en el equipo protegido.

► *Para detener o iniciar la aplicación con la Consola de la aplicación, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nodo **Kaspersky Embedded Systems Security**.
2. Seleccione uno de los siguientes elementos:
   - **Detener el servicio**
   - **Iniciar el servicio**

El servicio de Kaspersky Security se iniciará o se detendrá.

Permisos de acceso para las funciones de Kaspersky Embedded Systems Security 2.2

Esta sección contiene información acerca de los permisos para administrar Kaspersky Embedded Systems Security 2.2 y los servicios de Windows registrados por la aplicación, e instrucciones sobre cómo configurar estos permisos.

En este capítulo

Acerca de los permisos para administrar Kaspersky Embedded Systems Security 2.2

De forma predeterminada, se otorga acceso a todas las funciones de Kaspersky Embedded Systems Security 2.2 a usuarios del grupo Administradores en el equipo protegido, los usuarios del grupo Administradores ESS creado en el equipo protegido durante la instalación de Kaspersky Embedded Systems Security 2.2, además del grupo SYSTEM.

Los usuarios que tienen acceso a la función **Editar permisos** de Kaspersky Embedded Systems Security 2.2 pueden otorgar acceso a las funciones de Kaspersky Embedded Systems Security 2.2 a otros usuarios registrados en el equipo protegido o incluidos en el dominio.

Los usuarios que no están registrados en la lista de usuarios de Kaspersky Embedded Systems Security 2.2 no pueden abrir la Consola de la aplicación.

Puede elegir uno de los siguientes niveles preestablecidos de permisos de acceso de Kaspersky Embedded Systems Security 2.2 para un usuario o un grupo de usuarios:

- **Control total**: acceso a todas las funciones de la aplicación: capacidad de ver y modificar la configuración general de Kaspersky Embedded Systems Security 2.2, la configuración de los componentes y los permisos de usuarios de Kaspersky Embedded Systems Security 2.2, y de ver estadísticas de Kaspersky Embedded Systems Security 2.2.
- **Editar**: acceso a todas las funciones de la aplicación, excepto la edición de permisos del usuario: capacidad para ver y editar la configuración general de Kaspersky Embedded Systems Security 2.2 y los parámetros de sus componentes.
- **Lectura**: capacidad de ver la configuración general de Kaspersky Embedded Systems Security 2.2, la configuración de los componentes de Kaspersky Embedded Systems Security 2.2, las estadísticas de Kaspersky Embedded Systems Security 2.2 y los permisos de usuario de Kaspersky Embedded Systems Security 2.2.

También puede configurar permisos de acceso avanzados (consulte la sección “Configuración de permisos de acceso para Kaspersky Embedded Systems Security 2.2 y el servicio de Kaspersky Security”, en la página 83): autorice o bloquee el acceso a funciones específicas de Kaspersky Embedded Systems Security 2.2.

Si ha configurado manualmente permisos de acceso para un usuario o grupo, el nivel de acceso **Permisos especiales** se configura para este usuario o grupo.

Table 17. Acerca de los permisos de acceso para las funciones de Kaspersky Embedded Systems Security 2.2

Derechos del usuario	Descripción
Administración de tareas	Capacidad para iniciar/detener/pausar/reanudar tareas de Kaspersky Embedded Systems Security 2.2.
Creación y eliminación de tareas de Análisis a pedido	Capacidad para crear y eliminar tareas de Análisis a pedido.
Editar la configuración	Capacidad para: • Importar ajustes de Kaspersky Embedded Systems Security 2.2 desde un archivo de configuración. • Editar la configuración de la aplicación.
Leer configuración	Capacidad para: • Ver la configuración general y la configuración de tareas de Kaspersky Embedded Systems Security 2.2. • Exportar la configuración de Kaspersky Embedded Systems Security 2.2 al archivo de configuración. • Ver la configuración de los registros de tareas, del registro de auditoría del sistema y las notificaciones.
Administrar depósitos	Capacidad para: • Mover objetos a Cuarentena. • Eliminar objetos de la Cuarentena y de la Copia de seguridad. • Restaurar objetos de la Cuarentena y de la Copia de seguridad.
Administrar registros	Capacidad para eliminar registros de tareas y borrar el registro de auditoría del sistema.
Leer registros	Capacidad para ver eventos del antivirus en los registros de tareas y el registro de auditoría del sistema.
Leer estadísticas	Capacidad para ver estadísticas de cada tarea de Kaspersky Embedded Systems Security 2.2.
Licencia de la aplicación	Kaspersky Embedded Systems Security 2.2 se puede activar o desactivar.
Desinstalar la aplicación	Capacidad para desinstalar Kaspersky Embedded Systems Security 2.2.
Permisos de lectura	Capacidad para ver la lista de usuarios de Kaspersky Embedded Systems Security 2.2 y acceder a los privilegios de cada usuario.
Editar permisos	Capacidad para: • Modificar la lista de usuarios con acceso a la administración de la aplicación. • Modificar los permisos de acceso a las funciones de Kaspersky Embedded Systems Security 2.2.

Acerca de los permisos para administrar el servicio de Kaspersky Security

Durante la instalación, Kaspersky Embedded Systems Security 2.2 registra el servicio de Kaspersky Security (KAVFS) en Windows, e internamente habilita componentes funcionales que se inician cuando se inicia el sistema operativo. Para reducir el riesgo de que un tercero acceda a las funciones de la aplicación y la configuración de seguridad en el equipo protegido a través de la administración del servicio de Kaspersky Security, puede restringir los permisos de administración del servicio de Kaspersky Security desde la Consola de la aplicación o el complemento de administración.

De forma predeterminada, los permisos de acceso para administrar el servicio de Kaspersky Security se conceden a los usuarios del grupo "Administradores" en el equipo protegido, así como a los grupos de SERVICE e INTERACTIVE con permisos de lectura y al grupo SYSTEM con permisos de lectura y ejecución.

No se puede eliminar la cuenta de usuario de SYSTEM ni modificar los permisos para esta cuenta. Si los permisos de la cuenta de usuario de SYSTEM se modificaron, los privilegios máximos se restaurarán para esta cuenta cuando guarde los cambios.

Los usuarios que tienen acceso a funciones (consulte la sección “Acerca de los permisos para administrar Kaspersky Embedded Systems Security 2.2”, en la página 79) del nivel de permiso de edición pueden otorgar permisos de acceso para administrar el servicio de Kaspersky Security a otros usuarios registrados en el equipo protegido o incluido en el dominio.

Puede elegir uno de los siguientes niveles predeterminados de permisos de acceso para un usuario o grupo de usuarios de Kaspersky Embedded Systems Security 2.2 para administrar el servicio de Kaspersky Security:

- **Control total**: capacidad de ver y modificar la configuración general y los permisos de usuario para el servicio de Kaspersky Security, e iniciar y detener el servicio de Kaspersky Security.
- **Lectura**: capacidad de ver la configuración general y los permisos de usuario del servicio de Kaspersky Security.
- **Modificación**: capacidad de ver y modificar la configuración general y los permisos de usuario del servicio de Kaspersky Security.
- **Ejecución**: capacidad de iniciar y detener el servicio de Kaspersky Security.

También puede configurar los permisos del acceso avanzado: autorice o deniegue el acceso a funciones específicas de Kaspersky Embedded Systems Security 2.2 (consulte la tabla a continuación).

Si ha configurado manualmente permisos de acceso para un usuario o grupo, el nivel de acceso **Permisos especiales** se configura para este usuario o grupo.

Table 18. Delimitación de permisos de acceso para funciones de Kaspersky Embedded Systems Security 2.2

Función	Descripción
Visualización de configuraciones del servicio	Visualización: capacidad de ver las configuraciones generales y los permisos de usuario del servicio de Kaspersky Security.
Solicitar estado del servicio al Administrador de servicios	Capacidad para solicitar el estado de ejecución del servicio de Kaspersky Security desde el Administrador de control de servicios de Microsoft Windows.

Función	Descripción
Solicitar estado al servicio	Capacidad para solicitar el estado de ejecución del servicio desde el servicio de Kaspersky Security.
Enumerar servicios dependientes	Capacidad para ver una lista de servicios de los cuales depende el servicio de Kaspersky Security y que dependen del servicio de Kaspersky Security.
Modificación de la configuración del servicio	Capacidad de ver y modificar la configuración general y los permisos del usuario del servicio de Kaspersky Security.
Iniciar el servicio	Capacidad para iniciar el servicio de Kaspersky Security.
Detener el servicio	Capacidad para detener el servicio de Kaspersky Security.
Pausar/reanudar el servicio	Capacidad para pausar y reanudar el servicio de Kaspersky Security.
Permisos de lectura	Capacidad para ver la lista de usuarios del servicio de Kaspersky Security y los privilegios de acceso de cada usuario.
Editar permisos	Capacidad para: • Agregar y eliminar usuarios del servicio de Kaspersky Security • Modificar los permisos de acceso de usuarios para el servicio de Kaspersky Security
Eliminar el servicio	Capacidad para eliminar el registro del servicio de Kaspersky Security en el Administrador de control de servicios de Microsoft Windows.
Solicitudes de usuario al servicio	Capacidad para crear y enviar solicitudes de usuario al servicio de Kaspersky Security.

Registro del servicio de Kaspersky Security como servicio protegido

La tecnología *Luz de proceso protegido* (también denominada “PPL”) garantiza que el sistema operativo solo cargue servicios y procesos de confianza. Para que un servicio se ejecute como servicio protegido, debe instalarse un controlador de *antimalware de ejecución temprana* en el equipo protegido.

Un controlador de *antimalware de ejecución temprana* (también denominado “ELAM”) ofrece protección para los equipos en la red cuando se inician, antes de que se inicien los controladores de terceros.

El controlador ELAM se instala automáticamente durante la instalación de Kaspersky Embedded Systems Security 2.2 y se utiliza para registrar el servicio de Kaspersky Security como PPL cuando se inicia el sistema operativo. Cuando el servicio de Kaspersky Security (kavfs.exe) se inicia como proceso protegido del sistema, otros procesos no protegidos en el sistema no pueden inyectar subprocesos, escribir en la memoria virtual del proceso protegido ni detener el servicio.

Cuando un proceso se inicia como un PPL, no puede ser administrado por un usuario ignorando los permisos del usuario asignados. El registro del servicio de Kaspersky Security como PPL usando el controlador ELAM se admite en sistemas operativos Microsoft Windows 10 y superiores. Si instala Kaspersky Embedded Systems Security 2.2 en un equipo que ejecuta un sistema operativo compatible con PPL, no estará disponible la administración de permisos para el servicio de Kaspersky Security (KAVFS).

El servicio de Kaspersky Security inicia todos los procesos secundarios como PPL.

► *Para instalar Kaspersky Embedded Systems Security 2.2 como PPL, ejecute el siguiente comando:*

```
msiexec /i ks4ws_x64.msi NOPPL=0 EULA=1 PRIVACYPOLICY=1 /qn
```

Puede usar la línea de comandos para configurar el uso del PPL.

Acerca de los permisos de acceso para el servicio de Kaspersky Security Management

Puede revisar la lista de servicios de Kaspersky Embedded Systems Security 2.2.

Durante la instalación, Kaspersky Embedded Systems Security 2.2, registre el servicio de Kaspersky Security Management (KAVFSGT). Para administrar la aplicación mediante la Consola de la aplicación instalada en otro equipo, la cuenta con los permisos para conectarse a Kaspersky Embedded Systems Security 2.2 debe tener acceso absoluto al servicio de Kaspersky Security Management en el equipo protegido.

De forma predeterminada, se les concede acceso al servicio de Kaspersky Security Management a los usuarios del grupo de administración del equipo protegido y a los usuarios del grupo de administración de ESS que se haya creado en el equipo protegido durante la instalación de Kaspersky Embedded Systems Security 2.2.

Puede administrar el servicio de Kaspersky Security Management solo mediante el complemento **Servicios** de Microsoft Windows.

No puede autorizar o bloquear el acceso de los usuarios al servicio de Kaspersky Security Management con Kaspersky Embedded Systems Security 2.2.

Puede conectarse a Kaspersky Embedded Systems Security 2.2 desde una cuenta local si se registró una cuenta con el mismo nombre y contraseña en el equipo protegido.

Configuración de los permisos de acceso para Kaspersky Embedded Systems Security 2.2 y el servicio de Kaspersky Security

Puede modificar la lista de usuarios y los grupos de usuarios autorizados para acceder a funciones de Kaspersky Embedded Systems Security y 2.2 administrar el servicio de Kaspersky Security, y modificar los permisos de acceso de dichos usuarios y grupos de usuarios.

► *Para agregar o quitar un usuario o un grupo de la lista:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

> Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Adicional**, siga uno de estos pasos:
   - Seleccione **Permisos de acceso de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar funciones de Kaspersky Embedded Systems Security 2.2.
   - Seleccione **Permiso de acceso del usuario para la administración del servicio de Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar el servicio de Kaspersky Security.

     Se abre la ventana **Permisos para el grupo de Kaspersky Embedded Systems Security 2.2**.
4. En la ventana que se abre, realice las siguientes operaciones:
   - Para agregar un usuario o un grupo a la lista, haga clic en el botón **Agregar** y seleccione el usuario o el grupo a quien desea otorgar privilegios.
   - Para eliminar un usuario o un grupo de la lista, seleccione el usuario o el grupo cuyo acceso desea restringir y haga clic en el botón **Eliminar**.
5. Haga clic en el botón **Aplicar**.

Los usuarios seleccionados (grupos) se agregan o se eliminan.

► *Para modificar permisos de un usuario o un grupo para la administración de Kaspersky Embedded Systems Security 2.2 o el servicio de Kaspersky Security:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

   > Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Adicional**, siga uno de estos pasos:
   - Seleccione **Modificar los derechos de usuario para administrar la aplicación** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar Kaspersky Embedded Systems Security 2.2.
   - Seleccione **Modificar los derechos de usuario de administración del servicio de Kaspersky Security** si desea modificar la lista de usuarios que tienen permiso de acceso para administrar la aplicación mediante el servicio de Kaspersky Security.

Se abre la ventana del grupo **Permisos para Kaspersky Embedded Systems Security**.

4. En la ventana que se abre, en la lista **Grupos** o usuarios, seleccione un usuario o un grupo de usuarios para quienes desea cambiar los permisos.
5. En la sección **Permisos para el grupo "<Usuario (Grupo)>"**, seleccione las casillas de verificación **Autorizar** o **Bloquear** para los siguientes niveles de acceso:
   - **Control total**: conjunto completo de permisos para administrar Kaspersky Embedded Systems Security 2.2 o el servicio de Kaspersky Security.
   - **Lectura**:
     - Los siguientes permisos para administrar Kaspersky Embedded Systems Security 2.2: **Recuperar estadísticas**, **Leer configuración**, **Leer registros** y **Permisos de lectura**.
     - Los siguientes permisos para administrar el servicio de Kaspersky Security: **Leer configuración del servicio**, **Solicitar estado del servicio al Administrador de control de servicios**, **Solicitar estado al servicio**, **Leer lista de servicios dependientes**, **Permisos de lectura**.
   - **Modificación**:
     - Todos los permisos para administrar Kaspersky Embedded Systems Security 2.2, excepto **Editar permisos**.
     - Los siguientes permisos para administrar el servicio de Kaspersky Security: **Modificar configuración del servicio**, **Permisos de lectura**.
   - **Ejecución**: los permisos siguientes para administrar el servicio de Kaspersky Security: **Iniciando el servicio**, **Deteniendo del servicio**, **Pausar o reanudar el servicio**, **Permisos de lectura**, **Solicitudes de usuario al servicio**.
6. Para establecer la configuración adicional de permisos para un usuario o grupo (**Permisos especiales**), haga clic en el botón **Avanzado**.
   a. En la ventana **Configuración de la seguridad avanzada para Kaspersky Embedded Systems Security 2.2** que se abre, seleccione el usuario o el grupo que necesita.
   b. Haga clic en el botón **Editar**.
   c. En la lista desplegable ubicada en la parte superior de la ventana, seleccione el tipo de control de acceso (**Autorizar** o **Bloquear**).
   d. Seleccione las casillas de verificación frente a las funciones que desea autorizar o bloquear para el usuario o el grupo seleccionado.
   e. Haga clic en **Aceptar**.
   f. En la ventana **Configuración de seguridad avanzada para Kaspersky Embedded Systems Security 2.2**, haga clic en **Aceptar**.
7. En la ventana de grupo **Permisos para Kaspersky Embedded Systems Security**, haga clic en el botón **Aplicar**.

Se guardarán los permisos configurados para administrar Kaspersky Embedded Systems Security 2.2 o el servicio de Kaspersky Security.

Acceso protegido por contraseña a funciones de Kaspersky Embedded Systems Security 2.2

Puede restringir el acceso a la administración de la aplicación y a los servicios registrados mediante la configuración de permisos del usuario (consulte la sección “Permisos de acceso para las funciones de Kaspersky Embedded Systems Security 2.2" en la página 78). También puede establecer la protección con contraseña en Kaspersky Embedded Systems Security 2.2 para una protección adicional de la ejecución de operaciones críticas.

Kaspersky Embedded Systems Security 2.2 solicita una contraseña cuando intenta acceder a las siguientes funciones de la aplicación:

- conexión con la Consola de la aplicación;
- desinstalación de Kaspersky Embedded Systems Security 2.2;
- modificación de componentes de Kaspersky Embedded Systems Security 2.2;
- ejecución de los comandos de la línea de comandos.

La interfaz de Kaspersky Embedded Systems Security 2.2 oculta la contraseña especificada en pantalla. Kaspersky Embedded Systems Security 2.2 almacena la contraseña como una suma de control calculada cuando se especifica la contraseña.

Puede exportar e importar una configuración de aplicación protegida por contraseña. El archivo de configuración, creado como resultado de la exportación de la configuración de la aplicación protegida, contiene la suma de control de la contraseña y el valor del modificador utilizado para rellenar la cadena de esta.

No cambie la suma de control o el modificador en el archivo de configuración. La importación de una configuración protegida con contraseña que ha sido modificada manualmente puede causar que se bloquee completamente el acceso a la aplicación.

► *Para proteger el acceso a las funciones de Kaspersky Embedded Systems Security 2.2, siga estos pasos:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**. Expanda el grupo de administración con los equipos donde se incluyen los equipos cuya configuración de la aplicación desea establecer.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para ajustar la configuración de directivas para un grupo de equipos, seleccione la pestaña **Directivas** y abra **<Nombre de la directiva> > Propiedades**.
   - Si desea establecer la configuración de la aplicación para un solo equipo, abra las opciones requeridas en la ventana **Configuración de la aplicación** (consulte la sección “**Configuración de tareas locales en la ventana Configuración de la aplicación en Kaspersky Security Center**”, en la página 103) en Kaspersky Security Center.
3. En la sección **Seguridad**, haga clic en el botón **Configurar**.

   Se abre la ventana **Configuración de seguridad**.
4. En la sección **Configuración de protección con contraseña**, seleccione la casilla de verificación **Aplicar protección con contraseña**.

   Los campos **Contraseña** y **Confirmar contraseña** se activan.

5. En el campo **Contraseña**, escriba el valor que desea usar para proteger el acceso a las funciones de Kaspersky Embedded Systems Security 2.2.
6. En el campo **Confirmar contraseña**, escriba su contraseña nuevamente.
7. Haga clic en **Aceptar**.

Se guarda la configuración especificada. Kaspersky Embedded Systems Security 2.2 solicitará la contraseña especificada para acceder a las funciones protegidas.

Esta contraseña no se puede recuperar. Si pierde su contraseña pierde completamente el control de la aplicación. Además, será imposible desinstalar la aplicación del equipo protegido.

Puede cambiar o reiniciar la contraseña especificada en la configuración de la aplicación en cualquier momento.

► *Para reiniciar la contraseña,*

desactive la casilla **Aplicar protección con contraseña** en la configuración de la directiva o la aplicación.

La protección con contraseña se deshabilitará. Kaspersky Embedded Systems Security 2.2 elimina la suma de control antigua de la contraseña de la configuración de la aplicación.

Cómo habilitar las conexiones de red para el servicio de Kaspersky Security Management

Los nombres de configuración pueden variar en los diferentes sistemas operativos Windows.

► *Para permitir las conexiones de red para el servicio de Kaspersky Security Management en un equipo protegido, siga estos pasos:*

1. En el equipo protegido que ejecuta Microsoft Windows, seleccione **Inicio > Panel de control > Seguridad > Firewall de Windows**.
2. En la ventana **Configuración de Firewall de Windows**, seleccione **Cambiar configuración**.
3. En la lista de exclusiones predefinidas de la pestaña **Exclusiones**, seleccione las siguientes casillas de verificación: **COM + Acceso de red**, **Instrumentación de administración de Windows (WMI)** y **Administración remota**.
4. Haga clic en el botón **Agregar programa**.
5. Seleccione el archivo kavfsgt.exe de la ventana **Agregar programa**. Este archivo se almacena en la carpeta que especificó como carpeta de destino durante la instalación de la Consola de la aplicación.
6. Haga clic en **Aceptar**.
7. Haga clic en **Aceptar** en la ventana **Configuración de firewall de Windows**.

Se permitirán las conexiones de red para el servicio de Kaspersky Security Management en el equipo protegido.

Creación y configuración de directivas

Esta sección proporciona información sobre la utilización de directivas de Kaspersky Security Center para administrar Kaspersky Embedded Systems Security 2.2 en varios equipos.

En este capítulo

Acerca de las directivas

Pueden crearse directivas globales de Kaspersky Security Center para administrar la protección de varios equipos en los que está instalado Kaspersky Embedded Systems Security 2.2.

Una directiva implementa la configuración, las funciones y tareas de Kaspersky Embedded Systems Security 2.2 especificadas en la misma en todos los equipos protegidos para un grupo de administración.

Se pueden crear e implementar por turnos varias directivas para un grupo de administración. En la Consola de administración, la directiva activa actualmente para un grupo tiene el estado *activa*.

La información sobre la implementación de la directiva se carga en el registro de auditoría del sistema de Kaspersky Embedded Systems Security 2.2. Esta información se puede visualizar en la Consola de la aplicación, en el nodo **Registro de auditoría del sistema**.

Kaspersky Security Center ofrece una manera de aplicar directivas en equipos locales: *Prohibir cambiar la configuración*. Después de aplicar una directiva, Kaspersky Embedded Systems Security 2.2 utiliza los valores de configuración al lado de los cuales ha seleccionado el icono en las propiedades de la directiva en equipos locales, en lugar de los valores de configuración previos a la aplicación de la directiva. Kaspersky Embedded Systems Security 2.2 no aplica los valores de configuración de la directiva activa al lado de los cuales ha seleccionado el icono en las propiedades de la directiva.

Si una directiva está activa, los valores de configuración marcados con el icono en la directiva se muestran en la Consola de la aplicación, pero no se pueden modificar. Los valores de otras opciones de configuración (marcados con el icono en la directiva) pueden modificarse en la Consola de la aplicación.

La configuración establecida en la directiva activa y marcada con el icono también bloquea los cambios en Kaspersky Security Center para un equipo en la ventana **Propiedades: <Nombre del equipo>**.

La configuración que se especifica y se envía al equipo local usando una directiva activa se guarda en la configuración de las tareas locales después de que se deshabilita la directiva activa.

Si la directiva define la configuración para una tarea de Protección en tiempo real, y si dicha tarea está en ejecución en ese momento, la configuración definida por la directiva se modificará en cuanto se aplique la directiva. Si la tarea no está en ejecución, la configuración se implementará cuando se inicie.

Creación de una directiva

El proceso de creación de una directiva implica los siguientes pasos:

1. Crear una directiva mediante el asistente para creación de directivas. Las tareas de configuración de la Protección del equipo en tiempo real pueden establecerse mediante los cuadros de diálogo del asistente.
2. Establecer la configuración de la directiva. En la ventana **Propiedades: <Nombre de la directiva>** de la directiva creada, puede definir las tareas de configuración de la Protección del equipo en tiempo real, la configuración general de Kaspersky Embedded Systems Security 2.2, la configuración de la Cuarentena y la Copia de seguridad, el nivel de detalle para los registros de tareas y las notificaciones de administrador y de usuario sobre eventos de Kaspersky Embedded Systems Security 2.2.

► *Para crear una directiva para un grupo de equipos que ejecutan la aplicación instalada de Kaspersky Embedded Systems Security 2,2, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la consola de administración de Kaspersky Security Center y, a continuación, seleccione el grupo de administración que contiene los equipos para los que desea crear una directiva.
2. En el panel de detalles del grupo de administración seleccionado, seleccione la pestaña **Directivas** y haga clic en el vínculo **Crear una directiva** para iniciar el asistente y crear una directiva.

   Se abre la ventana **Nuevo asistente de directiva**.
3. En la ventana **Seleccionar la aplicación para la cual desea crear una directiva de grupo**, seleccione Kaspersky Embedded Systems Security 2.2 y haga clic en **Siguiente**.
4. Ingrese un **Nombre de la directiva de grupo** en el campo **Nombre**.

   El nombre de la directiva no puede contener los siguientes símbolos: " * < : > ? \ | .
5. Para aplicar la configuración de la directiva usada para la versión anterior de la aplicación:
   a. Seleccione la casilla de verificación **Usar configuración de la directiva para versiones anteriores de la aplicación**.
   b. Haga clic en el botón **Examinar** y seleccione la directiva que desea aplicar.
   c. Haga clic en **Siguiente**.
6. En la ventana **Selección del tipo de operación**, seleccione una de las opciones siguientes:
   - **Nueva**, para crear una directiva nueva con las opciones predeterminadas.
   - **Importar directiva creada con versiones anteriores de Kaspersky Embedded Systems Security**, para usar la directiva de esa versión como plantilla.
   - Haga clic en **Examinar** y seleccione un archivo de configuración donde esté almacenada una directiva existente.
7. En la ventana **Protección del equipo en tiempo real**, configure la Protección de archivos en tiempo real, las tareas de Uso de KSN y la funcionalidad de Prevención de exploits como se requiere. Autorice o bloquee el uso de tareas de directivas configuradas en equipos locales en la red:
   - Haga clic en el botón 🔒 para autorizar cambios en la configuración de tareas en equipos en red y bloquear la aplicación de la configuración de tareas establecida en la directiva.
   - Haga clic en el botón 🔓 para denegar cambios en la configuración de tareas en equipos en red y

autorizar la aplicación de la configuración de tareas establecida en la directiva.

La directiva creada recientemente usa las configuraciones predeterminadas de las tareas de Protección del equipo en tiempo real.

- Para modificar la configuración predeterminada de la tarea de Protección de archivos en tiempo real, haga clic en el botón **Configurar** en la sección **Protección de archivos en tiempo real**. En la ventana que se abre, configure los privilegios de acceso según sus necesidades. Haga clic en **Aceptar**.
- Para modificar la configuración predeterminada de la tarea de Uso de KSN, haga clic en el botón **Configurar** en la sección **Uso de KSN**. En la ventana que se abre, configure los privilegios de acceso según sus necesidades. Haga clic en **Aceptar**.

  Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de KSN en la ventana Manejo de datos (consulte la sección “Configuración del procesamiento de datos”, en la página 168).

- Para modificar la configuración predeterminada del componente Prevención de exploits, haga clic en el botón **Configurar** en la sección **Prevención de exploits**. En la ventana que se abre, configure la funcionalidad según sus necesidades. Haga clic en **Aceptar**.

8. Seleccione uno de los siguientes estados de la directiva en la ventana **Crear la directiva de grupo para la aplicación**:
   - **Directiva activa**, si desea aplicar la directiva inmediatamente después de su creación. Si ya existe una directiva activa en el grupo, se desactiva y se aplica una directiva nueva.
   - **Directiva inactiva**, si no desea aplicar la directiva creada inmediatamente. En este caso, la directiva se puede activar más tarde.
   - Seleccione la casilla de verificación **Abrir propiedades de la directiva inmediatamente después de su creación** para cerrar automáticamente el **Asistente de nueva directiva** y configurar la directiva recién creada después de hacer clic en el botón **Siguiente**.
9. Haga clic en el botón **Finalizar** en la ventana del asistente **Completar el asistente**.

La directiva creada se mostrará en la lista de directivas de la pestaña **Directivas** del grupo de administración seleccionado. En la ventana **Propiedades: <Nombre de la directiva>**, puede establecer otra configuración, tareas y funciones de Kaspersky Embedded Systems Security 2.2.

Configuración de directivas

En la ventana **Propiedades: <Nombre de la directiva>** de una directiva existente, puede establecer la configuración general de Kaspersky Embedded Systems Security 2.2, la configuración de la cuarentena y las copias de seguridad, la configuración de la Zona de confianza, la configuración de la Protección en tiempo real, la configuración del control de actividad local, el nivel de detalle para los registros de tareas y las notificaciones de administrador y de usuario sobre eventos de Kaspersky Embedded Systems Security 2.2, los privilegios de acceso para administrar la aplicación y el servicio de Kaspersky Security, y la configuración de la aplicación del perfil de la directiva.

► *Para establecer la configuración de la directiva:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center.
2. Expanda el grupo de administración, para el cual desea configurar las opciones de la directiva asociada y abra el nodo secundario **Directivas** en el panel de detalles.
3. Seleccione la directiva que desea configurar y abra la ventana **Propiedades: <Nombre de la directiva>**

con uno de los siguientes métodos:

- Seleccionando la opción **Propiedades** en el menú contextual de la directiva.
- Haciendo clic en el vínculo **Configurar directiva** en el panel de detalles de la directiva seleccionada.
- Haciendo doble clic en la directiva seleccionada.

4. En la pestaña **General** en la sección **Estado de la directiva**, habilite o deshabilite la directiva. Para esto, seleccione una de las siguientes opciones:
   - **Directiva activa**, si desea que la directiva se aplique en todos los equipos dentro del grupo de administración seleccionado.
   - **Directiva inactiva**, si no desea que la directiva se aplique en todos los equipos dentro del grupo seleccionado.

   El parámetro **Directiva fuera de oficina** no está disponible cuando se administra Kaspersky Embedded Systems Security 2.2.
5. En las secciones **Notificación del evento**, **Configuración de la aplicación**, **Registros y notificaciones**, **Adicional** e **Historial de revisiones**, puede modificar la configuración de la aplicación (consulte la tabla a continuación).
6. En las secciones **Protección del equipo en tiempo real**, **Control de actividad local**, **Control de actividad de red** e **Inspección del sistema**, configure los parámetros de la aplicación y del inicio de la aplicación (consulte la tabla a continuación).

   Puede habilitar o deshabilitar la ejecución de cualquier tarea en todos los equipos dentro del grupo de administración mediante una directiva de Kaspersky Security Center.

   Puede configurar la aplicación de la configuración de la directiva en todos los equipos en red para cada componente de la aplicación particular.
7. Haga clic en **Aceptar**.

La configuración establecida se aplica en la directiva.

Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones a través de la Consola de la aplicación en las secciones correspondientes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

Secciones con configuraciones de directivas de Kaspersky Embedded Systems Security 2.2

General

En la sección **General**, puede configurar las siguientes opciones de la directiva:

- Especificar el estado de la directiva
- Configurar la herencia de las opciones de las directivas principales y las directivas secundarias.

Notificaciones de eventos

En la sección **Notificaciones de eventos**, puede configurar las opciones de las siguientes categorías de eventos:

- *Eventos críticos*
- *Omisión*
- *Advertencia*
- *Evento informativo*

Puede usar el botón **Propiedades** para configurar las siguientes opciones de los eventos seleccionados:

- Indicar la ubicación de almacenamiento y el periodo de retención de la información sobre los eventos registrados.
- Indicar el método de notificación de los eventos registrados.

Configuración de la aplicación

Table 19. Configuración de la sección Configuración de la aplicación

Sección	Opciones
Escalabilidad e interfaz	En la sección **Escalabilidad e interfaz**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones: • Elija si desea ajustar la configuración de la escalabilidad automáticamente o manualmente. • Establecer la configuración de la visualización del icono de la aplicación
Seguridad	En la sección **Seguridad y fiabilidad**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones: • Establecer la configuración de ejecución de tareas • Especificar cómo debería comportarse la aplicación cuando el equipo se está ejecutando con energía de UPS • Habilitar o deshabilitar la protección con contraseña de funciones de la aplicación.
Conexiones	En la sección **Conexiones**, puede usar el botón **Configurar** para configurar las siguientes opciones del servidor proxy para la conexión a KSN y a los servidores de actualizaciones y activación: • Configurar las opciones del servidor proxy • Especificar la configuración de autenticación del servidor proxy
Ejecutar tareas del sistema	En la subsección **Ejecutar tareas del sistema**, puede usar el botón **Configurar** para autorizar o bloquear el inicio de las siguientes tareas del sistema según la programación configurada en los equipos locales: • Tarea Análisis a pedido. • Tareas Actualización y Copia de actualizaciones.

Adicional

Table 20. Configuración de la sección Adicional

Sección	Opciones
Zona de confianza	Haga clic en el botón **Configurar** en la sección **Zona de confianza** para configurar las siguientes opciones de la aplicación de la Zona de confianza: • Crear una lista de exclusiones de la Zona de confianza. • Habilitar o deshabilitar el análisis de las operaciones de copia de seguridad del archivo. • Crear una lista de procesos de confianza.

Sección	Opciones
Análisis de unidades extraíbles	Haga clic en el botón **Configurar** para configurar las opciones de análisis para discos USB extraíbles.
Permisos del acceso del usuario para la administración de aplicaciones	En esta sección, puede configurar los derechos del usuario y los derechos del grupo de usuarios para administrar Kaspersky Embedded Systems Security 2.2.
Permiso de acceso del usuario para la administración del servicio de Security	En esta sección, puede configurar derechos de usuarios y derechos de grupos de usuarios para administrar el servicio de Kaspersky Security.
Depósitos	En la sección **Depósitos**, haga clic en el botón **Configurar** para configurar las siguientes opciones de Cuarentena y Copia de seguridad: • Especificar la ruta de la carpeta en la cual desea colocar objetos en Cuarentena o Copia de seguridad. • Configurar el tamaño máximo de Copia de seguridad y Cuarentena y especificar el umbral de espacio disponible. • Especificar la ruta de la carpeta en la cual desea colocar objetos restaurados de la Cuarentena o la Copia de seguridad. • Configurar la transmisión de información sobre los objetos en Cuarentena y Copia de seguridad al Servidor de administración.

Protección del equipo en tiempo real

Table 21. Configuración de la sección Protección del equipo en tiempo real

Sección	Opciones
Protección de archivos en tiempo real	En la sección **Protección de archivos en tiempo real**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Indicar el modo de protección. • Configurar el uso del Analizador heurístico. • Configurar el uso de la Zona de confianza. • Indicar el alcance de la protección. • Configurar el nivel de seguridad para el alcance de la protección seleccionada: puede seleccionar un nivel de seguridad predefinido o establecer la configuración de la seguridad manualmente. • Configurar las opciones de la ejecución de tareas.
Uso de KSN	En la subsección **Uso de KSN**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Indicar las acciones a realizar en objetos dudosos según KSN. • Configurar la transferencia de datos y el uso de Kaspersky Security Center como servidor proxy de KSN. Haga clic en el botón **Manejo de datos** para aceptar o rechazar la Declaración de KSN y configurar las opciones de intercambio de datos confiables.

Sección	Opciones
Prevención de exploits	En la sección **Prevención de exploits**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de protección de memoria de proceso. • Indicar las acciones para reducir riesgos de exploits. • Añadir elementos a la lista de procesos protegidos y editar dicha lista.

Control de actividad local

Table 22. Configuración de la sección Control de actividad local

Sección	Opciones
Control de inicio de aplicaciones	En la sección **Control de inicio de aplicaciones**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de operación de tareas. • Configurar las opciones para controlar los inicios subsiguientes de la aplicación. • Indicar el área de la aplicación de las reglas de Control de inicio de aplicaciones. • Configurar el uso de KSN. • Configurar las opciones de la ejecución de tareas.
Control de dispositivos	En la sección **Control de dispositivos**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Seleccionar el modo de operación de tareas. • Configurar las opciones de inicio de tareas.

Control de actividad de red

Table 23. Configuración de la sección Control de actividad de red

Sección	Opciones
Administración de firewall	En la sección **Administración de firewall**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones de la tarea: • Configurar las reglas de firewall. • Configurar las opciones de la ejecución de tareas.

Inspección del sistema

Table 24. Configuración de la sección Inspección del sistema

Sección	Opciones
Monitor de integridad de archivos	En la sección **Monitor de integridad de archivos**, puede configurar el control de los cambios en archivos que pueden significar una infracción de la seguridad en un equipo protegido.
Inspección de registros	En la sección **Inspección de registros**, puede configurar el control de integridad del equipo protegido sobre la base de los resultados del análisis de Registro de eventos de Windows.

Registros y notificaciones

Table 25. Configuración de la sección Registros y notificaciones

Sección	Opciones
Registros de tareas	En la sección **Registros de tareas**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones: • Especificar el nivel de importancia de los eventos registrados para los componentes de la aplicación seleccionados. • Especificar la configuración de depósitos de almacenamiento del registro de tareas. • Especificar la integración de SIEM con la configuración de Kaspersky Security Center.
Notificaciones de eventos	En la sección **Notificaciones de eventos**, puede hacer clic en el botón **Configurar** para configurar las siguientes opciones: • Especificar la configuración de notificaciones del usuario para el evento *Objeto detectado*. • Especificar la configuración de notificaciones del administrador para cualquier evento seleccionado en la lista de eventos en la sección **Configuración de notificaciones**.
Interacción con el Servidor de administración	En la sección **Interacción con el Servidor de administración**, puede hacer clic en el botón **Configurar** para seleccionar los tipos de objetos que Kaspersky Embedded Systems Security 2.2 informará al Servidor de administración.

Historial de revisiones

En la sección **Historial de revisiones**, puede administrar revisiones: compararlas con la revisión actual u otra directiva, agregue descripciones de revisiones, guardar revisiones de un archivo o realizar una reversión.

Configuración del inicio programado de las tareas locales del sistema

Puede usar directivas para autorizar o bloquear el inicio de las tareas de Análisis a pedido y de Actualización del sistema local según la programación configurada localmente en cada equipo en el grupo de administración:

- Si el inicio programado de un tipo específico de tarea local del sistema está prohibido por una directiva, estas tareas no se realizarán en el equipo local según la programación. Puede iniciar las tareas locales del sistema manualmente.
- Si el inicio programado de un tipo específico de tarea local del sistema está permitido por una directiva, estas tareas se realizarán según los parámetros programados y configurados localmente para esta tarea.

De forma predeterminada, el inicio de tareas locales del sistema está prohibido por la directiva.

Recomendamos que no habilite el inicio de tareas locales del sistema si las actualizaciones o los análisis a pedido están siendo administrados por tareas de grupo de Kaspersky Security Center.

Si no usa las tareas actualización de grupo o análisis a pedido, permita que tareas locales del sistema se inicien en

la directiva: Kaspersky Embedded Systems Security 2.2 realizará actualizaciones de la base de datos de la aplicación y del módulo, e iniciará todas las tareas de análisis a pedido del sistema local de acuerdo con la programación predeterminada.

Puede usar directivas para autorizar o bloquear el inicio programado de las siguientes tareas del sistema locales:

- Tareas de Análisis a pedido: Análisis de áreas críticas, Análisis de archivos en cuarentena, Análisis al inicio del sistema operativo, Comprobación de integridad de módulos del programa.
- Tareas de actualización: Actualización de bases de datos, Actualización de módulos del programa y Copia de actualizaciones.

Si el equipo protegido se excluye del grupo de administración, la programación de tareas del sistema se habilitará automáticamente.

► *Para autorizar o bloquear el inicio programado de tareas del sistema de Kaspersky Embedded Systems Security 2.2 en una directiva, siga estos pasos:*

1. En el nodo **Dispositivos administrados** del árbol de la consola de administración, expanda el grupo requerido y seleccione la pestaña **Directivas**.
2. En la pestaña **Directivas**, en el menú contextual de la directiva para la que desea configurar el inicio programado de tareas del sistema de Kaspersky Embedded Systems Security 2.2 en el grupo de equipos, seleccione el comando **Propiedades**.
3. En la ventana **Propiedades: <Nombre de la directiva>**, abra la sección **Configuración de la aplicación**. En la sección **Ejecutar tareas del sistema**, haga clic en el botón **Configurar** y realice lo siguiente:
   - Seleccione las casillas de verificación **Permitir que se inicien las tareas de análisis a pedido** y **Permitir que se inicien las tareas de actualización y de Copia de actualizaciones** para autorizar el inicio programado de estas tareas.
   - Desactive las casillas de verificación **Permitir que se inicien las tareas de análisis a pedido** y **Permitir que se inicien las tareas de actualización y de Copia de actualizaciones** para deshabilitar el inicio programado estas tareas.

   La selección o la desactivación de la casilla de verificación no afectará la configuración del inicio de ninguna tarea local creada por el usuario de este tipo.
4. Asegúrese de que la directiva (consulte la sección “Acerca de las directivas”, en la página 89) que configura esté activa y se aplique al grupo de equipos seleccionado.
5. Haga clic en **Aceptar**.

La configuración del inicio de la tarea programada establecida se aplica para las tareas seleccionadas.

Creación y configuración de tareas con Kaspersky Security Center

Esta sección contiene información sobre tareas de Kaspersky Embedded Systems Security 2.2 y cómo crearlas, configurarlas, iniciarlas y detenerlas.

En este capítulo

Acerca de la creación de tareas en Kaspersky Security Center

Puede crear tareas de grupo para grupos de administración y conjuntos de equipos. Puede crear los siguientes tipos de tareas:

- Activación de la aplicación
- Copia de actualizaciones
- Actualización de bases de datos
- Actualización de módulos del programa
- Reversión de la actualización de bases de datos
- Análisis a pedido
- Control de integridad de la aplicación
- Generador de reglas de control de inicio de aplicaciones
- Generador de reglas para Control de dispositivos

Puede crear tareas de grupo y locales de las siguientes maneras:

- Para un equipo: en la ventana **Propiedades <Nombre del equipo>** en la sección **Tareas** .
- Para un grupo de administración: en el panel de detalles del nodo del grupo seleccionado de equipos en la pestaña **Tareas**.
- Para un conjunto de equipos: en el panel de detalles del nodo **Selecciones de dispositivos**.

Mediante el uso de directivas, puede deshabilitar programaciones de tareas del sistema local de actualizaciones y de Análisis a pedido (consulte la sección “Configuración del inicio programado de las tareas locales del sistema”, en la página 96) en todos los equipos protegidos desde el mismo grupo de administración.

Se proporciona información general sobre tareas en Kaspersky Security Center en la *Ayuda de Kaspersky Security Center* .

Creación de una tarea mediante Kaspersky Security Center

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

► *Para crear una tarea nueva en la Consola de administración de Kaspersky Security Center:*

1. Inicie el asistente de tareas de una de las siguientes maneras:
   - Para crear una tarea local:
     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo al cual pertenece el equipo protegido.
     b. En el panel de resultados, en la pestaña **Dispositivos**, abra el menú contextual del equipo protegido y seleccione **Propiedades**.
     c. En la ventana que se abre, haga clic en el botón **Agregar** en la sección **Tareas**.
   - Para crear una tarea de grupo:
     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo para el cual desea crear una tarea.
     b. En el panel de detalles, abra la pestaña **Tareas** y seleccione **Crear una tarea**.
   - Para crear una tarea para un conjunto personalizado de equipos, en el nodo **Selecciones de dispositivos** en el árbol de la Consola de administración de Kaspersky Security Center seleccione **Crear una nueva tarea**.

   Se abre la ventana del asistente de tareas.
2. En la ventana **Seleccionar el tipo de tarea**, en el encabezado **Kaspersky Embedded Systems Security**

2.2, seleccione el tipo de tarea que se creará.

3. Si selecciona cualquier tipo de tarea que no sea Reversión de la actualización de bases de datos o Activación de la aplicación, se abre la ventana **Configuración**. Según el tipo de tarea creada, realice una de las siguientes acciones:

   - *Para crear una tarea de Análisis a pedido*:

     a. Cree un área del análisis en la ventana **Área del análisis**.

        De manera predeterminada, el área del análisis incluye áreas críticas del equipo. Las áreas del análisis están marcadas en la tabla con el icono ☑.

        Puede cambiar el área del análisis: agregar áreas del análisis predefinidas, discos, carpetas, objetos de red y archivos, y asignar la configuración de seguridad específica para cada área agregada.

        - Para excluir todas las áreas críticas del análisis, abra el menú contextual en cada una de las líneas y seleccione la opción **Eliminar área**.
        - Para incluir un área del análisis predefinida, disco, carpeta, objeto de red o archivo en el área del análisis, haga clic con el botón derecho en la tabla **área del análisis** y seleccione Agregar área. En la ventana **Agregar objetos al área del análisis**, seleccione el área predefinida en la lista **Área predefinida**, especifique el disco, la carpeta, el objeto de red o el archivo en el equipo o en otro equipo en red y haga clic en el botón **Aceptar**.
        - Para excluir subcarpetas o archivos del análisis, seleccione la carpeta agregada (disco) en la ventana **Área del análisis** del asistente, abra el menú contextual y seleccione **Configuración**; luego, haga clic en el botón **Configurar** en la ventana Nivel de seguridad y en la ventana **Configuración del análisis a pedido** en la pestaña **General**, desactive las casillas de verificación **Subcarpetas** y **Subarchivos**.
        - Para cambiar la configuración de seguridad del área del análisis, abra el menú contextual en el análisis cuya configuración desea definir y seleccione **Configurar**. En la ventana **Configuración del análisis a pedido**, seleccione uno de los niveles de seguridad predefinidos o haga clic en el botón **Configurar** para definir la configuración de seguridad manualmente. La configuración se realiza de la misma forma que en la Consola de Kaspersky Embedded Systems Security 2.2.
        - Para omitir objetos integrados en el área del análisis agregada, abra el menú contextual en la tabla **área del análisis**, seleccione **Agregar exclusión** y especifique los objetos que desea excluir: seleccione el área del análisis predefinida en la lista área del análisis, especifique el disco, la carpeta, el objeto de red o el archivo en el equipo protegido o en otro equipo de red y haga clic en el botón **Aceptar**.
        - Las áreas del análisis excluidas están marcadas con el icono ☐ en la tabla.

     b. Realice lo siguiente en la ventana **Opciones**.

        Seleccione la casilla de verificación **Aplicar la Zona de confianza** si desea excluir objetos descritos en la zona de confianza de Kaspersky Embedded Systems Security 2.2 del área del análisis de la tarea.

        Si planea usar la tarea creada como una tarea del Análisis de áreas críticas, seleccione la casilla de verificación **Ejecutar tarea en segundo plano** en la ventana **Opciones**. Kaspersky Security Center evalúa la calificación de seguridad del equipo (o los equipos) según los resultados de rendimiento de las tareas con estado *Análisis de áreas críticas* y no solo con los resultados de desempeño de la tarea del sistema **Análisis de áreas críticas**. Al crear una tarea de Análisis a pedido local, esta casilla de verificación no está disponible.

        Para asignar la prioridad base **Bajo** al proceso de trabajo en que se ejecutará la tarea, seleccione

la casilla de verificación **Ejecutar tarea en segundo plano** en la ventana **Opciones**. De manera predeterminada, a los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security 2.2 se les asigna la prioridad **Medio** (Normal). Si se degrada la prioridad del proceso, se aumenta el tiempo requerido para ejecutar la tarea, pero puede tener un efecto beneficioso en la velocidad de ejecución de los procesos de otros programas activos.

- *Para crear una tarea de actualización*, configure los valores de la tarea según sus requisitos:

  a. Seleccione el origen de actualizaciones en la ventana **Origen de actualizaciones**.

  b. Haga clic en el botón **Configuración de conexión**. Se abrirá la ventana **Configuración de conexión**.

  c. En la ventana **Configuración de conexión**:

     Especifique el modo del servidor FTP para la conexión con el equipo protegido.

     Modifique el tiempo de espera de conexión al establecer conexión con el origen de actualizaciones, si es necesario.

     Defina la configuración de acceso al servidor proxy al establecer conexión con el origen de actualizaciones.

     Especifique la ubicación de los equipos protegidos con el fin de optimizar las descargas de actualizaciones.

- *Para crear una tarea de Actualización de módulos del programa*, configure los parámetros de actualización de los módulos del programa requeridos en la ventana **Configuración de la actualización de módulos del programa**:

  a. Seleccione una de estas opciones para copiar e instalar actualizaciones del módulo del software críticas o solo comprobar su disponibilidad sin instalarlas.

  b. Si la opción **Copiar e instalar actualizaciones críticas de módulos del programa** está seleccionada: es posible que deba reiniciarse el equipo para aplicar los módulos de software instalados. Si desea que Kaspersky Embedded Systems Security 2.2 reinicie el equipo automáticamente después de finalizar la tarea, seleccione la casilla de verificación **Permitir el reinicio del sistema operativo**. Para deshabilitar el reinicio automático del equipo al finalizar la tarea, desactive la casilla de verificación **Permitir el reinicio del sistema operativo**.

  c. Para obtener información sobre actualizaciones de módulos de Kaspersky Embedded Systems Security 2.2, seleccione **Informarme de las actualizaciones programadas que estén disponibles para los módulos del programa**.

     Kaspersky Lab no publica paquetes de actualizaciones planificadas en los servidores de actualización para la instalación automática; se deben descargar manualmente desde el sitio web de Kaspersky Lab. Es posible configurar una notificación de administrador del evento **Está disponible una nueva actualización programada de módulos del programa**. Esto incluirá la URL de nuestro sitio web desde donde puede descargar las actualizaciones programadas.

- *Para crear la tarea Copia de actualizaciones*, especifique el conjunto de actualizaciones y la carpeta de destino en la ventana **Configuración de la copia de actualizaciones**.

- *Para crear la tarea Activación de la aplicación*, en la ventana **Configuración de la activación**, aplique el archivo de clave que desea utilizar para activar la aplicación. Seleccione la casilla de verificación **Usar como clave adicional** si desea crear una tarea para renovar la licencia.

- *Para crear la tarea Generador de reglas de control de inicio de aplicaciones o la tarea Generador de reglas para Control de dispositivos*, en la ventana **Configuración**, especifique la configuración según la cual se creará la lista de reglas de autorización:

  a. Especifique un prefijo para los nombres de la regla (solo para la tarea Generador de reglas de

control de inicio de aplicaciones).

b. Configure el área de aplicación de las reglas de autorización (solo para la tarea Generador de reglas de control de inicio de aplicaciones). Haga clic en el botón **Siguiente**.

c. Especifique las acciones que la tarea de autorización realizará al generar las reglas de autorización (solo para la tarea Generador de reglas de control de inicio de aplicaciones) y después de la finalización de la tarea.

4. Configure la programación de la tarea (puede configurar una programación para todos los tipos de tareas excepto Reversión de la actualización de bases de datos). Realice las siguientes acciones en la ventana **Programación**:

   a. Seleccione la casilla de verificación **Ejecutar según programación** para habilitar la programación;

   b. Especifique la frecuencia de inicio de la tarea: seleccione uno de los valores siguientes de la lista **Frecuencia**: **Horaria**, **Diaria**, **Semanal**, **Al inicio de la aplicación**, **Tras la actualización de bases de datos de la aplicación** (la frecuencia de inicio **Después de que el Servidor de administración obtenga las actualizaciones** también puede especificarse en las siguientes tareas de grupo: Actualización de bases de datos y Actualización de módulos del programa):

      - Si selecciona **Horaria**, especifique la cantidad de horas en el valor **Cada <número> hora(s)** en el grupo de configuración **Configuración de inicio de la tarea**;
      - Si selecciona **Diaria**, especifique la cantidad de días en el valor **Cada <número> día(s)** en el grupo de configuración **Configuración de inicio de la tarea**.
      - Si selecciona **Semanal**, especifique la cantidad de semanas en el valor **Cada <número> semana(s)** en el grupo de configuración **Configuración de inicio de la tarea**. Especifique los días de la semana en que se iniciará la tarea (de manera predeterminada, los lunes).

   c. En el campo **Hora de inicio**, especifique la hora en que se iniciará la tarea; en el campo **Fecha de inicio**, especifique la fecha en que se comenzará a aplicar la programación.

   d. Especifique la configuración de programación restante si es necesario: haga clic en el botón **Avanzado** y haga lo siguiente en la ventana **Configuración avanzada de la programación**:

      - Especifique la duración máxima de la ejecución de la tarea: introduzca la cantidad de horas y minutos en el campo **Duración** en el grupo de configuración **Configuración de detención de la tarea**.
      - Especifique el intervalo de tiempo dentro de un periodo de 24 horas en que se debe pausar la ejecución de una tarea: en el grupo de configuración **Configuración de detención de la tarea**, introduzca los valores de inicio y de finalización del intervalo en el campo **Pausar de** y **a**.
      - Especifique la fecha en la cual se deshabilitará la programación: seleccione la casilla de verificación **Fin de la programación** y seleccione la fecha en la que se deshabilitará la programación mediante la ventana **Calendario**.
      - Habilite el inicio de tareas ignoradas: seleccione la casilla de verificación **Ejecutar tareas omitidas**.
      - Habilite la configuración de distribución de la hora de inicio: seleccione la casilla de verificación **Aleatorizar la hora de inicio de la tarea usando un margen de** y especifique el valor en minutos.

   e. Haga clic en **Aceptar**.

5. Si la tarea creada es para conjuntos de equipos, seleccione los equipos (o el grupo de equipos) de red en los que se ejecutará esta tarea.

6. En la ventana **Seleccionar una cuenta para ejecutar la tarea**, especifique la cuenta con la cual desea ejecutar la tarea.

7. En la ventana **Especificar nombre de tarea**, especifique el nombre de la tarea (100 caracteres como máximo) que no contenga los símbolos **" * < > ? \ | :** . Se recomienda que el tipo de tarea se agregue a su nombre (por ejemplo, "Análisis a pedido de carpetas compartidas").
8. En la ventana **Finalizar creación de la tarea**, seleccione la casilla de verificación **Ejecutar tarea cuando el asistente finalice** si desea que la tarea se inicie tan pronto como se crea. Haga clic en el botón **Finalizar**.

La tarea creada se mostrará en la lista **Tareas**.

Configuración de tareas locales en la ventana Configuración de la aplicación en Kaspersky Security Center

► *Para configurar tareas locales o establecer la configuración general de la aplicación en la ventana Configuración de la aplicación para un equipo de red, realice las tareas siguientes:*

1. Amplíe el nodo **Dispositivos administrados** en el árbol del Servidor de administración de Kaspersky Security Center y seleccione el grupo al cual pertenece el equipo protegido.
2. En el panel de detalles, seleccione la pestaña **Dispositivos**.
3. Abra la ventana **Propiedades: <Nombre del equipo>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre del equipo protegido
   - Abra el menú contextual del nombre del equipo protegido y seleccione el elemento **Propiedades**

   Se abre la ventana **Propiedades: <Nombre del equipo>**.
4. Para configurar las opciones de la tarea local, siga estos pasos:
   a. Vaya a la sección **Tareas**.
      - En la lista de tareas, seleccione una tarea local para configurar.
      - Haga doble clic en el nombre de la tarea en la lista de tareas.
      - Seleccione el nombre de la tarea y haga clic en el botón **Propiedades**.
      - Seleccione **Propiedades** en el menú contextual de la tarea seleccionada.
5. Para configurar las opciones de la aplicación, siga estos pasos:
   a. Vaya a la sección **Aplicaciones**.
      - En la lista de aplicaciones instaladas, seleccione la aplicación que desea configurar.
      - Haga doble clic en el nombre de la aplicación en la lista de aplicaciones instaladas
      - Seleccione el nombre de la aplicación en la lista de aplicaciones instaladas y haga clic en el botón **Propiedades**.
      - Abra el menú contextual del nombre de la aplicación en la lista de aplicaciones instaladas y seleccione el elemento **Propiedades**.

Si una aplicación está bajo una directiva de Kaspersky Security Center y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede editar a través de la ventana **Configuración de la aplicación**.

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

Configuración de tareas de grupo en Kaspersky Security Center

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

► *Para configurar una tarea de grupo para varios equipos:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. Según el tipo de tarea configurada, realice una de las siguientes acciones:
   - Para configurar una tarea de Análisis a pedido:
     a. En la sección **área del análisis**, configure un área del análisis.
     b. En la sección **Opciones**, configure el nivel de prioridad de la tarea y la integración con otros componentes del programa.
   - Para configurar una tarea de actualización, establezca los valores de la tarea según sus requisitos:
     a. En la sección **Configuración**, establezca la configuración del origen de actualizaciones y la optimización de uso del subsistema del disco.
     b. Haga clic en el botón **Configuración de conexión** para configurar las opciones de conexión con el origen de actualizaciones.
   - Para configurar la tarea de Actualización de módulos del programa, en la sección **Configuración de la actualización de módulos del programa**, elija una acción para realizar: copiar e instalar actualizaciones críticas de módulos de programa o solo comprobar si existen.
   - Para configurar la tarea Copia de actualizaciones, especifique el conjunto de actualizaciones y la carpeta de destino en la sección **Configuración de la copia de actualizaciones**.
   - Para configurar la tarea Activación de la aplicación, en la sección **Configuración de la activación**, aplique el archivo de clave que desea utilizar para activar la aplicación. Seleccione la casilla de verificación **Usar como código de activación o clave adicionales** si desea agregar una clave o código de activación para renovar la licencia.
   - Para configurar la generación automática de las reglas de autorización para el control del equipo, en la sección **Configuración**, especifique la configuración según la cual se creará la lista de reglas de autorización.
6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones del área de la tarea**. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
9. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

Se guardan las opciones de las tareas de grupo recientemente configuradas.

Los parámetros de tareas de grupo que están disponibles para la configuración se resumen en la tabla a continuación.

Table 26. Configuración de tareas de grupo de Kaspersky Embedded Systems Security 2.2

Tipos de tareas de Kaspersky Embedded Systems Security 2.2	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas

Tipos de tareas de Kaspersky Embedded Systems Security 2.2	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas
Generación de reglas automáticas (consulte la sección “Tareas del Generador de reglas de control de inicio de aplicaciones y Generador de reglas para Control de dispositivos”, en la página 109)	**Configuración**	Al configurar la tarea de Generador de reglas de control de inicio de aplicaciones, puede hacer lo siguiente: • Cambiar el alcance de la protección si agrega o elimina las rutas a las carpetas y especifica tipos de archivo cuyo inicio es autorizado por reglas generadas automáticamente. • Tenga en cuenta las aplicaciones actualmente en ejecución.
	Opciones	Puede especificar las acciones que desea realizar mientras crea reglas de autorización de Control de inicio de aplicaciones: • **Usar certificado digital** • **Usar sujeto y huella digital del certificado digital** • **De no haber un certificado, usar** • **Usar hash SHA256** • **Generar reglas para este usuario o grupo de usuarios** Puede establecer la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security 2.2 crea después de la finalización de la tarea.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Activación de la aplicación (consulte la sección “Tarea Activación de la aplicación”, en la página 111)	**Configuración de la activación**	Para activar la aplicación o renovar la fecha de caducidad, puede agregar una clave.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Copia de actualizaciones (consulte la sección “Tareas de actualización”, en la página 112)	**Origen de actualizaciones**	Puede especificar el Servidor de administración de Kaspersky Security Center o los servidores de actualización de Kaspersky Lab como el origen de actualizaciones de la aplicación. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualización de Kaspersky Lab, si los servidores personalizados manualmente no están disponibles.
	Ventana **Configuración de conexión**	En el cuadro de grupo **Configuración de la conexión con el origen de actualizaciones**, puede especificar si debería establecerse la conexión con los Servidores de actualización de Kaspersky Lab o algún otro servidor mediante el servidor proxy.

Tipos de tareas de Kaspersky Embedded Systems Security 2.2	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas
	Configuración de la copia de actualizaciones	Puede especificar el conjunto de actualizaciones que desea copiar. En el campo **Carpeta de almacenamiento local para las actualizaciones copiadas**, especifique una ruta a una carpeta, que Kaspersky Embedded Systems Security 2.2 utilizará para almacenar las actualizaciones copiadas.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Actualización de bases de datos (consulte la sección “Tareas de actualización”, en la página 112)	**Configuración**	Puede especificar el Servidor de administración de Kaspersky Security Center o los Servidores de actualización de Kaspersky Lab como origen de actualizaciones de la aplicación en el cuadro de grupo **Origen de actualizaciones**. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualización de Kaspersky Lab, si los servidores personalizados manualmente no están disponibles. En la sección Optimización de lectura y escritura en disco, puede configurar la función que reduce la carga de trabajo en el subsistema del disco: • **Reducir la carga de lectura y escritura en disco** • **RAM usada para la optimización (MB)**
	Ventana **Configuración de conexión**	En el cuadro de grupo **Configuración de la conexión con el origen de actualizaciones**, puede especificar si debería establecerse la conexión con los Servidores de actualización de Kaspersky Lab o algún otro servidor mediante el servidor proxy.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Actualización de módulos del programa (consulte la sección “Tareas de actualización”, en la página 112)	**Origen de actualizaciones**	Puede especificar el Servidor de administración de Kaspersky Security Center o los servidores de actualización de Kaspersky Lab como el origen de actualizaciones de la aplicación. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones. Puede especificar el uso de Servidores de actualización de Kaspersky Lab, si los servidores personalizados manualmente no están disponibles.

Tipos de tareas de Kaspersky Embedded Systems Security 2.2	Sección en la ventana Propiedades: <Nombre de la tarea>	Configuración de tareas
	Ventana **Configuración de conexión**	En el cuadro de grupo **Configuración de la conexión con el origen de actualizaciones**, puede especificar si debería establecerse la conexión con los Servidores de actualización de Kaspersky Lab o algún otro servidor mediante el servidor proxy.
	Configuración de la actualización de módulos del programa	Puede especificar qué acciones debe realizar Kaspersky Embedded Systems Security 2.2 cuando están disponibles o se hayan instalado actualizaciones críticas de los módulos de la aplicación, y también si Kaspersky Embedded Systems Security 2.2 debe recibir información sobre las actualizaciones programadas.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Análisis a pedido (consulte la sección “Creación de la tarea Análisis a pedido”, en la página 114)	**Área del análisis**	Puede especificar un área del análisis para la tarea de Análisis a pedido y configurar las opciones del nivel de seguridad.
	Ventana **Configuración del análisis a pedido**	Puede seleccionar uno de niveles de seguridad predefinidos o personalizar el nivel de seguridad manualmente.
	Opciones	Puede activar o desactivar el uso del analizador heurístico para la tarea de Análisis a pedido y establecer el nivel de análisis mediante un control deslizante en el cuadro de grupo **Analizador heurístico**. En el cuadro de grupo **Integración con otros componentes**, puede configurar los siguientes componentes: • Aplicar la zona de confianza para tareas de Análisis a pedido • Aplicar el Uso de KSN para las tareas de Análisis a pedido • Configurar una prioridad para la tarea de Análisis a pedido: ejecutar tarea en segundo plano (prioridad baja) o considere la tarea de Análisis de áreas críticas.
	Programación	Puede configurar las opciones del inicio programado de la tarea.
Comprobación de integridad de módulos del programa (en la página 113)	**Programación**	Puede configurar las opciones del inicio programado de la tarea.

Para las tareas, por ejemplo, la Reversión de la actualización de bases de datos, puede establecer solo la configuración de la tarea estándar en las secciones **Notificación** y **Exclusiones del área de la tarea**, controladas por Kaspersky Security Center. Para obtener información detallada sobre la configuración de opciones de estas

secciones, consulte la *Ayuda de Kaspersky Security Center*.

En esta sección

Tareas del Generador de reglas de control de inicio de aplicaciones y Generador de reglas para Control de dispositivos

► *Para configurar la tarea Generador de reglas para Control de dispositivos o la tarea Generador de reglas de control de inicio de aplicaciones, haga lo siguiente:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.
5. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
6. En la sección **Configuración**, puede establecer la siguiente configuración:
   - Cambie el alcance de la protección si agrega o elimina las rutas a las carpetas y especifica tipos de archivo cuyo inicio es autorizado por reglas generadas automáticamente.
   - Tenga en cuenta las aplicaciones actualmente en ejecución.

7. En la sección **Configuración**, puede especificar las acciones que desea realizar mientras crea reglas de autorización de Control de inicio de aplicaciones:

   - **Usar certificado digital**

     Si esta opción está seleccionada, se especifica la presencia de un certificado digital como el criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inician mediante archivos con un certificado digital. Esta opción se recomienda si desea autorizar el inicio de alguna aplicación de confianza en el sistema operativo.

     De forma predeterminada, esta opción está seleccionada.

   - **Usar sujeto y huella digital del certificado digital**

     La casilla de verificación habilita o deshabilita el uso del asunto y la huella del certificado digital del archivo como el criterio para activar las reglas de autorización para el Control de inicio de aplicaciones. Seleccionar esta casilla de verificación le permite especificar condiciones más estrictas de verificación del certificado digital.

     Si esta casilla de verificación está seleccionada, los valores del asunto y de la huella del certificado digital de los archivos para los cuales se generan las reglas se configuran como el criterio de activación de las reglas de autorización para el Control de inicio de aplicaciones. Kaspersky Embedded Systems Security 2.2 autorizará las aplicaciones que se inicien mediante archivos con una huella y un certificado digital especificados.

     Seleccionar esta casilla de verificación restringe ampliamente la activación de reglas de autorización sobre la base de un certificado digital, ya que una huella es un identificador exclusivo de un certificado digital y no se puede falsificar.

     Si esta casilla de verificación está desactivada, la existencia de cualquier certificado digital de confianza en el sistema operativo se configura como el criterio de activación de las reglas de autorización para el Control de inicio de aplicaciones.

     Esta casilla de verificación está activa si la opción **Usar certificado digital** está seleccionada.

     De forma predeterminada, la casilla está activada.

   - **De no haber un certificado, usar**

     Lista desplegable que le permite seleccionar el criterio de activación de reglas de autorización para el Control de inicio de aplicaciones si el archivo, que se usa para generar la regla, no tiene ningún certificado digital.

     - **Hash SHA256**. El valor de la suma de control del archivo, que se usa para generar la regla, se configura como el criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación permitirá el inicio de programas que se inicien mediante archivos con la suma de control especificada.
     - **Ruta de acceso al archivo**. La ruta de acceso al archivo, que se usa para generar la regla, se configura como el criterio de activación de la regla de autorización para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inicien con archivos ubicados en las carpetas de la pestaña especificada en la tabla Crear reglas de autorización para las aplicaciones de las siguientes carpetas.

   - **Usar hash SHA256**

     Si esta opción está seleccionada, el valor de la suma de control del archivo, que se usa para generar la regla, se especifica como el criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de

inicio de aplicaciones. La aplicación autorizará el inicio de programas que se inicien mediante archivos con el valor de suma de control especificado.

Esta opción se recomienda para los casos en los que se requieren reglas generadas para cumplir el nivel de seguridad superior: La suma de control de SHA256 puede aplicarse como una Id. de archivo única. El uso de la suma de control de SHA256 como un criterio de activación de la regla limita el área de aplicación de la regla a un archivo.

- **Generar reglas para este usuario o grupo de usuarios**.

  Campo que muestra a un usuario o grupo de usuarios. La aplicación supervisará las aplicaciones ejecutadas por el usuario especificado o el grupo de usuarios.

  La selección predeterminada es **Todos**.

Puede establecer la configuración para archivos de configuración con listas de reglas de autorización que Kaspersky Embedded Systems Security 2.2 crea después de la finalización de la tarea.

8. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
9. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.
10. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones** del área de la tarea.

    Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

11. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

    Se guardan las opciones de las tareas de grupo recientemente configuradas.

Activación de la tarea Aplicación

► *Para configurar la Activación de la tarea Aplicación, siga estos pasos:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.
5. Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.
6. En la sección **Configuración de la activación**, aplique el archivo de clave que desea usar para activar la

aplicación. Seleccione la casilla de verificación **Usar como clave adicional** si desea agregar una clave para extender la licencia.

7. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
8. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.
9. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones** del área de la tarea.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

10. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

    Se guardan las opciones de las tareas de grupo recientemente configuradas.

Tareas de actualización

Para configurar las tareas Copia de actualizaciones, Actualización de bases de datos o Actualización de módulos del programa, haga lo siguiente:

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. Según el tipo de tarea configurada, realice una de las siguientes acciones:
   - En la sección **Origen de actualizaciones**, configure las opciones del origen de actualizaciones y la optimización de uso del subsistema del disco.
     a. Puede especificar el Servidor de administración de Kaspersky Security Center o los Servidores de actualización de Kaspersky Lab como origen de actualizaciones de la aplicación en la sección **Origen de actualizaciones**. También puede crear una lista personalizada de orígenes de actualizaciones: si agrega servidores FTP o HTTP personalizados o carpetas de red manualmente y los configura como orígenes de actualizaciones.

        Puede especificar el uso de Servidores de actualización de Kaspersky Lab, si los servidores

personalizados manualmente no están disponibles.

b. En la sección **Optimización de lectura y escritura en disco** de la tarea Actualización de bases de datos, puede configurar la función que reduce la carga de trabajo en el subsistema del disco:

- **Reducir la carga de lectura y escritura en disco**

  Esta casilla de verificación habilita o deshabilita la función de optimización del subsistema del disco mediante el almacenamiento de archivos de actualización en una unidad virtual en la RAM.

  Si se activa la casilla, se habilita esta función.

  De forma predeterminada, la casilla está desactivada.

- **RAM usada para la optimización (MB)**

  El tamaño de la RAM (en MB) que la aplicación usa para almacenar archivos de actualización. El tamaño de RAM predeterminado es 512 MB. El tamaño de RAM mínimo es 400 MB.

c. Haga clic en el botón **Configuración de conexión** y, en la ventana **Configuración de conexión** que se abre, configure el uso de un servidor proxy para conectarse a servidores de actualizaciones de Kaspersky Lab y otros servidores.

- En la sección **Configuración de la actualización de módulos del programa** para la tarea de actualización de módulos del programa, puede especificar qué acciones debería realizar Kaspersky Embedded Systems Security 2.2 cuando haya disponibles actualizaciones críticas del módulo del programa o información sobre actualizaciones planificadas, y también puede especificar qué acciones debería realizar Kaspersky Embedded Systems Security 2.2 durante la instalación de actualizaciones críticas.
- Especifique el conjunto de actualizaciones y la carpeta de destino en la sección **Configuración de la copia de actualizaciones** para la tarea **Copia de actualizaciones**.

6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.

> Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

8. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

Se guardan las opciones de las tareas de grupo recientemente configuradas

Para la tarea Reversión de la actualización de bases de datos, puede establecer solo la configuración de la tarea estándar controlada por Kaspersky Security Center en las secciones **Notificaciones** y **Exclusiones** del área de la tarea. Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

Comprobación de integridad de módulos del programa

► *Para configurar la tarea de grupo Actualización de módulos del programa:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de

la aplicación.

2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

   Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. En la sección **Dispositivos**, seleccione los dispositivos para los cuales desea configurar la tarea Comprobación de integridad de módulos del programa.
6. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
7. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.
8. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones** del área de la tarea.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.

9. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

   Se guardan las opciones de las tareas de grupo recientemente configuradas.

Creación de una tarea de Análisis a pedido

► *Para crear una tarea nueva en la Consola de administración de Kaspersky Security Center:*

1. Inicie el asistente de tareas de una de las siguientes maneras:
   - Para crear una tarea local:
     a. Amplíe el nodo **Dispositivos administrados** en el árbol del Servidor de administración de Kaspersky Security Center y seleccione el grupo al cual pertenece el equipo protegido.
     b. En el panel de resultados, en la pestaña **Dispositivos**, abra el menú contextual de la línea con información sobre el equipo protegido y seleccione **Propiedades**.
     c. En la ventana que se abre, haga clic en el botón **Agregar** en la sección **Tareas**.
   - Para crear una tarea de grupo:
     a. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo para el cual desea crear una directiva.

b. En el panel de detalles, abra el menú contextual en la pestaña **Tareas** y seleccione **Nueva > Tarea**.

- Para crear una tarea para un conjunto personalizado de equipos, en el nodo **Selecciones de dispositivos** en el árbol de la Consola de administración de Kaspersky Security Center seleccione **Nueva tarea**.

Se abre la ventana del asistente de tareas.

2. En la ventana **Especificar nombre de tarea**, especifique el nombre de la tarea (de 100 caracteres como máximo) que no contenga los símbolos **I * < > ? \ / | :)**. Se recomienda que el tipo de tarea se agregue a su nombre (por ejemplo, "Análisis a pedido de carpetas compartidas").
3. En la ventana **Tipo de tarea**, en el encabezado **Kaspersky Embedded Systems Security 2.2**, seleccione la tarea **Análisis a pedido** y haga clic en **Siguiente**.
4. Cree un área del análisis en la ventana **área del análisis**:

> De manera predeterminada, el área del análisis incluye áreas críticas del equipo. Las áreas del análisis están marcadas en la tabla con el icono ☑. Las áreas del análisis excluidas están marcadas con el icono ☐ en la tabla.
> Puede cambiar el área del análisis: agregar áreas del análisis predefinidas, discos, carpetas, objetos de red y archivos, y asignar la configuración de seguridad específica para cada área agregada.

- Para excluir todas las áreas críticas del análisis, abra el menú contextual en cada una de las líneas y seleccione la opción **Eliminar área**.
- Para incluir un área del análisis predeterminada, disco, carpeta, objeto de red o archivo en el área del análisis:
  a. Haga clic con el botón derecho en la tabla **área del análisis** y seleccione **Agregar área**, o bien haga clic en el botón **Agregar**.
  b. En la ventana **Agregar objetos al área del análisis**, seleccione el área predefinida en la lista **Área predefinida**, especifique el disco, la carpeta, el objeto de red o el archivo en el equipo o en otro equipo en red y haga clic en el botón **Aceptar**.
- Para excluir subcarpetas o archivos del análisis, seleccione la carpeta (o el disco) agregado en la ventana **área del análisis** del asistente:
  a. Abra el menú contextual y seleccione la opción **Configurar**.
  b. Haga clic en el botón **Configurar** en la ventana **Nivel de seguridad**.
  c. En la pestaña **General** de la ventana **Configuración del análisis a pedido**, cancele la selección de las casillas de verificación **Subcarpetas** y **Subarchivos**.
- Para cambiar la configuración de seguridad del área del análisis:
  a. Abra el menú contextual en el análisis cuya configuración desea definir y seleccione **Configurar**.
  b. En la ventana **Configuración del Análisis a pedido**, seleccione uno de los niveles de seguridad predefinidos o haga clic en el botón **Configurar** para definir la configuración de seguridad manualmente.

> Las opciones de seguridad se configuran de la misma manera que en la tarea Protección de archivos en tiempo real (consulte la sección “Configuración manual de las opciones de seguridad”, en la página 157).

- Para omitir objetos integrados en el área del análisis agregada:

  a. Abra el menú contextual en la tabla **área del análisis** y seleccione **Agregar exclusión**.

  b. Especifique los objetos que desea excluir: seleccione el área predefinida en la lista **Área predefinida**, especifique el disco del equipo, la carpeta, el objeto de red o el archivo en el equipo o en otro equipo de la red.

  c. Haga clic en el botón **Aceptar**.

5. En la ventana **Opciones**, configure el analizador heurístico y la integración con los demás componentes:

- Configure el uso del analizador heurístico (consulte la sección “Uso del analizador heurístico”, en la página 152).
- Seleccione la casilla de verificación **Aplicar la Zona de confianza** si quiere excluir objetos descritos en la zona de confianza de Kaspersky Embedded Systems Security 2.2 del área del análisis de la tarea.

  Esta casilla de verificación habilita y deshabilita el uso de la Zona de confianza para una tarea.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 agrega operaciones del archivo de procesos de confianza a las exclusiones de análisis configuradas en la tarea.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 ignora las operaciones del archivo de procesos de confianza al formar el alcance de la protección para la tarea Protección de archivos en tiempo real.

  De forma predeterminada, la casilla está activada.

- Seleccione la casilla de verificación **Usar KSN para análisis** si desea usar los servicios en la nube de Kaspersky Security Network para la tarea.

  Esta casilla de verificación habilita y deshabilita el uso de servicios en la nube de Kaspersky Security Network (KSN) en la tarea.

  Si la casilla de verificación está seleccionada, la aplicación usa datos recibidos de los servicios KSN para asegurar un tiempo de respuesta más rápido de la aplicación a nuevas amenazas y reducir la posibilidad de falsos positivos.

  Si la casilla de verificación está desactivada, la tarea Análisis a pedido no usa el servicio KSN.

  De forma predeterminada, la casilla está activada.

- Para asignar la prioridad base **Bajo** al proceso de trabajo en que se ejecutará la tarea, seleccione la casilla de verificación **Ejecutar tarea en segundo plano** en la ventana **Opciones**.

  La casilla de verificación modifica la prioridad de la tarea.

  Si la casilla está activada, se reduce la prioridad de la tarea en el sistema operativo. El sistema operativo proporciona recursos para realizar la tarea según la carga en la CPU y el sistema de archivos del equipo de otras aplicaciones y tareas de Kaspersky Embedded Systems Security 2.2. Como resultado, el rendimiento de las tareas se ralentizará durante el aumento de las cargas y aumentará la velocidad con cargas menores.

  Si la casilla de verificación está desactivada, la tarea se iniciará y se ejecutará con la misma prioridad que las demás aplicaciones y tareas de Kaspersky Embedded Systems Security 2.2. En este caso, aumenta la velocidad de ejecución de la tarea.

  De forma predeterminada, la casilla está desactivada.

De manera predeterminada, a los procesos de trabajo en que se ejecutan las tareas de Kaspersky Embedded Systems Security 2.2 se les asigna la prioridad **Medio** (Normal).

- Para utilizar la tarea creada como una tarea del Análisis de áreas críticas, seleccione la casilla de verificación **Considerar la tarea como análisis de áreas críticas** en la ventana **Opciones**.

  La casilla de verificación cambia la prioridad de la tarea: habilita o deshabilita el registro del evento *Análisis de áreas críticas* y la actualización del estado de protección del equipo. Kaspersky Security Center evalúa la calificación de seguridad del equipo (o los equipos) según los resultados de rendimiento de las tareas con el estado *Análisis de áreas críticas*. La casilla de verificación no está disponible en las propiedades del sistema local y las tareas creadas por el usuario de Kaspersky Embedded Systems Security 2.2. Solo puede modificar esta configuración en Kaspersky Security Center.

  Si esta casilla de verificación está seleccionada, el Servidor de administración registra el evento Análisis de áreas críticas completo y actualiza el estado de protección del equipo sobre la base de los resultados de la ejecución de la tarea. La tarea de análisis tiene una prioridad alta.

  Si la casilla de verificación está desactivada, la tarea se ejecuta con prioridad baja.

  La casilla está activada en forma predeterminada para la tarea Análisis de áreas críticas.

6. Haga clic en **Siguiente**.
7. En la ventana **Programación**, configure una programación (consulte la sección “Configuración de las opciones de programación de inicio de tareas”, en la página 123) para la tarea.
8. Especifique la cuenta de usuario con la cual desea ejecutar la tarea y defina el nombre de la tarea.
9. Haga clic en **Finalizar**.

Se creará la nueva tarea Análisis a pedido para el equipo o el grupo de equipos seleccionado.

Configuración de la tarea Análisis a pedido

► *Para configurar una tarea de Análisis a pedido existente, siga estos pasos:*

1. En el árbol de la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y seleccione el grupo de administración para el que desea configurar las tareas de la aplicación.
2. En el panel de detalles de un grupo de administración elegido, abra la pestaña **Tareas**.
3. En la lista de tareas de grupo creadas anteriormente, seleccione la tarea que desea configurar. Abra la ventana **Propiedades: <Nombre de la tarea>** con uno de los siguientes métodos:
   - Haga doble clic en el nombre de la tarea en la lista de tareas creadas
   - Seleccione el nombre de la tarea en la lista de tareas creadas y haga clic en el vínculo **Configurar tarea**.
   - Abra el menú contextual del nombre de la tarea en la lista de tareas creadas y seleccione el elemento **Propiedades**.
4. En la sección **Notificación**, configure las opciones de notificación del evento de la tarea.

Para obtener información sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

5. En la sección **Configuración**, puede realizar las siguientes acciones:
   a. En la sección **área del análisis**, seleccione las casillas junto a esos recursos del archivo que desea que se incluyan en el área del análisis.
   b. Haga clic en el botón **Configurar** y seleccione el nivel de seguridad.

      Puede seleccionar uno de niveles de seguridad predefinidos o personalizar el nivel de seguridad manualmente.
   c. Para configurar el nivel de seguridad manualmente, en la ventana **Configuración del análisis a pedido** haga clic en el botón **Configurar**.
6. En la sección **Opciones**, puede realizar las siguientes acciones:
   a. Habilite o deshabilite el uso del **Analizador heurístico** y configure el nivel de análisis con el control deslizante en el bloque **Analizador heurístico**.
   b. Defina las opciones de configuración avanzada (consulte la sección “Creación de la tarea Análisis a pedido”, en la página 114).
7. Configure la programación de la tarea en la sección **Programación** (puede configurar una programación para todos los tipos de tareas excepto la Reversión de la actualización de bases de datos).
8. En la sección **Cuenta**, especifique la cuenta cuyos derechos se utilizarán para la ejecución de la tarea.
9. Si es necesario, especifique los objetos para excluir del área de la tarea en la sección **Exclusiones** del área de la tarea.

   Para obtener información sobre la configuración de opciones en estas secciones, consulte la *Ayuda de Kaspersky Security Center*.
10. En la ventana **Propiedades: <Nombre de la tarea>**, haga clic en **Aceptar**.

    Se guardan las opciones de las tareas de grupo recientemente configuradas.

Asignar el estado de la tarea de Análisis de áreas críticas a una tarea de Análisis a pedido

De manera predeterminada, Kaspersky Security Center asigna el estado *Advertencia* al equipo si la tarea de Análisis de áreas críticas se ejecuta con menor frecuencia que la especificada por la configuración de los umbrales de generación de eventos **Hace mucho tiempo que no se realiza un análisis de áreas críticas** de Kaspersky Embedded Systems Security 2.2.

► *Para configurar el análisis de todos los equipos en un único grupo de administración, siga estos pasos:*

1. Cree una tarea de Análisis a pedido de grupo.
2. En la ventana **Opciones** del asistente de tareas, seleccione la casilla de verificación **Considerar la tarea como análisis de áreas críticas**. La configuración de tarea especificada (configuración de seguridad y área del análisis) se aplicará a todos los equipos del grupo. Configure la programación de la tarea.

Puede seleccionar la casilla de verificación **Considerar la tarea como análisis de áreas críticas** tanto cuando crea la tarea de Análisis a pedido para un grupo de equipos o un conjunto de equipos, como en otro momento, desde la ventana **Propiedades: <Nombre de la tarea>**.

3. La utilización de una directiva nueva o existente deshabilita el inicio programado de las tareas de análisis del sistema (consulte la sección “Configuración del inicio programado de las tareas locales del sistema”, en la página 96) en los equipos del grupo.

El servidor de administración de Kaspersky Security Center evaluará el estado de seguridad del equipo protegido y se lo notificará según los resultados de la última ejecución de la tarea con el estado tarea de Análisis de áreas críticas y no según los resultados de la tarea del sistema de *Análisis de áreas críticas*.

Puede asignar el estado de la tarea de *Análisis de áreas críticas* tanto a tareas en grupo de Análisis a pedido como a tareas para conjuntos de equipos.

La Consola de la aplicación se puede utilizar para ver si la tarea de Análisis a pedido es una tarea de Análisis de áreas críticas.

En la Consola de la aplicación, la casilla de verificación **Considerar la tarea como análisis de áreas críticas** se muestra en las propiedades de la tarea, pero no se puede modificar.

Análisis de archivos almacenados en la nube

Acerca de los archivos en la nube

Kaspersky Embedded Systems Security 2.2 puede interactuar con archivos en la nube de Microsoft OneDrive. La aplicación admite la nueva función archivos a petición de OneDrive.

Kaspersky Embedded Systems Security 2.2 no admite otros servicios de almacenamiento en la nube.

OneDrive Files On-Demand ayuda a acceder a todos los archivos en OneDrive sin necesidad de descargarlos todos y utilizar espacio de almacenamiento en el dispositivo. Puede descargar archivos en el disco duro cuando lo necesite.

Cuando la función OneDrive Files On-Demand está activada, ve los iconos de estado junto a cada archivo en la columna **Estado** en el Explorador de archivos. Cada archivo tiene uno de los siguientes estados:

Este icono de estado indica que el archivo *solo está disponible en línea*. Los archivos que están solo en línea no se almacenan físicamente en el disco duro. No puede abrir archivos que están solo en línea cuando su dispositivo no está conectado a Internet.

Este icono de estado indica que un archivo *está disponible localmente*. Esto sucede cuando abre un archivo solo en línea y lo descarga a su dispositivo. Puede abrir un archivo disponible localmente en cualquier momento, incluso sin acceso a Internet. Para liberar espacio, puede cambiar el archivo nuevamente a solo en línea.

Este icono de estado indica que un archivo *está almacenado en el disco duro y siempre está disponible*.

Análisis de archivos en la nube

Kaspersky Embedded Systems Security 2.2 solo puede analizar archivos en la nube que están almacenados localmente en un equipo protegido. Estos archivos de OneDrive deben tener los estados y . Los archivos

se omiten durante el análisis, ya que no están ubicados físicamente en el equipo protegido.

Kaspersky Embedded Systems Security 2.2 no descarga automáticamente los archivos de la nube durante el análisis, aunque estén incluidos en el área del análisis.

Varias tareas de Kaspersky Embedded Systems Security 2.2 procesan los archivos en la nube en distintas situaciones según el tipo de tarea:

- Análisis de archivos en la nube en tiempo real: puede agregar carpetas que contienen archivos en la nube área de la tarea Protección de archivos en tiempo real. El archivo se analiza cuando el usuario accede a él. Si el usuario accede al archivo , se descarga para estar disponible localmente y su estado cambia a . Esto permite que la tarea de Protección de archivos en tiempo real procese el archivo.
- Análisis a pedido de archivos en la nube: puede agregar carpetas que contienen archivos en la nube al área de la tarea Análisis a pedido. La tarea analiza archivos con los estados y . Si se encuentra algún archivo en el área, se omitirá durante el análisis, y se registrará un evento informativo en el registro de tareas para indicar que el archivo analizado solo es un marcador de posición de un archivo en la nube y no existe en un disco local.
- Generación y uso de reglas de Control de aplicaciones: puede crear reglas de autorización y de denegación de archivos y con la tarea del Generador de reglas de control de inicio de aplicaciones. La tarea Control de inicio de aplicaciones aplica el principio de denegación predeterminada y las reglas creadas para procesar y bloquear archivos en la nube.

  La tarea Control de inicio de aplicaciones bloquea el inicio de todos los archivos en la nube más allá de su estado. Los archivos no se incluyen en el área de generación de reglas que realiza la aplicación, ya que no están presentes físicamente en un disco duro. Como no puede crearse ninguna regla para estos archivos, están sujetos al principio de denegación predeterminada.

Cuando se detecta una amenaza en un archivo de OneDrive en la nube, la aplicación realiza la acción especificada en la configuración de la tarea que lleva a cabo el análisis. De esta manera, se puede realizar una copia de seguridad del archivo, o bien se lo puede eliminar, desinfectar o mover a la cuarentena.

Los cambios en los archivos locales se sincronizan con las copias almacenadas en OneDrive de acuerdo con los principios descritos en la documentación de Microsoft OneDrive.

Configuración del diagnóstico de la interrupción en Kaspersky Security Center

Si ocurre un problema durante la operación de Kaspersky Embedded Systems Security 2.2 (por ejemplo, si se interrumpe Kaspersky Embedded Systems Security 2.2) y desea diagnosticarlo, puede habilitar la creación de archivos de rastreo y el archivo de volcado del proceso de Kaspersky Embedded Systems Security 2.2, y enviar estos archivos para su análisis al Servicio de soporte técnico de Kaspersky Lab.

Kaspersky Embedded Systems Security 2.2 no envía ningún archivo de volcado ni rastreo automáticamente. Solo los usuarios con los permisos correspondientes pueden enviar datos de diagnóstico.

Kaspersky Embedded Systems Security 2.2 escribe la información en los archivos de rastreo y el archivo de volcado de memoria en formato no cifrado. El usuario selecciona la carpeta donde se guardan los archivos, que es administrada por la configuración del sistema operativo y la configuración de Kaspersky Embedded Systems Security 2.2. Puede configurar permisos de acceso (consulte la sección "Permisos de acceso para las funciones de Kaspersky Embedded Systems Security 2.2", en la página 78) para permitir el acceso a registros, archivos de volcado y rastreo solo a usuarios requeridos.

► *Para configurar el diagnóstico de interrupciones en Kaspersky Security Center:*

1. En la Consola de administración de Kaspersky Security Center, abra la ventana **Configuración de la aplicación** (consulte la sección "**Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center**", en la página 103).
2. Abra la sección **Diagnóstico de mal funcionamiento** y realice lo siguiente:
   - Si desea que la aplicación escriba información de depuración en el archivo, seleccione la casilla de verificación **Escribir información de depuración en archivo de rastreo**.
     - En el campo a continuación, especifique la carpeta en la cual Kaspersky Embedded Systems Security 2.2 guardará los archivos de rastreo.
     - Configure el nivel de detalle de la información de depuración.

       Esta lista desplegable le permite seleccionar el nivel de detalle de la información de depuración que Kaspersky Embedded Systems Security 2.2 guarda en el archivo de rastreo.

       Puede seleccionar uno de los siguientes niveles de detalle:

       - **Eventos críticos**: Kaspersky Embedded Systems Security 2.2 guarda información únicamente sobre los eventos críticos en el archivo de rastreo.
       - **Errores**: Kaspersky Embedded Systems Security 2.2 guarda información sobre los eventos críticos y los errores en el archivo de rastreo.
       - **Eventos importantes**: Kaspersky Embedded Systems Security 2.2 guarda información sobre los eventos críticos, los errores y los eventos importantes en el archivo de rastreo.
       - **Eventos informativos**: Kaspersky Embedded Systems Security 2.2 guarda información sobre los eventos críticos, los errores, los eventos importantes y los eventos informativos en el archivo de rastreo.
       - **Toda la información de depuración**: Kaspersky Embedded Systems Security 2.2 guarda toda la información de depuración en el archivo de rastreo.

       Un representante de Soporte técnico determina el nivel de detalle que se debe establecer a fin de resolver el problema que surgió.

       El nivel predeterminado de detalle está configurado como **Toda la información de depuración**.

       La lista desplegable se encuentra disponible si está activada la casilla **Escribir información de depuración en archivo de rastreo**.
     - Especifique el tamaño máximo de los archivos de rastreo.
     - Especifique los componentes que quiere depurar. Los códigos de componentes deben estar separados con punto y coma. Los códigos distinguen entre mayúsculas y minúsculas (consulte la

tabla a continuación).

Table 27. Códigos del subsistema de Kaspersky Embedded Systems Security 2.2

Código del componente	Nombre del componente
*	Todos los componentes.
gui	Subsistema de la interfaz del usuario, complemento de Kaspersky Embedded Systems Security 2.2 en Microsoft Management Console.
ak_conn	Subsistema para integrar el Agente de red y Kaspersky Security Center.
bl	Proceso de control, implementa tareas de control de Kaspersky Embedded Systems Security 2.2.
wp	Proceso de trabajo, administra las tareas de protección antivirus.
blgate	Proceso de administración remota de Kaspersky Embedded Systems Security 2.2.
ods	Subsistema del Análisis a pedido.
oas	Subsistema de Protección de archivos en tiempo real.
qb	Subsistema de cuarentena y Copia de seguridad.
scandll	Módulo auxiliar para análisis del antivirus.
core	Subsistema para la funcionalidad de antivirus básica.
avscan	Subsistema de procesamiento del antivirus.
avserv	Subsistema para controlar el núcleo del antivirus.
prague	Subsistema para la funcionalidad básica.
updater	Subsistema para actualizar los módulos del programa y las bases de datos.
snmp	Subsistema de soporte del protocolo SNMP.
perfcount	Subsistema del contador de rendimiento.

La configuración de rastreo del complemento de Kaspersky Embedded Systems Security 2.2 (gui) y el Complemento de administración de Kaspersky Security Center (ak_conn) se aplica después de que se reinician estos componentes. La configuración de rastreo del subsistema de soporte del protocolo SNMP (snmp) se aplica después de que se reinicia el servicio SNMP. La configuración de rastreo del subsistema de contadores de rendimiento (perfcount) se aplica luego de que se reinician todos los procesos que usan contadores de rendimiento. La configuración de rastreo para otros subsistemas de Kaspersky Embedded Systems Security 2.2 se aplica tan pronto como se guarda la configuración del diagnóstico de la interrupción.

De forma predeterminada, Kaspersky Embedded Systems Security 2.2 registra la información de depuración de todos los componentes de Kaspersky Embedded Systems Security 2.2.

El campo de entrada se encuentra disponible si está activada la casilla **Escribir información de depuración en archivo de rastreo**.

- Si desea que la aplicación cree un archivo de volcado de memoria, seleccione la casilla de verificación **Crear archivo de volcado**.
  - En el campo a continuación, especifique la carpeta en la cual Kaspersky Embedded Systems Security 2.2 guardará el archivo de volcado de memoria.

3. Haga clic en **Aceptar**.

La configuración de la aplicación establecida se aplica en el equipo protegido.

Administración de programaciones de tareas

Puede configurar la programación de inicio para tareas de Kaspersky Embedded Systems Security 2.2 y establecer la configuración para ejecutar tareas según una programación.

En esta sección

Configuración de las opciones de programación de inicio de tareas

Puede configurar la programación de inicio de las tareas creadas por el usuario y del sistema local en la Consola de la aplicación. No puede configurar la programación de inicio de tareas de grupo.

► *Para configurar las opciones de programación de inicio de tareas, siga estos pasos:*

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados** y haga lo siguiente:
   - Si desea ajustar la configuración de la directiva, en el grupo de equipos seleccione **Directiva > <nombre de la directiva> > <sección> > Configurar > Administración de tareas**.
   - Si desea establecer la configuración de la aplicación para un solo equipo con Kaspersky Security Center, abra la ventana **Configuración de la tarea** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación en Kaspersky Security Center “**Configuración de tareas locales en la ventana Configuración de la aplicación en Kaspersky Security Center** " en la página 103) de Kaspersky Security Center.

     Se abre la ventana **Configuración**.
2. En la ventana que se abre, en la pestaña **Programación**, seleccione la casilla de verificación **Ejecutar según programación**.

   Los campos con la configuración de programación para la tarea Análisis a pedido y la tarea Actualización no estarán disponibles si el inicio programado está bloqueado por una directiva de Kaspersky Security Center.
3. Configure los valores de programación de acuerdo con sus requisitos. Para ello, realice las siguientes acciones:
   a. En la lista **Frecuencia**, seleccione uno de los siguientes valores:
      - **Horaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de horas; especifique el número de horas en el campo **Cada <número> hora(s)**.
      - **Diaria**, si desea que la tarea se ejecute con intervalos durante un número especificado de días; especifique el número de horas en el campo **Cada <número> día(s)**.
      - **Semanal**, si desea que la tarea se ejecute con intervalos durante un número especificado de

semanas; especifique el número de horas en el campo **Cada <número> semana(s)**. Especifique los días de la semana durante los cuales la tarea se iniciará (de manera predeterminada, las tareas se ejecutan los lunes).

- **Al inicio de la aplicación**, si desea que la tarea se ejecute cada vez que se inicia Kaspersky Embedded Systems Security 2.2.
- **Tras la actualización de bases de datos de la aplicación**, si desea que la tarea se ejecute después de cada actualización de bases de datos de la aplicación.

b. Especifique la hora del primer inicio de la tarea en el campo **Hora de inicio**.

c. En el campo **Fecha de inicio**, especifique la fecha desde la que se aplicará la programación.

Después de especificar la frecuencia de inicio de la tarea, la hora del primer inicio de esta y la fecha desde la que se aplicará la programación, la información sobre la hora calculada para el próximo inicio de la tarea se mostrará en la parte superior de la ventana en el campo **Próximo inicio**. La información actualizada sobre la hora estimada del próximo inicio de la tarea se mostrará cada vez que abra la ventana **Configuración de tareas** de la pestaña **Programación**.
El valor **Bloqueado por directiva** se muestra en el campo **Próximo inicio** si la configuración de la directiva activa de Kaspersky Security Center prohíbe el inicio de tareas programadas del sistema (consulte la sección “Configuración del inicio programado de las tareas locales del sistema”, en la página 96).

4. Use la pestaña **Avanzado** para configurar las siguientes opciones de programación de acuerdo con sus requisitos.

- En la sección **Configuración de detención de la tarea**:

  a. Seleccione la casilla de verificación **Duración** y escriba el número requerido de horas y minutos en los campos a la derecha para especificar la duración máxima de la ejecución de la tarea.

  b. Seleccione la casilla de verificación **Pausar de** y escriba los valores de inicio y de finalización del intervalo de tiempo en los campos a la derecha para especificar el intervalo de tiempo inferior a 24 horas durante el cual la ejecución de la tarea se pausará.

- En la sección **Configuración avanzada**:

  a. Seleccione la casilla de verificación **Fin de la programación** y especifique la fecha desde la cual la programación dejará de funcionar.

  b. Seleccione la casilla de verificación **Ejecutar tareas omitidas** para habilitar el inicio de las tareas omitidas.

  c. Seleccione la casilla de verificación **Aleatorizar el inicio de la tarea usando un margen de** y especifique el valor en minutos.

5. Haga clic en el botón **Aplicar** para guardar la configuración del inicio de la tarea.

Cómo habilitar y deshabilitar tareas programadas

Puede habilitar y deshabilitar tareas programadas antes o después de configurar las opciones de programación.

► *Para habilitar o deshabilitar la programación de inicio de tareas, siga estos pasos:*

1. En el árbol de la Consola de la aplicación, abra el menú contextual del nombre de la tarea para la cual desea configurar la programación de inicio.

2. Seleccione **Propiedades**.

   Se abre la ventana **Configuración de tareas**.

3. En la ventana que se abre en la pestaña **Programación**, realice una de las siguientes acciones:

   - Seleccione la casilla de verificación **Ejecutar según programación** si desea habilitar el inicio programado de la tarea.
   - Cancela la selección de la casilla de verificación **Ejecutar según programación** si desea deshabilitar el inicio programado de la tarea.

   > Las opciones de programación del inicio de la tarea configuradas no se eliminan y se aplicarán en el siguiente inicio programado de la tarea.

4. Haga clic en el botón **Aplicar**.

Se guardan las opciones de programación de inicio de la tarea configuradas.

Administración de las configuraciones de la aplicación

Esta sección contiene información acerca de cómo ajustar las configuraciones generales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center.

En este capítulo

Administración de Kaspersky Embedded Systems Security 2.2 mediante Kaspersky Security Center

Puede administrar centralmente varios equipos si Kaspersky Embedded Systems Security 2.2 está instalado e incluido en un grupo de administración por medio del complemento de administración de Kaspersky Embedded Systems Security 2.2. Kaspersky Security Center también le permite ajustar, por separado, los parámetros de configuración de operación de cada equipo incluido en el grupo de administración.

El *grupo de administración* se crea en Kaspersky Security Center manualmente e incluye varios equipos con Kaspersky Embedded Systems Security 2.2 instalado, para los cuales es conveniente configurar las mismas opciones de control y protección. Para obtener más información sobre la utilización de grupos de administración, consulte la *Ayuda de Kaspersky Security Center*.

La configuración de la aplicación para un equipo no está disponible si el funcionamiento de Kaspersky Embedded Systems Security 2.2 en ese equipo es controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Embedded Systems Security 2.2 puede administrarse desde Kaspersky Security Center de las siguientes maneras:

- **Utilización de directivas de Kaspersky Security Center**. Es posible usar directivas de Kaspersky Security Center para configurar remotamente la misma configuración de protección para un grupo de equipos. La configuración de la tarea especificada en la directiva activa tiene prioridad sobre las opciones de la tarea configuradas localmente en la Consola de la aplicación o remotamente en la ventana **Propiedades: <Nombre del equipo>** de Kaspersky Security Center.

  Puede usar directivas para establecer la configuración general de la aplicación, la configuración de la tarea Protección en tiempo real, la configuración de las tareas de control de actividad local, la configuración del inicio de las tareas del sistema programadas y la configuración de uso del perfil.

- **Utilización de tareas de grupo de Kaspersky Security Center**. Las tareas de grupo de Kaspersky Security Center permiten la configuración remota de las opciones comunes de las tareas con un periodo de vencimiento para un grupo de equipos.

- Puede usar tareas de grupo para activar la aplicación, configurar la tarea de Análisis a pedido, actualizar la configuración de tareas y configurar la tarea de Generador de reglas de control de inicio de aplicaciones.
- **Utilización de tareas para un conjunto de dispositivos**. Las tareas para un conjunto de dispositivos permiten la configuración remota de las opciones comunes de las tareas con un periodo de ejecución limitado para equipos que no pertenecen a ninguno de los grupos de administración.
- **Utilización de la ventana Propiedades de un solo equipo**. En la ventana **Propiedades: <Nombre del equipo>** puede configurar remotamente las opciones de tareas para un solo equipo incluido en el grupo de administración.
  Puede establecer tanto la configuración general de la aplicación como la configuración de todas las tareas de Kaspersky Embedded Systems Security 2.2 si el equipo seleccionado no es controlado por una directiva de Kaspersky Security Center activa.

Kaspersky Security Center hace posible configurar los parámetros de la aplicación y las funciones avanzadas, y le permite trabajar con registros y notificaciones. Puede configurar estos parámetros para un grupo de equipos, así como para un equipo particular.

Configuración de las opciones generales de la aplicación en Kaspersky Security Center

Puede establecer la configuración general de Kaspersky Embedded Systems Security 2.2 desde Kaspersky Security Center para un grupo de equipos o para un equipo.

En esta sección

Configuración de escalabilidad y de la interfaz en Kaspersky Security Center

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

► *Para establecer la configuración de escalabilidad y de la interfaz de la aplicación, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección

"Configuración de directivas", en la página 91).

- Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

> Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Configuración de la aplicación**, en el bloque **Escalabilidad e interfaz**, haga clic en **Configuración**.
4. En la ventana **Escalabilidad e interfaz** en la pestaña **General**, establezca la configuración siguiente:
   - En la sección **Configuración de escalabilidad**, establezca la configuración que define el número de procesos usados por Kaspersky Embedded Systems Security 2.2:
     - **Detectar automáticamente la configuración de escalabilidad**.

       Kaspersky Embedded Systems Security 2.2 regula automáticamente el número de procesos usados.
     - **Configurar manualmente el número de procesos de trabajo**.

       Kaspersky Embedded Systems Security 2.2 regula la cantidad de procesos en funcionamiento activos según los valores especificados.

       Este es el valor predeterminado.
       - **Número máximo de procesos activos.**

         Número máximo de procesos que utiliza Kaspersky Embedded Systems Security 2.2. El campo de entrada se encuentra disponible si se selecciona la opción **Configurar manualmente el número de procesos de trabajo**.
       - **Número de procesos para la protección en tiempo real.**

         Número máximo de procesos usados por los componentes de la tarea Protección en tiempo real. El campo de entrada se encuentra disponible si se selecciona la opción **Configurar manualmente el número de procesos de trabajo**.
       - **Número de procesos para tareas de Análisis a pedido en segundo plano.**

         Número máximo de procesos usados por el componente de Análisis a pedido al ejecutar tareas de Análisis a pedido en segundo plano. El campo de entrada se encuentra disponible si se selecciona la opción **Configurar manualmente el número de procesos de trabajo**.

   > En la sección **Interacción con el usuario**, configure la visualización del icono de la bandeja del sistema en el área de notificación: seleccione o desactive la casilla de verificación **Mostrar icono de bandeja de sistema en la barra de tareas**.

5. Haga clic en **Aceptar**.

Se guarda la configuración de la aplicación.

Configuración de opciones de seguridad en Kaspersky Security Center

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

► *Para configurar los valores de seguridad manualmente, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Configuración de la aplicación**, haga clic en el botón **Configurar** en **Seguridad y fiabilidad**.
4. En la ventana **Configuración de seguridad**, configure las siguientes opciones:
   - En la sección **Configuración de confiabilidad**, establezca la configuración de la recuperación de las tareas de Kaspersky Embedded Systems Security 2.2 cuando la aplicación devuelva un error o deje de funcionar.
     - **Ejecutar recuperación de tarea**

       Esta casilla de verificación habilita o deshabilita la recuperación de las tareas de Kaspersky Embedded Systems Security 2.2 cuando la aplicación devuelve un error o deja de funcionar.

       Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 recupera automáticamente las tareas de Kaspersky Embedded Systems Security 2.2 cuando la aplicación devuelve un error o deja de funcionar.

       Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 no recupera las tareas de Kaspersky Embedded Systems Security 2.2 cuando la aplicación devuelve un error o deja de funcionar.

       De forma predeterminada, la casilla está activada.
     - **Recuperar tareas de análisis a pedido no más de (veces)**

       Número de intentos para recuperar una tarea Análisis a pedido después de que Kaspersky Embedded Systems Security 2.2 devuelve un error. El campo de entrada se encuentra disponible si se activa la casilla **Ejecutar recuperación de tarea**.

- En la sección **Acciones si se pasa a un sistema de alimentación de respaldo (UPS)**, especifique limitaciones de la carga del equipo creadas por Kaspersky Embedded Systems Security 2.2 después de cambiar a la alimentación de UPS:
  - **No iniciar las tareas de análisis programado**

    Esta casilla de verificación habilita o deshabilita el inicio de una tarea de análisis programado después de que el equipo cambia a una fuente de UPS hasta que el modo de suministro de energía estándar se restaura.

    Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 no inicia tareas de análisis programado después de que el equipo cambia a una fuente de UPS hasta que el modo de suministro de energía estándar se restaura.

    Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 inicia tareas de análisis programado sin tener en cuenta el modo de suministro de energía.

    De forma predeterminada, la casilla está activada.
  - **Detener las tareas de análisis en curso**

    La casilla de verificación habilita o deshabilita la ejecución de tareas de análisis en ejecución después de que el equipo cambia a una fuente de UPS.

    Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 pausa las tareas de análisis en ejecución después de que el equipo cambia a una fuente de UPS.

    Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 continúa las tareas de análisis en ejecución después de que el equipo cambia a una fuente de UPS.

    De forma predeterminada, la casilla está activada.

  El equipo cambia a la alimentación de UPS solo si el nivel de carga de la batería cae por debajo del 90%.
- En la sección **Configuración de protección con contraseña**, establezca una contraseña para proteger el acceso a las funciones de Kaspersky Embedded Systems Security 2.2.

5. Haga clic en **Aceptar**.

Se guarda la configuración establecida de escalabilidad y de confiabilidad.

Configuración de opciones de conexión mediante Kaspersky Security Center

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

Los parámetros de conexión configurados se utilizan para conectar Kaspersky Embedded Systems Security 2.2 a servidores de activación y actualización durante la integración de aplicaciones con Servicios KSN.

► *Para configurar los parámetros de conexión, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Configuración de la aplicación**, haga clic en el botón **Configurar** en el bloque **Servidor proxy**.

   Se abrirá la ventana **Configuración de conexión**.
4. En la ventana **Configuración de conexión**, configure las siguientes opciones:
   - En la sección **Configuración del servidor proxy**, seleccione la configuración de uso del servidor proxy:
     - **No usar un servidor proxy**.

       Si esta opción está seleccionada, Kaspersky Embedded Systems Security 2.2 se conecta a Servicios KSN directamente, sin usar ningún servidor proxy.
     - **Detectar automáticamente la configuración del servidor proxy**.

       Si esta opción está seleccionada, Kaspersky Embedded Systems Security 2.2 define automáticamente la configuración para la conexión con los Servicios KSN con el protocolo de detección automática de proxy web (WPAD).

       De forma predeterminada, esta opción está seleccionada.
     - **Usar la configuración especificada del servidor proxy**.

       Si esta opción está seleccionada, Kaspersky Embedded Systems Security 2.2 se conecta al KSN con la configuración del servidor proxy especificada manualmente.
     - La dirección IP o el nombre del símbolo del servidor proxy y el número de puerto.
     - **No usar el servidor proxy para las direcciones locales**.

       La casilla de verificación habilita o deshabilita el uso de un servidor proxy al acceder a equipos ubicados en la misma red que el equipo con Kaspersky Embedded Systems Security 2.2 instalado.

       Si esta casilla de verificación está seleccionada, se accede a los equipos directamente desde la red, que aloja el equipo con Kaspersky Embedded Systems Security 2.2 instalado. No se utiliza ningún servidor proxy.

       Si la casilla de verificación está desactivada, se aplica el servidor proxy para la conexión a equipos locales.

       De forma predeterminada, la casilla está activada.

- En la sección **Configuración de autenticación del servidor proxy**, especifique la configuración de autenticación:
  - Seleccione la configuración de autenticación en la lista desplegable.
    - **No usar autenticación**: no se realiza la autenticación. Este modo está seleccionado en forma predeterminada.
    - **Usar autenticación NTLM**: la autenticación se realiza usando el protocolo de autenticación de red NTLM desarrollado por Microsoft.
    - **Usar autenticación NTLM con nombre de usuario y contraseña**: la autenticación se realiza usando el nombre y la contraseña a través del protocolo de autenticación de red NTLM desarrollado por Microsoft.
    - **Aplicar nombre de usuario y contraseña**: la autenticación se realiza usando el nombre de usuario y contraseña.
  - Escriba el nombre de usuario y la contraseña, de ser necesario.
- En el bloque **Licencia**, desactive o seleccione **Usar Kaspersky Security Center como servidor proxy al activar la aplicación**.

5. Haga clic en **Aceptar**.

Los parámetros de conexión configurados se guardan.

Configuración de funciones avanzadas

Puede establecer la configuración de las funciones avanzadas de Kaspersky Embedded Systems Security 2.2 desde Kaspersky Security Center para un grupo de equipos o para un solo equipo.

En esta sección

Configuración de los parámetros de la Zona de confianza en Kaspersky Security Center

De manera predeterminada, la Zona de confianza se aplica en tareas y directivas recientemente creadas.

► *Para establecer la configuración de la Zona de confianza:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Adicional**, haga clic en el botón **Configurar** en el bloque **Zona de confianza**.

   Se abre la ventana **Zona de confianza**.
4. En la pestaña **Exclusiones**, especifique los objetos que debe omitir Kaspersky Embedded Systems Security 2.2 durante el análisis:
   - Para crear exclusiones recomendadas, haga clic en el botón **Agregar exclusiones recomendadas**.

     Si hace clic en este botón, podrá ampliar la lista de exclusiones al agregar exclusiones recomendadas por Microsoft y exclusiones recomendadas por Kaspersky Lab.
   - Para importar exclusiones, haga clic en el botón **Importar** y, en la ventana que se abre, seleccione los archivos que Kaspersky Embedded Systems Security 2.2 considerará de confianza.
   - Para especificar manualmente las condiciones en las cuales un archivo se considerará de confianza, haga clic en el botón **Agregar**. En la ventana que se abre, especifique la siguiente configuración:
     - **Objeto para analizar**

       Agrega un archivo, carpeta, unidad o archivo de script a una exclusión.

       Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 omite el área, el archivo, la carpeta, la unidad o el archivo de script predefinido especificado al ejecutar el análisis con el uso del componente de Kaspersky Embedded Systems Security 2.2 seleccionado en la sección **Área de aplicación de exclusión**.

       De forma predeterminada, la casilla está activada.
     - **Objetos que detectar**

       Los objetos se excluyen del análisis por el nombre o la máscara del nombre del objeto detectable. La lista de nombres de objetos detectables está disponible en el sitio web de la Enciclopedia de Virus.

       Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 omite los objetos especificados detectables durante el análisis.

Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 detecta todos los objetos especificados en la aplicación de forma predeterminada.

De forma predeterminada, la casilla está desactivada.

- **Área de aplicación de exclusión**

  El nombre de la tarea de Kaspersky Embedded Systems Security 2.2 en la cual se utiliza la regla.

- Si es necesario, especifique información adicional que explique la exclusión en el campo **Comentario**.

5. En la ventana **Zona de confianza** en la pestaña **Procesos de confianza**, especifique los procesos que Kaspersky Embedded Systems Security 2.2 omitirá durante el análisis:

   - **No analizar las operaciones de copia de seguridad de archivos**

     La casilla de verificación habilita o deshabilita el análisis de operaciones de lectura de archivos si dichas operaciones son realizadas por las herramientas de Copia de seguridad instaladas en el equipo.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 omite las operaciones de lectura de archivos realizadas por las herramientas de Copia de seguridad instaladas en el equipo.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 analiza las operaciones de lectura de archivos realizadas por las herramientas de Copia de seguridad instaladas en el equipo.

     De forma predeterminada, la casilla está activada.

   - **No analizar la actividad de archivos de los procesos especificados**

     La casilla de verificación habilita o deshabilita el análisis de la actividad de archivos de procesos de confianza.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 omite las operaciones de los procesos de confianza durante el análisis.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 analiza las operaciones de archivos de procesos de confianza.

     De forma predeterminada, la casilla está desactivada.

6. Si es necesario, agregue procesos cuya actividad de archivos no desea analizar (consulte la Sección “Cómo agregar procesos de confianza”, en la página 135) haciendo clic en el botón **Agregar**.

7. Haga clic en **Aceptar** en la ventana **Zona de confianza** para guardar los cambios.

Cómo agregar procesos de confianza

► *Para agregar uno o varios procesos a la lista de procesos de confianza:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Adicional**, haga clic en el botón **Configurar** en el bloque **Zona de confianza**.

   Se abre la ventana **Zona de confianza**.
4. En la pestaña **Procesos de confianza**, seleccione la casilla de verificación **No analizar la actividad de archivos de los procesos especificados**.
5. Haga clic en el botón **Agregar**.
6. Desde el menú contextual del botón, seleccione una de las opciones:
   - **Varios procesos**.

     En la ventana **Adición de procesos de confianza** que se abre, configure lo siguiente:

     a. **Utilizar la ruta de acceso completa del proceso del disco para que se considere de confianza**.

        Si la casilla se selecciona, Kaspersky Embedded Systems Security 2.2 usará la ruta de acceso completa al archivo para determinar el estado de confianza del proceso.

        Si se cancela la selección de la casilla de verificación, la ruta de acceso al archivo no se considera como criterio para determinar el estado de confianza del proceso.

        De forma predeterminada, la casilla está activada.

     b. **Usar el hash del archivo del proceso para considerarlo de confianza**.

        Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security 2.2 usará el hash del archivo seleccionado para determinar el estado de confianza del proceso.

        Si se cancela la selección de la casilla de verificación, el hash del archivo no se considerará como criterio para determinar el estado de confianza del proceso.

        De forma predeterminada, la casilla está activada.

     c. Haga clic en el botón **Examinar** para agregar datos basados en procesos ejecutables.

d. Seleccione un archivo ejecutable en la ventana que se abre.

> Solo puede agregar un archivo ejecutable a la vez. Repita los pasos c y d para agregar otros archivos ejecutables.

e. Haga clic en el botón **Procesos** para agregar datos basados en procesos en ejecución.

f. Seleccione los procesos en la ventana que se abre. Para seleccionar varios procesos, mantenga presionado el botón **CTRL** al realizar la selección.

g. Haga clic en **Aceptar**.

> Se requiere que la cuenta desde la que se ejecuta la tarea de Protección de archivos en tiempo real cuente con los derechos de administrador en el equipo con Kaspersky Embedded Systems Security 2.2 instalado con el fin de autorizar la visualización de la lista de procesos activos. Se pueden ordenar los procesos en la lista de procesos activos por nombre de archivo, Id. de proceso (PID) o ruta de acceso al archivo ejecutable del proceso en el equipo local. Tenga en cuenta que para seleccionar los procesos en ejecución debe hacer clic en el botón **Procesos** usando solo la Consola de la aplicación en un equipo local o en la configuración de host especificada mediante Kaspersky Security Center.

- **Un proceso basado en el nombre y la ruta de acceso.**

  En la ventana **Agregar proceso de confianza manualmente** que se abre, configure lo siguiente:

  a. Escriba una ruta de acceso al archivo ejecutable (incluido el nombre de archivo).

  b. Haga clic en **Aceptar**.

- **Un proceso basado en las propiedades del objeto.**

  En la ventana **Agregar proceso de confianza** que se abre, configure lo siguiente:

  a. Haga clic en el botón **Examinar** y seleccione un proceso.

  b. **Utilizar la ruta de acceso completa del proceso del disco para que se considere de confianza**.

     Si la casilla se selecciona, Kaspersky Embedded Systems Security 2.2 usará la ruta de acceso completa al archivo para determinar el estado de confianza del proceso.

     Si se cancela la selección de la casilla de verificación, la ruta de acceso al archivo no se considera como criterio para determinar el estado de confianza del proceso.

     De forma predeterminada, la casilla está activada.

  c. **Usar el hash del archivo del proceso para considerarlo de confianza**.

     Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security 2.2 usará el hash del archivo seleccionado para determinar el estado de confianza del proceso.

     Si se cancela la selección de la casilla de verificación, el hash del archivo no se considerará como criterio para determinar el estado de confianza del proceso.

     De forma predeterminada, la casilla está activada.

  d. Haga clic en **Aceptar**.

> Para agregar el proceso seleccionado a la lista de procesos de confianza, debe seleccionarse al menos un criterio de confianza.

7. En la ventana **Agregar proceso de confianza**, haga clic en el botón **Aceptar**.

El proceso o archivo seleccionado se agregará a la lista de procesos de confianza en la ventana **Zona de confianza**.

Aplicación de la máscara “no es un virus”

La máscara “no es un virus” permite omitir archivos de software y recursos web legítimos que pueden considerarse dañinos durante el análisis. La máscara afecta las siguientes tareas:

- Protección de archivos en tiempo real.
- Análisis a pedido.

Si no se agrega la máscara a la lista de exclusiones, Kaspersky Embedded Systems Security 2.2 aplicará las acciones especificadas en la configuración de la tarea al software o los recursos web que se consideran en esta categoría.

► *Para aplicar la máscara “no es un virus”:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

   > Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Adicional**, haga clic en el botón **Configurar** en el bloque **Zona de confianza**.

   Se abre la ventana **Zona de confianza**.
4. En la pestaña **Exclusiones**, desplácese hasta la lista y seleccione la línea con el valor **no es un virus:*** valor, si la casilla de verificación está marcada.
5. Haga clic en **Aceptar**.

Se aplica la nueva configuración.

Análisis de unidades extraíbles

Puede configurar el análisis de discos extraíbles conectados al equipo protegido mediante el puerto USB.

Kaspersky Embedded Systems Security 2.2 analiza una unidad extraíble mediante la tarea Análisis a pedido. La aplicación crea automáticamente una nueva tarea de Análisis a pedido cuando la unidad extraíble está conectada y la suprime después de que se completa el análisis. La tarea creada se realiza con el nivel de seguridad predefinido determinado para el análisis de la unidad extraíble. No puede configurar los valores de la tarea temporal de Análisis a pedido.

Los análisis de Kaspersky Embedded Systems Security 2.2 conectaron discos USB extraíbles cuando se registran como dispositivos de almacenamiento USB en el sistema operativo. La aplicación no analiza una unidad extraíble si la conexión está bloqueada por la tarea Control de dispositivos. La aplicación no analiza dispositivos móviles conectados a MTP.

Kaspersky Embedded Systems Security 2.2 permite el acceso a unidades extraíbles durante el análisis.

Los resultados de análisis para cada unidad extraíble están disponibles en el registro para la tarea Análisis a pedido creada al conectar la unidad extraíble.

Puede cambiar las configuraciones predeterminadas de la tarea Monitor de Integridad de archivos (consulte la tabla a continuación).

Table 28. Configuración de Análisis de unidades extraíbles

Configuración	Valor predeterminado	Descripción
Analizar unidades extraíbles al conectar via USB	La casilla se desactiva.	Puede activar o desactivar el análisis de las unidades extraíbles después de conectarlas al equipo protegido por USB.
Analizar las unidades extraíbles si el volumen de los datos almacenados no excede (MB):	1024 MB	Puede reducir el área del componente si configura el volumen máximo de datos del disco analizado. Kaspersky Embedded Systems Security 2.2 no realiza análisis de unidades extraíbles si el volumen de los datos almacenados excede el valor especificado.
Analizar con nivel de seguridad	Máxima protección	Puede configurar las tareas creadas de Análisis a pedido a través de uno de los tres niveles de seguridad: • Máxima protección • Recomendado • Máximo rendimiento El algoritmo usado cuando se detectaron objetos infectados, posiblemente infectados y otros objetos, así como otras configuraciones de análisis para cada nivel de seguridad, equivalen a los niveles de seguridad predefinidos en las tareas Análisis a pedido.

► *Para configurar el análisis de unidades extraíbles al conectarlas, realice las siguientes acciones:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky

Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.

2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

   > Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Adicional**, haga clic en **Configuración** en el bloque **Análisis de unidades extraíbles**.

   Se abre la ventana **Análisis de unidades extraíbles**.

4. En la sección **Analizar al conectar**, realice las siguientes acciones:

   - Seleccione la casilla de verificación **Analizar unidades extraíbles al conectar via USB** si desea que Kaspersky Embedded Systems Security 2.2 analice automáticamente las unidades extraíbles cuando se conectan.
   - De ser necesario, seleccione **Analizar las unidades extraíbles si el volumen de los datos almacenados no excede (MB)** y especifique el valor máximo en el campo de la derecha.
   - En la lista desplegable **Analizar con nivel de seguridad**, especifique el nivel de seguridad con la configuración necesaria para el análisis de las unidades extraíbles.

5. Haga clic en **Aceptar**.

   La configuración especificada se guarda y se aplica.

Configuración de permisos de acceso en Kaspersky Security Center

Puede configurar permisos de acceso para administrar la aplicación y el servicio de Kaspersky Security en Kaspersky Security Center para un grupo de equipos o para un equipo independiente.

> El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

► *Para acceder a permisos para administrar la aplicación y el servicio de Kaspersky Security:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:

   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección

"Configuración de directivas", en la página 91).

- Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

  Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. Abra la sección **Adicional** y realice lo siguiente:
   - Para configurar permisos de acceso para administrar Kaspersky Embedded Systems Security 2.2 para un usuario o un grupo de usuarios, en la sección **Permisos de acceso de usuario para administrar la aplicación**, haga clic en el botón **Configurar**.
   - Para configurar permisos de acceso para administrar el servicio de Kaspersky Security para un usuario o un grupo de usuarios, en la sección **Permiso de acceso del usuario para la administración del servicio de Security**, haga clic en el botón **Configurar**.
4. En la ventana que se abre, configure los privilegios de acceso (consulte la sección "Permisos de acceso para las funciones de Kaspersky Embedded Systems Security 2.2"en la página 78) según sus necesidades.

Se guarda la configuración especificada.

Configuración de opciones de Cuarentena y Copia de seguridad en Kaspersky Security Center

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

► *Para establecer la configuración general de Copia de seguridad en Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

> Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Adicional**, haga clic en el botón **Configurar** del bloque **Depósitos**.
4. Use la pestaña **Copia de seguridad** de la ventana de configuración de **Depósitos** para configurar las siguientes opciones de **Copia de seguridad**:
   - Para especificar la **Carpeta de Copia de seguridad**, utilice el campo **Carpeta de Copia de seguridad** para seleccionar la carpeta requerida en la unidad local del equipo protegido o introduzca la ruta de acceso completa.
   - Para establecer el tamaño máximo de **Copia de seguridad**, seleccione la casilla de verificación **Tamaño máx. de copia de seguridad (MB)** y especifique el valor necesario en megabytes en el campo de entrada.
   - Para establecer el valor umbral de espacio libre en Copia de seguridad, defina el valor de la opción **Tamaño máx. de copia de seguridad (MB)**, seleccione la casilla de verificación **Valor umbral de espacio disponible (MB)** y especifique el valor mínimo de espacio libre en la carpeta de **Copia de seguridad** en megabytes.
   - Para especificar una carpeta para objetos restaurados, seleccione la carpeta correspondiente en la unidad local del equipo protegido en la sección Configuración de restauración o introduzca el nombre de la carpeta y su ruta completa en el campo **Carpeta de destino para restaurar objetos**.
5. En la ventana de configuración de **Depósitos** de la pestaña **Cuarentena**, configure las siguientes opciones de **Cuarentena**:
   - Para cambiar la carpeta de **Cuarentena**, en el campo de entrada de la carpeta **Cuarentena** especifique la ruta de acceso completa de la carpeta en el disco local del equipo protegido.
   - Para establecer el tamaño máximo de **Cuarentena**, seleccione la casilla de verificación **Tamaño máximo de cuarentena (MB)** y especifique el valor de este parámetro en megabytes en el campo de entrada.
   - Para establecer la cantidad mínima de espacio libre en la **Cuarentena**, seleccione la casilla de verificación **Tamaño máximo de cuarentena (MB)**, la casilla de verificación **Valor umbral de espacio disponible (MB)** y, a continuación, especifique el valor de este parámetro en megabytes en el campo de entrada.
   - Para cambiar la carpeta de almacenamiento de los objetos restaurados de la cuarentena, en el campo de entrada **Carpeta de destino para restaurar objetos**, especifique la ruta completa de la carpeta en el disco local del equipo protegido.
6. Haga clic en **Aceptar**.

Los parámetros configurados de la Cuarentena y las Copia de seguridad se guardan.

Configuración de registros y notificaciones

La consola de administración de Kaspersky Security Center se puede usar para configurar las notificaciones para el administrador y los usuarios sobre los eventos futuros relacionados con Kaspersky Embedded Systems Security 2.2 y el estado de la protección antivirus en el equipo protegido:

- El administrador puede recibir información sobre eventos de tipos seleccionados.
- Los usuarios de la LAN que tienen acceso al equipo protegido y los usuarios del equipo de terminales pueden recibir información sobre eventos del tipo *Objeto detectado*.

Es posible configurar notificaciones sobre eventos de Kaspersky Embedded Systems Security 2.2 para un solo equipo en la ventana **Propiedades: <Nombre del equipo>** del equipo seleccionado, o para un grupo de equipos en la ventana **Propiedades: <Nombre de directiva>** del grupo de administración seleccionado.

En la pestaña **Eventos** o en la ventana **Configuración de notificaciones**, puede configurar los siguientes tipos de notificaciones:

- Las notificaciones para el administrador sobre eventos de tipos seleccionados se pueden configurar mediante la pestaña **Eventos** (la pestaña estándar de la aplicación Kaspersky Security Center). Para obtener más información sobre los métodos de notificación, consulte la *Ayuda de Kaspersky Security Center*.
- Las notificaciones para el administrador y para los usuarios se pueden configurar en la ventana **Configuración de notificaciones**.

  El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

Puede configurar notificaciones para algunos tipos de eventos en la ventana o en la pestaña solamente; y puede usar tanto la ventana como la pestaña para configurar notificaciones para otros tipos de eventos.

Si configuran las notificaciones sobre eventos del mismo tipo usando el mismo modo en la pestaña **Eventos** y en la ventana **Configuración de notificaciones**, el administrador del sistema recibirá las notificaciones de esos eventos dos veces pero en el mismo modo.

En esta sección

Configuración del registro

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

► *Para configurar los registros de Kaspersky Embedded Systems Security 2.2, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** en el bloque **Registros de tareas**.
4. En la ventana **Configuración de registros**, defina la siguiente configuración de Kaspersky Embedded Systems Security 2.2 según sus requisitos:
   - Configure el nivel de detalle de los eventos en los registros. Para ello, realice las siguientes acciones:
     a. En la lista **Componente**, seleccione el componente de Kaspersky Embedded Systems Security 2.2 para el cual desea configurar el nivel de detalle.
     b. Para definir el nivel de detalle en los registros de tareas y el registro de auditoría del sistema para el componente seleccionado, elija el nivel necesario en **Nivel de importancia**.
   - Para cambiar la ubicación predeterminada de los registros, especifique la ruta completa a la carpeta o haga clic en el botón **Examinar** para seleccionarla.
   - Especifique durante cuantos días se almacenarán los registros de tareas.
   - Especifique la cantidad de días que la información que se muestra en el nodo **Registro de auditoría del sistema** se almacenará.
5. Haga clic en **Aceptar**.

Los parámetros de registro configurados se guardaron.

Registro de seguridad

Kaspersky Embedded Systems Security 2.2 mantiene un registro de eventos asociados con la violación de la

seguridad o los intentos de violación de la seguridad en el equipo protegido. Los siguientes eventos se incluyen en este registro:

- Eventos de Prevención de exploits.
- Eventos de inspección de registros críticos
- Los eventos críticos que indican un intento de violación de la seguridad (para la Protección del equipo en tiempo real, el Análisis a pedido, el Monitor de integridad de archivos, el Control de inicio de aplicaciones y las tareas de Control de dispositivos).

Puede borrar el registro de seguridad y el registro de auditoría del sistema. Además, Kaspersky Embedded Systems Security 2.2 registra eventos de auditoría del sistema relacionados con el borrado del registro de seguridad.

Configuración de las opciones de integración de SIEM

Para reducir la carga en dispositivos de rendimiento reducido y reducir el riesgo de la degradación del sistema a consecuencia de volúmenes aumentados de registros de la aplicación, puede configurar la publicación de eventos de auditoría y eventos de rendimiento de la tarea en el *servidor syslog* mediante el protocolo Syslog.

Un servidor syslog es un servidor externo para agregar eventos (SIEM). Obtiene y analiza eventos recibidos y también realiza otras acciones para administrar registros.

Puede usar la integración de SIEM en dos modos:

- Duplicar eventos en el servidor syslog: este modo indica que todos los eventos de rendimiento de la tarea cuya publicación se configura en la configuración de registros, así como todos los eventos de auditoría del sistema, continúen almacenándose en el equipo local hasta después de que se envíen a SIEM.

  Se recomienda usar este modo para reducir máximamente la carga en el equipo protegido.

- Eliminar copias locales de eventos: este modo indica que todos los eventos que se registran durante el funcionamiento de la aplicación y se publican en SIEM se eliminen del equipo local.

  > La aplicación nunca elimina las versiones locales del registro de seguridad.

Kaspersky Embedded Systems Security 2.2 puede convertir los eventos en los registros de la aplicación a formatos admitidos por el servidor syslog, para que dichos eventos se puedan transmitir y sean reconocidos de manera exitosa por SIEM. La aplicación admite la conversión al formato de datos estructurado y al formato JSON.

Para reducir el riesgo de transmisión no exitosa de eventos a SIEM, puede definir la configuración para conectar al espejo syslog idéntico.

El servidor syslog idéntico es un servidor syslog adicional al cual la aplicación cambia automáticamente si la conexión con el servidor syslog principal no está disponible o si el servidor principal no se puede utilizar.

De forma predeterminada, la integración de SIEM no se usa. Puede habilitar y deshabilitar la integración de SIEM y configurar las opciones de funcionalidad (consulte la tabla a continuación).

Table 29. Configuración de integración de SIEM

Configuración	Valor predeterminado	Descripción

Configuración	Valor predeterminado	Descripción
Enviar eventos a un servidor remoto de Syslog, mediante un protocolo de Syslog	No aplicado	Puede habilitar o deshabilitar la integración de SIEM al seleccionar o al desactivar la casilla, respectivamente.
Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog	No aplicado	Puede ajustar la configuración para almacenar copias locales de registros después de que se envíen a SIEM al seleccionar o al desactivar la casilla.
Formato de los eventos	Datos estructurados	Puede seleccionar uno de dos formatos a los cuales la aplicación convierte sus eventos antes de enviarlos al servidor syslog para el mejor reconocimiento de estos eventos por SIEM.
Protocolo de conexión	TCP	Puede usar la lista desplegable para configurar la conexión con el servidor syslog principal mediante protocolos TCP o UDP; o con el servidor syslog idéntico mediante el protocolo TCP.
Configuración de conexión al servidor syslog principal	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor syslog principal. Puede especificar la dirección IP solo en el formato IPv4.
Utilizar el servidor reflejado de Syslog si no es posible acceder al servidor principal	No aplicado	Puede usar la casilla para habilitar o deshabilitar el uso de un servidor syslog idéntico.
Configuración de conexión al servidor syslog idéntico	Dirección IP: 127.0.0.1 Puerto: 514	Puede usar los campos apropiados para configurar la dirección IP y el puerto usados para conectarse al servidor syslog principal. Puede especificar la dirección IP solo en el formato IPv4.

► *Para configurar la integración de SIEM:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** en el bloque **Registros de tareas**.

   Se abre la ventana **Configuración de registros y notificaciones**.

4. Seleccione la pestaña **Integración de SIEM**.

5. En la sección **Configuraciones de integración**, seleccione la casilla **Enviar eventos a un servidor remoto de Syslog, mediante un protocolo de Syslog**.

   La casilla habilita o deshabilita la funcionalidad para enviar eventos publicados a un servidor syslog externo.

   Si la casilla se selecciona, la aplicación envía eventos publicados a SIEM según la configuración de integración de SIEM establecida.

   Si la casilla se desactiva, la aplicación no realiza la integración de SIEM. No puede ajustar la configuración de integración de SIEM si la casilla se desactiva.

   De forma predeterminada, la casilla está desactivada.

6. Si es necesario, en la sección **Configuraciones de integración**, seleccione la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog**.

   La casilla habilita o deshabilita la eliminación de copias locales de registros cuando se envían a SIEM.

   Si la casilla se selecciona, la aplicación elimina las copias locales de eventos después de que se han publicado correctamente en SIEM. Este modo se recomienda en equipos de rendimiento reducido.

   Si la casilla se desactiva, la aplicación solo envía eventos a SIEM. Las copias de los de registros continúan almacenándose a nivel local.

   De forma predeterminada, la casilla está desactivada.

   El estado de la casilla **Eliminar las copias locales de los eventos que se enviaron a un servidor remoto de Syslog** no afecta la configuración para almacenar eventos del registro de seguridad: la aplicación nunca elimina automáticamente eventos del registro de seguridad.

7. En la sección **Formato de los eventos**, especifique el formato al cual desea convertir los eventos operativos de la aplicación de modo que se puedan enviar a SIEM.

   De forma predeterminada, la aplicación los convierte en el formato de datos estructurado.

8. En la sección **Configuración de conexión**:

   - Especifique el protocolo de conexión de SIEM.
   - Especifique la configuración para conectarse al servidor syslog principal.

     Puede especificar una dirección IP en formato IPv4 únicamente.
   - Si es necesario, seleccione la casilla **Utilizar el servidor reflejado de Syslog si no es posible acceder al servidor principal** si desea que la aplicación use otra configuración de conexión cuando sea incapaz de enviar eventos al servidor syslog principal.
     - Especifique la siguiente configuración para conectarse al servidor syslog idéntico: **Dirección IP** y **Puerto**.

       Los campos **Dirección IP** y **Puerto** para el servidor syslog idéntico no se pueden modificar si se desactiva la casilla **Utilizar el servidor reflejado de Syslog si no es posible acceder al servidor principal**.

       Puede especificar una dirección IP en formato IPv4 únicamente.

9. Haga clic en **Aceptar**.

La configuración de integración de SIEM establecida se aplicará.

Configuración de las opciones de notificación

► *Para configurar las notificaciones de Kaspersky Embedded Systems Security 2.2, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** en el bloque **Notificaciones de eventos**.
4. En la ventana **Configuración de notificaciones**, defina la siguiente configuración de Kaspersky Embedded Systems Security 2.2 según sus requisitos:
   - En la lista **Configuración de notificaciones**, seleccione el tipo de notificación cuya configuración desea establecer.
   - En la sección **Notificar a los usuarios**, configure el método de notificación a los usuarios. Si es necesario, escriba el texto del mensaje de notificación.
   - En la sección **Notificar a los administradores**, configure el método de notificación al administrador. Si es necesario, escriba el texto del mensaje de notificación. Si es necesario, establezca la configuración de notificaciones adicionales con un clic en el botón **Configurar**.
   - En la sección **Umbrales de generación de eventos**, especifique los intervalos de tiempo después de los cuales Kaspersky Embedded Systems Security 2.2 registra los eventos *La base de datos de la aplicación está desactualizada, La base de datos de la aplicación es obsoleta* y *Hace mucho tiempo que no se realiza un análisis de áreas críticas*.
     - **La base de datos de la aplicación está desactualizada (días)**

       Número de días que han pasado desde la última actualización de bases de datos.

       El valor predeterminado es 7 días.
     - **La base de datos de la aplicación es obsoleta (días)**

       Número de días que han pasado desde la última actualización de bases de datos.

       El valor predeterminado es 14 días.
     - **Hace mucho tiempo que no se realiza un análisis de áreas críticas (días)**

       La cantidad de días después del último Análisis de áreas críticas satisfactorio.

       El valor predeterminado es 30 días.

5. Haga clic en **Aceptar**.

La configuración de notificaciones se guarda.

Configuración de la interacción con el servidor de administración

► *Para seleccionar los tipos de objetos sobre los cuales Kaspersky Embedded Systems Security 2.2 envía información al Servidor de administración de Kaspersky Security Center:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Registros y notificaciones**, haga clic en el botón **Configurar** en el bloque **Interacción con Servidor de administración**.

   Se abre la ventana **Listas de redes del Servidor de administración**.
4. En la ventana **Listas de redes del Servidor de administración**seleccione los tipos de objetos sobre los cuales Kaspersky Embedded Systems Security 2.2 enviará la información al Servidor de administración de Kaspersky Security Center:
   - Objetos en Cuarentena.
   - Objetos con Copia de seguridad.
5. Haga clic en **Aceptar**.

   Kaspersky Embedded Systems Security 2.2 enviará información sobre los tipos de objetos seleccionados al Servidor de administración.

Protección del equipo en tiempo real

Esta sección brinda información sobre los componentes de Protección del equipo en tiempo real: Protección de archivos en tiempo real, Uso de KSN y Prevención de exploits. Esta sección también brinda instrucciones sobre cómo configurar tareas de Protección en tiempo real y cómo administrar la configuración de seguridad de un equipo protegido.

En este capítulo

Protección de archivos en tiempo real

Esta sección contiene información acerca de la tarea de Protección de archivos en tiempo real y cómo configurarla.

En esta sección

Acerca de la tarea Protección de archivos en tiempo real

Cuando se está ejecutando la tarea Protección de archivos en tiempo real, Kaspersky Embedded Systems Security 2.2 analiza los siguientes objetos del equipo protegido cuando se accede a ellos:

- Archivos.
- Flujos de sistemas de archivos alternativos (flujos NTFS).
- Sectores de inicio y registro de inicio maestro en los discos duros locales y dispositivos externos.
- Archivos de contenedor de Windows Server® 2016 y Windows Server 2019.

Cuando una aplicación escribe un archivo en un equipo o lee un archivo desde él, Kaspersky Embedded Systems Security 2.2 intercepta dicho archivo, lo analiza en busca de amenazas y, si detecta una amenaza, realiza una acción predeterminada o una acción que usted haya especificado: intenta desinfectar el archivo, lo pasa a Cuarentena o simplemente lo elimina. Kaspersky Embedded Systems Security 2.2 devuelve el archivo a la aplicación si no está infectado o si se ha desinfectado correctamente.

Kaspersky Embedded Systems Security 2.2 intercepta las operaciones de archivo ejecutadas en Windows Server

2016 y Windows Server 2019.

Un contenedor es un entorno aislado, que permite la ejecución de aplicaciones sin interacción directa con el sistema operativo. Si el contenedor está ubicado en el alcance de la protección de tareas, Kaspersky Embedded Systems Security 2.2 analiza los archivos de contenedor a los que acceden los usuarios para detectar amenazas del equipo. Cuando se detecta una amenaza, la aplicación intenta desinfectar el contenedor. Si el intento tiene éxito, el contenedor continúa funcionando; si la desinfección produce un error, el contenedor se apaga.

Kaspersky Embedded Systems Security 2.2 también detecta malware para procesos que se ejecutan bajo el Subsistema de Windows para Linux®. Para tales procesos, la tarea de Protección de archivos en tiempo real aplica la acción definida por la configuración actual.

Configuración de la tarea Protección de archivos en tiempo real

De manera predeterminada, la tarea del sistema Protección de archivos en tiempo real utiliza la configuración descrita en la siguiente tabla. Puede cambiar los valores de esta configuración.

Table 30. Configuración de la tarea Protección de archivos en tiempo real predeterminada

Configuración	Valor predeterminado	Descripción
Alcance de la protección	El equipo completo, excluidas las unidades virtuales.	Se puede limitar el alcance de la protección.
Nivel de seguridad	La configuración común para todo el alcance de la protección; equivale al nivel de seguridad **Recomendado**.	Para los nodos seleccionados en el árbol de recursos de archivo del equipo, puede realizar lo siguiente: • Aplicar otro nivel de seguridad predefinido • Modificar el nivel de seguridad manualmente • Guardar la configuración de seguridad del nodo seleccionado como una plantilla para usarla más tarde.
Modo de protección de objetos	Al acceder y realizar modificaciones.	Puede seleccionar el modo de protección, es decir, definir el tipo de acceso en el que Kaspersky Embedded Systems Security 2.2 analizará los objetos.
Analizador heurístico	Se aplica el nivel de seguridad **Medio**.	Se puede habilitar o deshabilitar el Analizador heurístico y se puede configurar el nivel de análisis.
Aplicar la Zona de confianza	Aplicado.	Lista general de exclusiones que se puede utilizar en tareas seleccionadas.
Usar KSN para protección	Aplicado.	Puede mejorar la protección del equipo con la infraestructura de servicios en la nube de Kaspersky Security Network (disponible si se acepta la Declaración de KSN).
Programación del inicio de la tarea	Al inicio de la aplicación.	Puede configurar el inicio de la tarea programado.

► *Para configurar la tarea Protección de archivos en tiempo real, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Protección de archivos en tiempo real**, haga clic en el botón **Configurar** del bloque **Protección de archivos en tiempo real**.

   Se abre la ventana **Protección de archivos en tiempo real**.
4. Defina los siguientes valores de configuración de tarea:
   - En la pestaña **General**:
     - Modo de protección (consulte la sección "Selección del modo de protección", en la página 152)
     - Uso del Analizador heurístico (en la página 152)
     - Configuración de la integración de tareas con otros componentes de Kaspersky Embedded Systems Security 2.2.
   - En la pestaña **Administración de tareas**:
     - Opciones de programación de inicio de tareas (consulte la sección "Configuración de las opciones de programación de inicio de tareas", en la página 123).
5. Seleccione la pestaña **alcance de la protección** y haga lo siguiente:
   - Haga clic en el botón **Agregar** o **Editar** para editar el alcance de la protección (consulte la sección "Alcance de la protección en la tarea Protección de archivos en tiempo real", en la página 154).
     - En la ventana que se abre, elija lo que desea incluir en el alcance de la protección de la tarea:
       - **Área predefinida**
       - **Disco, carpeta o ubicación de red**
       - **Archivo**
     - Seleccione uno de los niveles de seguridad predefinidos (consulte la sección "Selección de niveles de seguridad predefinidos", en la página 155) o configure manualmente las opciones de protección (consulte la sección "Configuración manual de las opciones de protección", en la página 157).
6. Haga clic en **Aceptar** en la ventana **Protección de archivos en tiempo real**.

Kaspersky Embedded Systems Security 2.2 aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de tareas.

Uso del Analizador heurístico

Puede usar el Analizador heurístico y configurar el nivel de análisis para las tareas de Kaspersky Embedded Systems Security 2.2.

► *Para configurar el Analizador heurístico:*

1. Abra la configuración de aplicaciones (consulte la sección “Administración de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center”, en la página 126) o la configuración de directivas (consulte la sección “Configuración de directivas”, en la página 91), para las cuales desea configurar el Analizador heurístico.
2. Desactive o seleccione la casilla de verificación **Usar el analizador heurístico**.

   Esta casilla de verificación habilita y deshabilita el Analizador heurístico durante el análisis de objetos.

   Si la casilla está activada, el Analizador heurístico está habilitado.

   Si la casilla está desactivada, el Analizador heurístico está deshabilitado.

   De forma predeterminada, la casilla está activada.
3. Si es necesario, ajuste el nivel de análisis con el control deslizante.

   El control deslizante le permite ajustar el nivel del análisis heurístico. El nivel de intensidad del análisis ofrece un equilibrio entre la profundidad de las búsquedas de nuevas amenazas, el consumo de recursos del sistema operativo y el tiempo requerido para el análisis.

   Los siguientes niveles de intensidad del análisis están disponibles:

   - **Ligero**. El analizador heurístico realiza menos operaciones encontradas en archivos ejecutables. La probabilidad de detección de amenazas en este modo es en cierto grado inferior. El análisis es más rápido y consume menos recursos.
   - **Medio**. El Analizador heurístico realiza el número de instrucciones encontradas en los archivos ejecutables recomendados por los expertos de Kaspersky Lab.

     Este nivel está seleccionado de forma predeterminada.
   - **Profundo**. El analizador heurístico realiza más operaciones encontradas en archivos ejecutables. La probabilidad de detección de amenazas en este modo es mayor. El análisis consume más recursos del sistema, lleva más tiempo y puede causar un número más alto de falsas alarmas.

     El control deslizante está disponible si la casilla **Usar el analizador heurístico** está seleccionada.
4. Haga clic en **Aceptar**.

La configuración de la tarea se aplica inmediatamente a la tarea en ejecución. Si la tarea no se está ejecutando, la configuración modificada se aplica en el siguiente inicio.

Selección del modo de protección

En la tarea Protección de archivos en tiempo real, se puede seleccionar el modo de protección. La sección **Modo de protección de objetos** le permite especificar el tipo de acceso a objetos que Kaspersky Embedded Systems Security 2.2 debería analizar.

El parámetro **Modo de protección de objetos** tiene el valor común para todo el alcance de la protección especificada en la tarea. No es posible especificar valores diferentes en el parámetro para nodos individuales dentro del alcance de la protección.

► *Para seleccionar el modo de protección, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

   > Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configurar** del bloque **Protección de archivos en tiempo real**.

   Se abre la ventana **Protección de archivos en tiempo real**.
4. En la ventana que se abre, abra la pestaña **General** y seleccione el modo de protección que desea configurar:
   - **Modo inteligente**

     Kaspersky Embedded Systems Security 2.2 selecciona objetos para analizar por su cuenta. El objeto se analiza cuando se abre y, luego, nuevamente después de guardarlo si se modificó. Si el proceso realizó varias llamadas al objeto mientras se estaba ejecutando y si el proceso lo modificó, Kaspersky Embedded Systems Security 2.2 analiza el objeto de nuevo solo después de que el proceso lo guarda por última vez.
   - **Al acceder y realizar modificaciones**

     Kaspersky Embedded Systems Security 2.2 analiza el objeto cuando se abre y vuelve a analizarlo después de que se guarda si el objeto se modifica.

     De forma predeterminada, esta opción está seleccionada.
   - **Al acceder**

     Kaspersky Embedded Systems Security 2.2 analiza todos los objetos cuando se abren para su lectura, ejecución o modificación.
   - **Durante ejecución**

     Kaspersky Embedded Systems Security 2.2 analiza el archivo solo cuando se accede para su ejecución.
5. Haga clic en **Aceptar**.

Se aplicará el modo de protección seleccionado.

Alcance de la protección en la tarea Protección de archivos en tiempo real

Esta sección proporciona instrucciones sobre la creación y la administración de un alcance de la protección en la tarea Protección de archivos en tiempo real.

En esta sección

Áreas de protección predefinidas

Los recursos del archivo del equipo protegido se muestran en la configuración de la tarea **Protección de archivos en tiempo real** en la pestaña **Alcance de la protección**.

El árbol o la lista de recursos de archivos muestran los nodos a los cuales tiene acceso de lectura según la configuración de seguridad de Microsoft Windows.

Kaspersky Embedded Systems Security 2.2 abarca las siguientes áreas de protección predefinidas:

- **Discos duros locales**. Kaspersky Embedded Systems Security 2.2 protege archivos en los discos duros del equipo.
- **Unidades extraíbles**. Kaspersky Embedded Systems Security 2.2 protege archivos en dispositivos externos, por ejemplo, unidades USB o CD. Todas las unidades extraíbles, discos, carpetas o archivos individuales pueden incluirse o excluirse del alcance de la protección.
- **Red**. Kaspersky Embedded Systems Security 2.2 analiza los archivos que se escriben en las carpetas de red o que son leídos por las aplicaciones que se ejecutan en el equipo. Kaspersky Embedded Systems Security 2.2 no protege archivos cuando aplicaciones de otros equipos acceden a ellos.
- **Unidades virtuales**. Las unidades, archivos y carpetas dinámicos que se conectan temporalmente al equipo se pueden incluir en el alcance de la protección, por ejemplo, unidades de clústeres comunes.

De forma predeterminada, puede ver y configurar las áreas de protección predefinidas en el árbol de recursos de archivos de red; también puede agregar áreas de protección predefinidas a la lista de recursos de archivos de red durante su formación en la configuración del alcance de la protección.

De forma predeterminada, el alcance de la protección incluye todas las áreas predefinidas, excepto las unidades virtuales.

Las unidades virtuales creadas mediante un comando SUBST no se muestran en el árbol de recursos de archivo del equipo de la Consola de la aplicación. Para incluir objetos de la unidad virtual en el alcance de la protección, incluya la carpeta del equipo con la que se asocia la unidad virtual en el alcance de la protección. Las unidades de red conectadas tampoco se mostrarán en la lista de recursos de archivos del equipo. Para incluir objetos de unidades de red en el alcance de la protección, especifique la ruta a la carpeta que corresponde a esta unidad de red en formato UNC.

Selección de niveles de seguridad predefinidos

Se puede aplicar uno de los siguientes niveles de seguridad predefinidos para los nodos seleccionados en la lista de recursos de archivos del equipo: **Máximo Rendimiento**, **Recomendado** y **Máxima Protección**. Cada uno de estos niveles contiene su propio conjunto de configuraciones de seguridad predefinidas (consulte la tabla a continuación).

Máximo rendimiento

El nivel de seguridad **Máximo rendimiento** se recomienda si, además del uso de Kaspersky Embedded Systems Security 2.2 en los equipos, existen medidas adicionales de seguridad del equipo en la red, por ejemplo, si hay firewalls y directivas de seguridad existentes.

Recomendado

El nivel de seguridad **Recomendado** garantiza una óptima combinación de protección e impacto en el rendimiento de los equipos protegidos. Este nivel es recomendado por los expertos de Kaspersky Lab como suficiente para proteger equipos en la mayoría de las redes empresariales. El nivel de seguridad **Recomendado** está configurado de manera predeterminada.

Máxima protección

Se recomienda el nivel de seguridad **Máxima protección** si la red de la organización ha elevado los requisitos de seguridad del equipo.

Table 31. Niveles de seguridad predefinidos y valores de configuración correspondientes

Opciones	Nivel de seguridad		
	Máximo rendimiento	Recomendado	Máxima protección
Protección de objetos	Por extensión	Por formato	Por formato
Proteger solo los archivos nuevos y modificados	Habilitado	Habilitado	Deshabilitado
Acción que se realizará con los objetos infectados y otros objetos	Bloquear acceso y desinfectar. Eliminar si falla la desinfección	Bloquear acceso y realizar la acción recomendada	Bloquear acceso y desinfectar. Eliminar si falla la desinfección
Acción que se realizará con los objetos probablemente infectados	Bloquear acceso y colocar en Cuarentena	Bloquear acceso y realizar la acción recomendada	Bloquear acceso y colocar en Cuarentena
Excluir archivos	No	No	No
No detectar	No	No	No
Detener el análisis si demora más de (seg.)	60 segundos.	60 segundos.	60 segundos.
Omitir objetos compuestos de más de (MB)	8 MB	8 MB	Sin configurar
Analizar secuencias alternativas de NTFS	Sí	Sí	Sí

Opciones	Nivel de seguridad		
Analizar sectores de inicio del disco y MBR	Sí	Sí	Sí
Protección de objetos compuestos	• Objetos empaquetados* *Solo objetos nuevos y modificados	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* *Solo objetos nuevos y modificados	• Archivos SFX* • Objetos empaquetados* • Objetos OLE integrados* * Todos los objetos
Eliminar totalmente el archivo compuesto que la aplicación no puede modificar en caso de un objeto integrado detectado	No	No	Sí

Los parámetros **Protección de objetos**, **Usar la tecnología iChecker**, **Usar la tecnología iSwift** y **Usar el analizador heurístico** no se incluyen en la configuración de los niveles de seguridad predefinidos. Si modifica la configuración de seguridad de **Protección de objetos**, **Usar la tecnología iChecker**, **Usar la tecnología iSwift** o **Usar el analizador heurístico** después de seleccionar uno de los niveles de seguridad predefinidos, el nivel de seguridad que ha seleccionado no cambiará.

► *Para seleccionar uno de los niveles de seguridad predeterminados, realice uno de los siguientes pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configurar** del bloque **Protección de archivos en tiempo real**.

   Se abre la ventana **Protección de archivos en tiempo real**.
4. En la pestaña **Alcance de la protección**, seleccione el nodo cuya configuración de seguridad desea configurar y haga clic en **Configurar**.

   La ventana **Configuración de Protección de archivos en tiempo real** se abre.

5. Seleccione el nivel de seguridad deseado en la lista desplegable:
   - **Máxima protección**
   - **Recomendado**
   - **Máximo rendimiento**
6. Haga clic en **Aceptar**.

Se guardaron las opciones configuradas recientemente.

Kaspersky Embedded Systems Security 2.2 aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de tareas.

Configuración manual de las opciones de seguridad

De manera predeterminada, la tarea de Protección de archivos en tiempo real utiliza la configuración de seguridad común para todo el alcance de la protección. Estos valores corresponden a los del nivel de seguridad predefinido **Recomendado** (consulte la sección “Selección de niveles de seguridad predefinidos”, en la página 155).

Los valores predeterminados de la configuración de seguridad se pueden modificar configurándolos como valores comunes para todo el alcance de la protección, o como valores diferentes para los diversos nodos de la lista o del árbol de recursos de archivos del equipo.

Al trabajar con el árbol de recursos de archivos del equipo, las opciones de seguridad que se configuran para el nodo principal seleccionado se aplican automáticamente a todos los nodos secundarios. La configuración de seguridad del nodo principal no se aplica a nodos secundarios que se configuran por separado.

► *Para configurar las opciones de seguridad del nodo seleccionado en forma manual:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configurar** del bloque **Protección de archivos en tiempo real**.

   Se abre la ventana **Protección de archivos en tiempo real**.
4. En la pestaña **alcance de la protección**, seleccione el nodo cuya configuración de seguridad desea configurar y hacer clic en **Configurar**.

   La ventana **Configuración de Protección de archivos en tiempo real** se abre.

5. En la pestaña **Nivel de seguridad**, puede seleccionar cualquier nivel existente o hacer clic en el botón **Configurar** para configurar las opciones personalizadas.
6. Puede configurar los valores de seguridad requeridos del nodo seleccionado de acuerdo con sus requisitos:
   - Configuración general (consulte la sección “Configuración general de las opciones de tareas”, en la página 158)
   - Acciones (consulte la sección “Configuración de acciones”, en la página 160)
   - Rendimiento (consulte la sección “Configuración de rendimiento”, en la página 162)
7. Haga clic en **Guardar** en la ventana **Configuración del alcance de la protección**.

Se guarda la nueva configuración del alcance de la protección.

Configuración de las opciones generales de tareas

► *Para configurar las opciones de seguridad generales de la tarea Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración de Protección de archivos en tiempo real** (consulte la sección “Configuración manual de las opciones de seguridad”, en la página 157).
2. Seleccione la pestaña **General**.
3. En la sección **Protección de objetos**, especifique los tipos de objetos que desea incluir en el alcance de la protección:
   - **Todos los objetos**

     Kaspersky Embedded Systems Security 2.2 analiza todos los objetos.
   - **Objetos analizados según su formato**

     Kaspersky Embedded Systems Security 2.2 solo analiza los objetos infectables según el formato del archivo.

     Kaspersky Lab compila la lista de formatos. Se incluye en las bases de datos de Kaspersky Embedded Systems Security 2.2.
   - **Objetos analizados según la lista de extensiones de la base de datos antivirus**

     Kaspersky Embedded Systems Security 2.2 solo analiza los objetos infectables según la extensión del archivo.

     Kaspersky Lab compila la lista de extensiones. Se incluye en las bases de datos de Kaspersky Embedded Systems Security 2.2.
   - **Objetos analizados según la lista de extensiones especificada**

     Kaspersky Embedded Systems Security 2.2 analiza los archivos según su extensión. La lista de extensiones de archivos se puede personalizar manualmente en la ventana **Lista de extensiones**, que se puede abrir con un clic en el botón **Editar**.
   - **Analizar sectores de inicio del disco y MBR**

     Habilita la protección de los sectores de inicio y los registros de inicio maestros.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza los sectores de inicio y los registros de inicio maestro en los discos duros y las

unidades extraíbles del equipo.

De forma predeterminada, la casilla está activada.

- **Analizar secuencias alternativas de NTFS**

  Análisis de flujos de archivos y carpetas alternativos en las unidades del sistema de archivos NTFS.

  Si se selecciona la casilla de verificación, la aplicación analiza un objeto posiblemente infectado y todos los flujos NTFS asociados con ese objeto.

  Si se cancela la selección de la casilla de verificación, la aplicación solo analiza el objeto que se detectó y se consideró como posiblemente infectado.

  De forma predeterminada, la casilla está activada.

4. En la sección **Rendimiento**, seleccione o cancele la selección de la casilla de verificación **Proteger solo los archivos nuevos y modificados**.

   Esta casilla de verificación activa y desactiva el análisis y la protección de archivos que Kaspersky Embedded Systems Security 2.2 reconoció como nuevos o modificados desde el último análisis.

   Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza y protege solo los archivos que reconoció como nuevos o modificados desde el último análisis.

   Si se cancela la selección de la casilla de verificación, puede seleccionar si desea analizar y proteger solo archivos nuevos o todos los archivos, más allá de su estado de modificación.

   De forma predeterminada, la casilla está seleccionada para los niveles de seguridad **Máximo rendimiento** y **Recomendado**. Si se configura el nivel de seguridad **Máxima protección**, la casilla de verificación se desactiva.

   Para cambiar entre opciones disponibles cuando la casilla está desactivada, haga clic en el vínculo **Todos** / **Solo nuevos** para cada uno de los tipos de objeto compuestos.

5. En la sección **Protección de objetos compuestos**, especifique los objetos compuestos que desea incluir en el alcance de la protección:

   - **Todos/solo archivos nuevos**

     Análisis de archivos ZIP, CAB, RAR, ARJ y otros formatos de archivos.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza los archivos comprimidos.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 omite los archivos comprimidos durante el análisis.

     El valor predeterminado depende del nivel de seguridad seleccionado.

   - **Todos/solo archivos SFX nuevos**

     Análisis de archivos autoextraíbles.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza archivos comprimidos SFX.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 omite los archivos comprimidos SFX durante el análisis.

El valor predeterminado depende del nivel de seguridad seleccionado.

Esta opción se encuentra activa cuando la casilla de verificación **Archivos comprimidos** está desactivada.

- **Todos/solo bases de datos de correo electrónico nuevas**

  Análisis de archivos de bases de datos de correo de Microsoft Outlook® y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza todos los archivos de la base de datos de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 omite los archivos de la base de datos de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/solo objetos empaquetados nuevos**

  Análisis de archivos ejecutables empaquetados mediante compresores de código binario, tales como UPX o ASPack.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza los archivos ejecutables comprimidos por empaquetadores.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 omite los archivos ejecutables comprimidos por empaquetadores durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/solo correo sin formato nuevo**

  Análisis de archivos de formatos de correo, tales como mensajes de Microsoft Outlook y Microsoft Outlook Express.

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza los archivos con formato de correo.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 omite los archivos con formato de correo durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

- **Todos/solo objetos OLE incrustados nuevos**

  Análisis de objetos integrados en archivos (por ejemplo, macros de Microsoft Word o archivos adjuntos del mensaje de correo electrónico).

  Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza los objetos integrados en archivos.

  Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 omite los objetos integrados en archivos durante el análisis.

  El valor predeterminado depende del nivel de seguridad seleccionado.

6. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de acciones

► *Para configurar las acciones en objetos infectados y otros objetos detectados para la tarea de Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración de Protección de archivos en tiempo real** (consulte la sección

"Configuración manual de las opciones de seguridad", en la página 157).

2. Seleccione la pestaña **Acciones**.
3. Seleccione la acción que se debe realizar en los objetos infectados y otros objetos detectados:
   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security 2.2 no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada alcance de la protección. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security 2.2 cambia automáticamente el nivel de seguridad a **Personalizado**.

   - **Bloquear acceso**.

     Cuando se selecciona esta opción, Kaspersky Embedded Systems Security 2.2 bloquea el acceso al objeto detectado o probablemente infectado. Puede seleccionar una acción adicional sobre los objetos bloqueados en la lista desplegable.

   - **Realizar acción adicional**.

     Seleccione la acción en la lista desplegable:

     - **Desinfectar**.
     - **Desinfectar. Eliminar si falla la desinfección**.
     - **Eliminar**.
     - **Recomendado**.
4. Seleccione la acción a realizar en los objetos probablemente infectados:
   - **Solo notificar**.

     Cuando se selecciona este modo, Kaspersky Embedded Systems Security 2.2 no bloquea el acceso a los objetos infectados y a otros objetos detectados ni realiza ninguna acción relacionada con ellos. Se registra el siguiente evento en el registro de tareas: *Objeto no desinfectado. Motivo: No se tomó ninguna acción para neutralizar el objeto detectado debido a la configuración definida por el usuario.* El evento especifica toda la información disponible sobre el objeto detectado.

     El modo **Solo notificar** debe configurarse por separado para cada alcance de la protección. Este modo no se usa de forma predeterminada en ninguno de los niveles de seguridad. Si selecciona este modo, Kaspersky Embedded Systems Security 2.2 cambia automáticamente el nivel de seguridad a **Personalizado**.

   - **Bloquear acceso**.

     Cuando se selecciona esta opción, Kaspersky Embedded Systems Security 2.2 bloquea el acceso al objeto detectado o probablemente infectado. Puede seleccionar una acción adicional sobre los objetos bloqueados en la lista desplegable.

   - **Realizar acción adicional**.

     Seleccione la acción en la lista desplegable:

     - **Cuarentena**.

- **Eliminar**.
- **Recomendado**.

5. Configure las acciones que se deben realizar en los objetos según el tipo de objeto detectado:
   a. Borre o seleccione la casilla de verificación **Realizar acciones según el tipo de objeto detectado**.

      Si se selecciona la casilla, puede configurar la acción principal y secundaria para cada tipo de objeto detectado haciendo clic en el botón **Configurar** ubicado junto a la casilla de verificación.

      Si la casilla de verificación no está seleccionada, Kaspersky Embedded Systems Security 2.2 realiza las acciones seleccionadas en las secciones **Acción que se realizará con los objetos infectados y otros objetos** y **Acción que se realizará con los objetos probablemente infectados** para los tipos de objetos correspondientes.

      De forma predeterminada, la casilla está desactivada.

   b. Haga clic en el botón **Configurar**.
   c. En la ventana que se abre, seleccione la acción primaria y secundaria (en caso de que falle la primaria) para cada tipo de objeto detectado.
   d. Haga clic en **Aceptar**.
6. Seleccione la acción a realizar en archivos compuestos no modificables: seleccione o borre la casilla de verificación **Eliminar totalmente el archivo compuesto que la aplicación no puede modificar en caso de un objeto integrado detectado**.

   Esta casilla habilita o deshabilita la eliminación forzada del archivo compuesto principal cuando se detecta un objeto secundario malicioso, probablemente infectado u otro objeto secundario integrado.

   Si se selecciona la casilla de verificación y se configura la tarea para eliminar los objetos infectados y probablemente infectados. Kaspersky Embedded Systems Security 2.2 elimina de manera forzada todo el objeto compuesto principal cuando se detecta un objeto malicioso u otro objeto integrado. La eliminación forzada de un archivo principal junto con todo su contenido sucede si la aplicación no puede eliminar únicamente el objeto secundario detectado (por ejemplo, si el objeto principal es inmodificable).

   Si se desactiva esta casilla y la tarea se configura para eliminar objetos infectados y probablemente infectados, Kaspersky Embedded Systems Security 2.2 no realiza la acción seleccionada si el objeto principal es inmodificable.

   De forma predeterminada, la casilla de verificación para el nivel de seguridad **Máxima protección** está seleccionada, y las casillas para los niveles de seguridad **Recomendado** y **Máximo rendimiento** están desactivadas.
7. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Configuración de rendimiento

► *Para configurar el rendimiento para la tarea Protección de archivos en tiempo real:*

1. Abra la ventana **Configuración de protección de archivos en tiempo real** (consulte la sección “Configuración manual de las opciones de seguridad”, en la página 157).
2. Seleccione la pestaña **Rendimiento**.

3. En la sección **Exclusiones**:
   - Borre o seleccione la casilla de verificación **Excluir archivos**.

     Excluir archivos del análisis por nombre de archivo o máscara de nombre de archivo.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 omite los objetos especificados durante el análisis.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 analiza todos los objetos.

     De forma predeterminada, la casilla está desactivada.
   - Borre o seleccione la casilla de verificación **No detectar**.

     Los objetos se excluyen del análisis por el nombre o la máscara del nombre del objeto detectable. La lista de nombres de objetos detectables está disponible en el sitio web de la Enciclopedia de Virus https://securelist.lat/.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 omite los objetos especificados detectables durante el análisis.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 detecta todos los objetos especificados en la aplicación de forma predeterminada.

     De forma predeterminada, la casilla está desactivada.
   - Haga clic en el botón **Editar** en cada para parámetro agregar exclusiones.
4. En la sección **Configuración avanzada**:
   - **Detener el análisis si demora más de (seg.)**

     Limita la duración del análisis de objetos. El valor predeterminado es 60 segundos.

     Si la casilla está desactivada, la duración del análisis se limita al valor especificado.

     Si la casilla está desactivada, la duración del análisis es ilimitada.

     De forma predeterminada, la casilla está activada.
   - **Omitir objetos compuestos de más de (MB)**

     Excluye del análisis objetos más grandes que el tamaño especificado.

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 omite los objetos compuestos cuyo tamaño supera el límite especificado durante el análisis antivirus.

     Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 analiza los objetos compuestos de cualquier tamaño.

     De manera predeterminada, la casilla está activada para los niveles de seguridad **Recomendado** y **Máximo rendimiento**.
   - **Usar la tecnología iSwift**

     iSwift compara el identificador NTFS del archivo, que está almacenado en una base de datos, con un identificador actual. El análisis se realiza solo para archivos cuyos identificadores han cambiado (archivos nuevos y archivos modificados desde el último análisis de objetos del sistema NTFS).

     Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza solo los archivos nuevos o modificados desde el último análisis de objetos del

sistema NTFS.

Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 analiza los archivos del sistema NTFS sin considerar la fecha de creación o modificación del archivo.

De forma predeterminada, la casilla está activada.

- **Usar la tecnología iChecker**

  iChecker calcula y recuerda las sumas de comprobación de los archivos analizados. Si un objeto se modifica, la suma de control cambia. La aplicación compara todas las sumas de comprobación durante la tarea de análisis, y analiza solo los archivos nuevos y modificados desde el ultimo análisis.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 analiza solo los archivos nuevos y modificados.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 analiza los archivos sin considerar la fecha de creación o modificación del archivo.

  De forma predeterminada, la casilla está activada.

5. Haga clic en **Guardar**.

Se guardará la nueva configuración de la tarea.

Uso de KSN

Esta sección contiene información acerca de la tarea de Uso de KSN y cómo configurarla.

En esta sección

Acerca de la tarea Uso de KSN

Kaspersky Security Network (también denominado “KSN”) es una infraestructura de servicios en línea que proporciona acceso a la base de conocimientos operativa de Kaspersky Lab sobre la reputación de archivos, recursos web y programas. Kaspersky Security Network permite que Kaspersky Embedded Systems Security 2.2 reaccione rápidamente ante amenazas nuevas, mejora el rendimiento de varios componentes de protección y reduce la posibilidad de falsos positivos.

Para iniciar la tarea Uso de KSN, debe aceptar la Declaración de Kaspersky Security Network.

La información recibida por Kaspersky Embedded Systems Security 2.2 de Kaspersky Security Network se refiere solo a la reputación de los programas.

La participación en KSN permite a Kaspersky Lab recibir información en tiempo real sobre tipos y fuentes de amenazas nuevas, desarrollar modos de neutralizarlas y reducir el número de falsos positivos en los componentes de la aplicación.

La información más detallada sobre la transferencia, el procesamiento, el almacenamiento y la destrucción de información sobre uso de aplicaciones está disponible en la ventana Manejo de datos de la tarea Uso de KSN, y en la Política de privacidad en el sitio web de Kaspersky Lab.

La participación en Kaspersky Security Network es voluntaria. La decisión en cuanto a la participación en Kaspersky Security Network se toma después de la instalación de Kaspersky Embedded Systems Security 2.2. Puede cambiar de opinión sobre la participación en Kaspersky Security Network en cualquier momento.

Kaspersky Security Network puede utilizarse en las siguientes tareas de Kaspersky Embedded Systems Security 2.2:

- Protección de archivos en tiempo real.
- Análisis a pedido.
- Control de inicio de aplicaciones.

Kaspersky Security Network Privada

Consulte detalles sobre la forma de configurar Kaspersky Security Network Privada (de aquí en más, “KSN Privada”) en la *Ayuda de Kaspersky Security Center*.

Si utiliza KSN Privada en el equipo protegido, vaya a la ventana **Manejo de datos** (consulte la sección “Configuración de procesamiento de datos”, en la página 168) de la tarea Uso de KSN que puede leer en la Declaración de KSN y habilite la tarea seleccionando **Acepto los términos de la Declaración de Kaspersky Security Network**. Al aceptar los términos, acepta enviar todos los tipos de datos mencionados en la Declaración de KSN (solicitudes de seguridad, datos estadísticos) a servicios de KSN.

Después de aceptar los términos de KSN Privada, las casillas de verificación que configuran el uso de KSN global no están disponibles.

Si deshabilita KSN Privada cuando se está ejecutando la tarea Uso de KSN, se produce el error *Infracción de la licencia* y la tarea se detiene. Para seguir protegiendo el equipo, debe aceptar la Declaración de KSN en la ventana **Manejo de datos** y reiniciar la tarea.

Cancelación de la aceptación de la Declaración de KSN

Puede cancelar la aceptación y detener todo intercambio de datos con Kaspersky Security Network en cualquier momento. Las siguientes acciones se consideran como una cancelación completa o parcial de la Declaración de KSN:

- Si se desactiva la casilla de verificación **Enviar datos sobre archivos analizados**: la aplicación deja de enviar sumas de comprobación de archivos analizados al servicio de KSN.
- Si se desactiva la casilla de verificación **Enviar estadísticas de Kaspersky Security Network**: la aplicación deja de procesar datos con estadísticas de KSN adicionales.
- Si se desactiva la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Security**

Network: la aplicación detiene todo el procesamiento de datos relacionados con KSN y se detiene la tarea Uso de KSN.

- Si se desinstala el componente Uso de KSN: se detiene todo el procesamiento de datos relacionado con KSN.
- Si se desinstala Kaspersky Embedded Systems Security 2.2: se detiene todo el procesamiento de datos relacionado con KSN.

Configuración de la tarea Uso de KSN

Puede cambiar la configuración predeterminada de la tarea Uso de KSN (consulte la siguiente tabla).

Table 32. Configuración predeterminada de la tarea Uso de KSN

Configuración	Valor predeterminado	Descripción
Acciones a realizar en objetos dudosos según KSN	Eliminar	Puede especificar acciones que Kaspersky Embedded Systems Security 2.2 tomará sobre los objetos identificados por KSN como dudosos.
Transferencia de datos	Se calcula la suma de control del archivo (hash MD5) para los archivos que no superan 2 MB de tamaño.	Puede especificar el tamaño máximo de archivos para los cuales se calcula una suma de control con el algoritmo MD5 para la entrega a KSN. Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 calcula el hash MD5 para los archivos de cualquier tamaño.
Declaración de KSN	Se borra la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Security Network**.	Decida si desea participar en KSN después de la instalación. Puede cambiar su decisión en cualquier momento.
Enviar estadísticas de Kaspersky Security Network	Seleccionado (se aplica solo si se aceptó la Declaración de KSN)	Si se aceptó la Declaración de KSN, se enviarán automáticamente las estadísticas de KSN a menos que desactive la casilla de verificación.
Enviar datos sobre archivos analizados	Seleccionado (se aplica solo si se aceptó la Declaración de KSN)	Si se aceptó la Declaración de KSN, se envían los datos sobre los archivos analizados desde el inicio de la tarea. Puede desactivar la casilla de verificación en cualquier momento.
Acepto los términos de la Declaración de Kaspersky Managed Protection	Desactivada	Puede habilitar o deshabilitar el servicio KMP. El servicio está disponible solo si se firmó el acuerdo adicional durante el proceso de compra de la aplicación.
Programación del inicio de la tarea	La primera ejecución no está programada.	Puede iniciar la tarea manualmente o configurar un inicio programado.
Usar Kaspersky Security Center como proxy de KSN	Seleccionada	De forma predeterminada, los datos se envían a KSN mediante Kaspersky Security Center.

► *Para configurar la tarea Uso de KSN, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configurar** en el bloque **Uso de KSN**.

   Se abre la ventana **Uso de KSN**.
4. En la pestaña **General**, configure la siguiente configuración de tarea:
   - En la sección **Acción para realizar con los objetos dudosos según KSN**, especifique la acción que Kaspersky Embedded Systems Security 2.2 debe realizar si detecta un objeto identificado por KSN como dudoso:
     - **Eliminar**

       Kaspersky Embedded Systems Security 2.2 elimina el objeto de estado dudoso según KSN y coloca una copia en Copia de seguridad.

       De forma predeterminada, esta opción está seleccionada.
     - **Registrar información**

       Kaspersky Embedded Systems Security 2.2 registra información sobre el objeto de estado dudoso según KSN en el registro de tareas. Kaspersky Embedded Systems Security 2.2 no elimina el objeto dudoso.
   - En la sección **Transferencia de datos**, limite el tamaño de los archivos para los cuales se calcula la suma de control:
     - Seleccione o desactive la casilla de verificación **No calcular la suma de control antes de enviar el archivo a KSN si el tamaño del archivo es mayor a (MB)**.

       Esta casilla de verificación habilita o deshabilita el cálculo de la suma de control para archivos del tamaño especificado para la entrega de esta información al servicio KSN.

       La duración del cálculo de la suma de control depende del tamaño del archivo.

       Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 no calcula la suma de control para los archivos que superan el tamaño especificado (en MB).

       Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 calcula la suma de control para los archivos de cualquier tamaño.

De forma predeterminada, la casilla está activada.

- Si es necesario, en el campo a la derecha, cambie el tamaño máximo de archivos para los cuales Kaspersky Embedded Systems Security 2.2 calcula la suma de control.

- Desactive o seleccione la casilla de verificación **Usar Kaspersky Security Center como proxy de KSN**.

  La casilla de verificación permite administrar la transferencia de datos entre los equipos protegidos y KSN.

  Si se desactiva la casilla, los datos del Servidor de administración y los equipos protegidos se envían directamente a KSN (no mediante Kaspersky Security Center). La directiva activa define qué tipo de datos pueden enviarse directamente a KSN.

  Si se selecciona la casilla, todos los datos se envían a KSN mediante Kaspersky Security Center.

  De forma predeterminada, la casilla está activada.

Para habilitar el proxy de KSN, debe haberse aceptado la Declaración de KSN, y Kaspersky Security Center debe estar configurado correctamente. Consulte la *Ayuda de Kaspersky Security Center* para obtener más detalles.

5. De ser necesario, configure la programación de inicio de tareas en la pestaña **Administración de tareas**. Por ejemplo, puede iniciar la tarea según una programación y especificar la frecuencia **Al inicio de la aplicación** si desea que la tarea se ejecute automáticamente cuando se reinicia el equipo.

   La aplicación iniciará automáticamente la tarea Uso de KSN según la programación.

6. Configure el manejo de datos (consulte la sección “Configuración de procesamiento de datos” en la página 168) antes de iniciar la tarea.

7. Haga clic en **Aceptar**.

Se aplica la configuración modificada. La fecha y tiempo de modificación de la configuración, así como la información sobre la configuración de la tarea antes y después de la modificación, se guardan en el registro de tareas.

Configuración del procesamiento de la información

► *Para configurar los datos que procesarán los servicios de KSN y aceptar la Declaración de KSN:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Manejo de datos** en el bloque **Uso de KSN**.

   Se abre la ventana **Manejo de datos**.

4. En la ficha **Estadísticas y servicios**, lea la declaración y seleccione la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Security Network**.

5. Para aumentar el nivel de protección, se seleccionan automáticamente las siguientes casillas de verificación:

   - **Enviar datos sobre archivos analizados**.

     Si se selecciona la casilla, Kaspersky Embedded Systems Security 2.2 envía la suma de control de los archivos analizados a Kaspersky Lab. La conclusión sobre la seguridad de cada archivo se basa en la reputación recibida de KSN.

     Si se desactiva la casilla, Kaspersky Embedded Systems Security 2.2 no envía la suma de control de los archivos a KSN.

     Tenga en cuenta que las solicitudes de reputación de archivos se podrían enviar en un modo limitado. Las limitaciones se utilizan para proteger a los servidores de reputación de Kaspersky Lab contra los ataques de DDoS. En esta situación, los parámetros de solicitudes de reputación de archivos que se envían se definen por las reglas y los métodos establecidos por los expertos de Kaspersky Lab, y no pueden ser configurados por el usuario en un equipo protegido. Las actualizaciones de estas reglas y métodos se reciben junto con las actualizaciones de la base de datos de la aplicación. Si se aplican las limitaciones, aparece el estado *Habilitado por Kaspersky Lab para proteger a los servidores de KSN contra DDoS* en las estadísticas de la tarea Uso de KSN.

     De forma predeterminada, la casilla está activada.

   - **Enviar estadísticas de Kaspersky Security Network.**

     Si se selecciona la casilla, Kaspersky Embedded Systems Security 2.2 envía estadísticas adicionales que pueden contener datos personales. La lista de todos los datos que se envían como estadísticas de KSN se especifica en la Declaración de KSN. Los datos recibidos por Kaspersky Lab se usan para mejorar la calidad de las aplicaciones y el nivel del índice de detección de amenazas.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 no envía estadísticas adicionales. De forma predeterminada, la casilla está activada.

   Puede desactivar estas casillas de verificación y dejar de enviar datos adicionales en cualquier momento.

6. En la ficha **Kaspersky Managed Protection**, lea la declaración y seleccione la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Managed Protection**.

   Si se selecciona la casilla, significa que acepta enviar estadísticas sobre la actividad del equipo protegido a los especialistas de Kaspersky Lab. Los datos recibidos se utilizan para análisis e informes las veinticuatro horas, algo que se requiere para evitar incidentes de violación de la seguridad.

   De forma predeterminada, la casilla está desactivada.

Los cambios de estado de la casilla de verificación **Acepto los términos de la Declaración de Kaspersky Managed Protection** no inician o detienen inmediatamente el procesamiento de datos. Para aplicar los cambios, debe reiniciar Kaspersky Embedded Systems Security 2.2.

Para usar el servicio KMP, debe firmar el acuerdo correspondiente y ejecutar archivos de configuración en un equipo protegido.

Para usar el servicio KMP, deben aceptarse los términos de procesamiento de datos de la Declaración de KSN en la pestaña **Estadísticas y servicios**.

7. Haga clic en **Aceptar**.

   Se guardará la configuración de procesamiento de datos.

Configuración de la transferencia de datos adicional

Kaspersky Embedded Systems Security 2.2 se puede configurar para enviar los siguientes datos a Kaspersky Lab:

- Sumas de comprobación de archivos analizados (casilla de verificación **Enviar datos sobre archivos analizados**).
- Estadísticas adicionales, incluidos datos personales (casilla de verificación **Enviar estadísticas de Kaspersky Security Network**).

Consulte la sección “Manejo de datos locales” de este guía para acceder a información detallada sobre los datos que se envían a Kaspersky Lab.

Las casillas correspondientes se pueden seleccionar o desactivar solo si se seleccionó la casilla **Acepto los términos de la Declaración de Kaspersky Security Network**.

De forma predeterminada, Kaspersky Embedded Systems Security 2.2 envía sumas de comprobación y estadísticas adicionales después de aceptar la Declaración de KSN.

Table 33. Posibles estados de las casillas de verificación y condiciones correspondientes

Estado de la casilla	Condiciones para el estado de la casilla Enviar datos sobre archivos analizados	Condiciones para el estado de la casilla Enviar estadísticas de Kaspersky Security Network
☑	• se envían solicitudes de reputación • la casilla es editable	• se envían estadísticas adicionales • la casilla es editable
☑	• no se envían solicitudes de reputación • la casilla no es editable	• no se envían estadísticas adicionales • la casilla no es editable
☐	• no se envían solicitudes de reputación • la casilla es editable	• no se envían estadísticas adicionales • la casilla es editable
☐	• no se envían solicitudes de reputación • la casilla no es editable	• no se envían estadísticas adicionales • la casilla no es editable

Prevención de exploits

Esta sección contiene instrucciones sobre cómo configurar las opciones de protección de la memoria de proceso.

En este capítulo

Acerca de la prevención de exploits

Kaspersky Embedded Systems Security 2.2 permite proteger la memoria de proceso contra exploits. Esta función se implementa en el componente Prevención de exploits. Puede cambiar el estado de actividad del componente y configurar las opciones de protección de memoria de proceso.

El componente protege la memoria de proceso contra exploits al insertar un Agente de protección externo ("Agente") en el proceso protegido.

Un Agente de protección de proceso es un módulo de Kaspersky Embedded Systems Security 2.2 cargado dinámicamente que se introduce en procesos protegidos para supervisar su integridad y reducir el riesgo de ataques de exploit.

La operación del Agente dentro del proceso protegido requiere el comienzo y la detención del proceso: la carga inicial del Agente en un proceso agregado a la lista de procesos protegidos solo es posible si el proceso se reinicia. Además, después de que un proceso se haya eliminado desde la lista de procesos protegidos, el Agente solo se puede descargar después de que el proceso se haya reiniciado.

El Agente se debe detener para descargarlo desde procesos protegidos: si el componente Prevención de exploits no está instalado, la aplicación congela el entorno y obliga al Agente a ser descargado de los procesos protegidos. Si durante la desinstalación del componente se inserta el Agente en alguno de los procesos protegidos, usted debe finalizar el proceso afectado. Es posible que se deba reiniciar el equipo (por ejemplo, si el proceso del sistema está protegido).

Si se detectan pruebas de un ataque de exploit en un proceso protegido, Kaspersky Embedded Systems Security 2.2 realiza una de las siguientes acciones:

- Finaliza el proceso si se lleva a cabo un intento de ataque de exploit.
- Informa que el proceso se ha puesto en peligro.

Puede detener la protección del proceso con uno de los siguientes métodos:

- Desinstalación del componente.
- Eliminación del proceso de la lista de procesos protegidos y reinicio del proceso.

Servicio de prevención de exploits de Kaspersky Security

Se requiere el servicio de prevención de exploits de Kaspersky Security en el equipo protegido para que el componente Prevención de exploits sea más efectivo. Este servicio y el componente Prevención de exploits son parte de la instalación recomendada. Durante la instalación del servicio en el equipo protegido, se crea y se inicia el

proceso kavfswh. Esto comunica la información sobre procesos protegidos del componente al Agente de seguridad.

Después de que el servicio de prevención de exploits de Kaspersky Security se detiene, Kaspersky Embedded Systems Security 2.2 continúa protegiendo los procesos agregados a la lista de procesos protegidos, y también se carga en procesos agregados recientemente y se aplican todas las técnicas de prevención de exploits disponibles para proteger la memoria de proceso.

Si el servicio de prevención de exploits de Kaspersky Security se detiene, la aplicación no recibirá información sobre eventos que ocurren con procesos protegidos (incluida información sobre ataques de exploits y cancelación de procesos). Además, el Agente no podrá recibir la información sobre la configuración de protección nueva y la adición de procesos nuevos a la lista de procesos protegidos.

Modo de Prevención de exploits

Puede seleccionar uno de los modos siguientes para configurar acciones para reducir los riesgos de que las vulnerabilidades sufran ataques de exploits en procesos protegidos:

- **Finalizar en exploit**: aplique este modo para cancelar un proceso cuando se lleva a cabo un intento de exploit.

  Cuando se detecta un intento de realizar un ataque de exploit en una vulnerabilidad de un proceso del sistema operativo crítico protegido, Kaspersky Embedded Systems Security 2.2 no cancela el proceso independientemente del modo indicado en la configuración del componente Prevención de exploits.

- **Solo notificar sobre el proceso abusado**: aplique este modo para recibir la información sobre casos de exploits en procesos protegidos mediante eventos en la Auditoría de seguridad filtrada.

  Si se selecciona este modo, Kaspersky Embedded Systems Security 2.2 registra todos los intentos de realizar ataques de exploit en las vulnerabilidades al crear eventos.

Configuración de protección de memoria de proceso

► *Para configurar las opciones de protección de la memoria de procesos agregados a la lista de procesos protegidos, realice las siguientes acciones:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configurar** en el bloque **Prevención de exploits**.

   Se abre la ventana **Prevención de exploits**.

4. En la sección **Modo de prevención de exploits**, configure las siguientes opciones:

   - **Evitar exploit de procesos vulnerables**.

     Si se selecciona esta casilla, Kaspersky Embedded Systems Security 2.2 reduce los riesgos de que las vulnerabilidades sufran ataques de exploit en los procesos de la lista de procesos protegidos.

     Si se desactiva esta casilla, Kaspersky Embedded Systems Security 2.2 no protege los procesos del equipo contra exploits.

     De forma predeterminada, la casilla está desactivada.

   - **Finalizar en exploit**.

     Si se selecciona este modo, Kaspersky Embedded Systems Security 2.2 cancela un proceso protegido al detectar un intento de ataque de exploit si una técnica de reducción de impacto activa se ha aplicado al proceso.

   - **Solo notificar sobre el proceso abusado**.

     Si se selecciona este modo, Kaspersky Embedded Systems Security 2.2 informa los exploits al mostrar una ventana de terminal. El proceso puesto en peligro continúa ejecutándose.

     Si Kaspersky Embedded Systems Security 2.2 detecta un ataque de exploit en un proceso crítico mientras se está ejecutando la aplicación en **Finalizar en exploit**, el componente cambia de manera forzada al modo **Solo notificar sobre el proceso abusado**.

5. En la sección **Acciones de prevención**, configure las siguientes opciones:

   - **Notificar sobre procesos abusados mediante Terminal Service.**

     Si se selecciona esta casilla, Kaspersky Embedded Systems Security 2.2 muestra una ventana de terminal con una descripción que explica por qué la protección se activó y una indicación del proceso en el cual se detectó un intento de ataque de exploit.

     Si se desactiva la casilla, Kaspersky Embedded Systems Security 2.2 muestra una ventana de terminal cuando se detectan un intento de ataque de exploit o la cancelación de un proceso en peligro. Una ventana de terminal se muestra sin tener en cuenta el estado del servicio de prevención de exploits de Kaspersky Security. De forma predeterminada, la casilla está activada.

   - **Evitar exploit de procesos vulnerables incluso si el servicio de Kaspersky Security está deshabilitado**.

     Si se selecciona esta casilla, Kaspersky Embedded Systems Security 2.2 reducirá el riesgo de ataques de exploit en vulnerabilidades en los procesos que se ya se hayan iniciado sin tener en cuenta si el servicio de Kaspersky Security se está ejecutando. Kaspersky Embedded Systems Security 2.2 no protegerá a los procesos agregados después de que el servicio de Kaspersky Security se detenga. Después de que el servicio se inicie, la reducción de impacto de exploit se detendrá para todos los procesos.

     Si se desactiva esta casilla, Kaspersky Embedded Systems Security 2.2 no protege a los procesos contra exploits cuando se detiene el servicio de Kaspersky Security.

De forma predeterminada, la casilla está activada.

6. Haga clic en **Aceptar**.

Kaspersky Embedded Systems Security 2.2 guarda y aplica las opciones de protección de memoria de proceso configuradas.

Cómo agregar un proceso para protección

El componente Prevención de exploits protege varios procesos de forma predeterminada. Para excluir los procesos del alcance de la protección, desactive las casillas correspondientes en la lista.

► *Para agregar un proceso a la lista de procesos protegidos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Protección del equipo en tiempo real**, haga clic en el botón **Configurar** en el bloque **Prevención de exploits**.

   Se abre la ventana **Prevención de exploits**.
4. En la pestaña **Procesos protegidos**, haga clic en el botón **Examinar**.

   Se abre la ventana del Explorador de Microsoft Windows.
5. Seleccione el proceso que desea agregar a la lista.
6. Haga clic en el botón **Abrir**.

   Se muestra el nombre de proceso en la línea.
7. Haga clic en el botón **Agregar**.

   El proceso se añadirá a la lista de procesos protegidos.
8. Seleccione el proceso agregado y haga clic en **Configurar técnicas de prevención de exploits**.

   Se abre la ventana **Técnicas de prevención de exploits**.
9. Seleccione una de las opciones para aplicar técnicas de reducción de impacto:
   - **Aplicar todas las técnicas de prevención de exploits disponibles**.

     Si se selecciona esta opción, la lista no se puede modificar. Todas las técnicas disponibles para un proceso se aplican de forma predeterminada.

- **Aplicar las técnicas de prevención de exploits mencionadas para el proceso**.

  Si esta opción se selecciona, puede modificar la lista de técnicas de reducción de impacto aplicadas:

  a. Seleccione las casillas al lado de las técnicas que desea aplicar para proteger el proceso seleccionado.

  b. Seleccione o desactive la casilla de verificación **Aplicar técnica de Reducción de la superficie de ataque**.

10. Configure las opciones de la Técnica de reducción de la superficie de ataque:

    - Ingrese los nombres de los módulos cuyo inicio se bloqueará desde el proceso protegido en el campo **Denegar módulos**.
    - En el campo **No denegar módulos si se inician en la zona de Internet**, seleccione las casillas al lado de las opciones en las cuales desea permitir que se inicien los módulos:
      - Internet
      - Intranet local
      - Sitios web de confianza
      - Sitios restringidos
      - Equipo

    Estas configuraciones solo se aplican a Internet Explorer®.

11. Haga clic en **Aceptar**.

El proceso se añade al alcance de la protección de la tarea.

Técnicas de prevención de exploits

Table 34. Técnicas de prevención de exploits

Técnica de prevención de exploits	Descripción
Prevención de ejecución de datos (DEP)	La prevención de ejecución de datos bloquea la ejecución del código arbitrario en áreas protegidas de la memoria.
Randomización del diseño del espacio de direcciones (ASLR)	Cambia el diseño de estructuras de datos en el espacio de direcciones del proceso.
Protección de sobreescritura del controlador de excepciones estructuradas (SEHOP)	Reemplazo de registros de excepciones o reemplazo del controlador de excepciones.
Asignación de página nula	Prevención de desvío el indicador nulo
Verificación de llamada de la red de LoadLibrary (anti-ROP)	Protección contra DLL de carga desde rutas de la red.
Pilas ejecutables (anti ROP)	Bloqueo de ejecución no autorizada de áreas de las pilas.
Verificación anti RET (anti ROP)	Compruebe que la instrucción de LLAMADA se invoque de manera segura.

Técnica de prevención de exploits	Descripción
Anti traslado de pilas (anti ROP)	La Protección contra el traslado de indicadores de pilas de ESP a una dirección ejecutable.
Monitor de acceso a la función exportar tabla de direcciones simple (Monitor de acceso a EAT y Monitor de acceso a EAT mediante el registro de depuraciones)	Protección de acceso de lectura a la función exportar tabla de direcciones para kernel32.dll, kernelbase.dll y ntdll.dll.
Asignación de Heap Spray (Heapspray)	Protección contra asignación de memoria para ejecutar código malicioso.
Simulación del flujo de ejecución (programación orientada a la anti-devolución)	Detección de cadenas sospechosas de instrucciones (posible gadget ROP) en el componente API de Windows.
Monitor de llamada de IntervalProfiler (Protección del controlador funcional auxiliar [AFDP])	Protección contra elevación de privilegios a través de una vulnerabilidad en el controlador AFD (ejecución de código arbitrario en anillo 0 a través de una llamada de QueryIntervalProfile).
Reducción de la superficie de ataque (ASR)	Bloqueo del inicio de complementos automáticos vulnerables mediante el proceso protegido.
Hollowing antiproceso (Hollowing)	Protección contra creación y ejecución de copias maliciosas de procesos de confianza.
Anti AtomBombing (APC)	Exploit de la tabla de atom global mediante llamadas de procedimiento asíncronas (APC).
Anti CreateRemoteThread (RThreadLocal)	Otro proceso ha creado un subproceso en el proceso protegido.
Anti CreateRemoteThread (RThreadRemote)	El proceso protegido ha creado un subproceso en otro proceso.

Control de actividad local

Esta sección proporciona información sobre la funcionalidad de Kaspersky Embedded Systems Security 2.2 que controla los inicios de aplicaciones, las conexiones mediante dispositivos externos mediante USB y el firewall de Windows.

En este capítulo

Administración del inicio de aplicaciones desde Kaspersky Security Center

Puede autorizar o denegar el inicio de aplicaciones en todos los equipos dentro de la red corporativa creando listas comunes de reglas de Control de inicio de aplicaciones en Kaspersky Security Center para grupos de equipos.

En esta sección

Acerca del uso de un perfil para configurar tareas de Control de inicio de aplicaciones en una directiva de Kaspersky Security Center

Las reglas de Control de inicio de aplicaciones configuradas en la directiva se aplican a todos los equipos dentro del grupo de administración. Si un grupo de administración incluye equipos de diversos tipos, se pueden requerir listas de reglas personalizadas para el Control de inicio de aplicaciones de cada equipo. Puede usar *perfiles de la directiva* para aplicar directivas diferentes a equipos dentro de un solo grupo de administración.

Se recomienda aplicar perfiles de directivas para definir reglas de Control de inicio de aplicaciones para diferentes tipos de equipos dentro de un solo grupo de administración regido por una directiva unificada. Esto permite optimizar la protección de equipos, ya que las reglas especificadas solo abarcan los inicios de aplicaciones que son habituales para este tipo exacto de equipo.

Los perfiles de la directiva se aplican a equipos del grupo de administración según las *etiquetas* asignadas a ellos. Puede configurar un perfil de la directiva para todos los equipos del grupo, que tienen una sola etiqueta.

Encontrará información detallada sobre etiquetas y perfiles de la directiva, así como instrucciones sobre su utilización, en la *Ayuda de Kaspersky Security Center*.

► *Para aplicar un perfil de la directiva en la tarea de Control de inicio de aplicaciones:*

1. En el árbol de la consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**. Expanda el grupo de administración para el cual desea configurar la aplicación de perfiles de la directiva.
2. Asigne etiquetas a cada equipo dentro del grupo de administración según el tipo de equipo. Para ello, realice las siguientes acciones:
   - En el panel de detalles del grupo de administración seleccionado, abra la pestaña **Dispositivos** y seleccione el equipo al cual desea asignar etiquetas. En la ventana **Propiedades: <Nombre del equipo>** seleccionado, seleccione la sección **Etiquetas** y cree una lista de etiquetas. Haga clic en **Aceptar**.
3. Cree un perfil de la directiva y configure su aplicación para proteger equipos dentro del grupo de administración. Para ello, realice las siguientes acciones:
   - En el panel de detalles del grupo de administración seleccionado, abra la pestaña **Directivas** y seleccione la directiva para la cual desea configurar la aplicación de perfiles. En la ventana **Propiedades: <Nombre de la directiva>** de la directiva seleccionada, abra la sección **Perfiles de la directiva** y haga clic en el botón **Agregar** para crear un perfil nuevo. Se abre la ventana **Propiedades: <Nombre del perfil>**. Haga lo siguiente:
     a. En la sección **Reglas de activación**, configure el área de aplicación del perfil y especifique las condiciones en las cuales el perfil se activará.
     b. En la sección **Control de inicio de aplicaciones**, configure las listas de reglas de Control de inicio de aplicaciones para el perfil que está modificando.
     c. Haga clic en **Aceptar**.
4. En la ventana **Propiedades: <Nombre de la directiva>**, haga clic en **Aceptar**.

El perfil configurado se aplicará en la directiva relacionada con la tarea de Control de inicio de aplicaciones.

Configuración de la tarea Control de inicio de aplicaciones

Puede cambiar la configuración predeterminada de la tarea Control de inicio de aplicaciones (ver la tabla a continuación).

Table 35. Configuración de tarea Control de inicio de aplicaciones de forma predeterminada

Configuración	Valor predeterminado	Descripción
Modo de la tarea	**Solo estadísticas**. La tarea registra los eventos de inicio y bloqueo de aplicaciones según las reglas del conjunto. El inicio de aplicaciones no se rechaza.	Puede seleccionar el modo **Activo** para la protección del equipo después de que se genera la lista final de reglas.
Administración de reglas	**Reemplazar las reglas locales con reglas de las directivas**	Puede seleccionar un modo en el cual las reglas especificadas en una directiva se apliquen conjuntamente con las reglas del equipo local.
Área de aplicación de las reglas	La tarea controla el inicio de los archivos ejecutables, los scripts y los paquetes MSI.	Puede especificar tipos de archivos cuyo inicio está controlado por reglas.

Configuración	Valor predeterminado	Descripción
Uso de KSN	Los datos sobre la reputación de la aplicación en KSN no se usan.	Puede usar los datos de la reputación de la aplicación en KSN al ejecutar una tarea de Control de inicio de aplicaciones.
Permitir automáticamente la distribución de software para las aplicaciones y los paquetes mencionados	No aplicado.	Puede permitir la distribución de software usando los instaladores y las aplicaciones especificadas en la configuración. De forma predeterminada, la distribución de software solo se permite cuando se usa el servicio de Windows Installer.
Permitir siempre la distribución de software a través de Windows Installer	Aplicado.	Puede autorizar cualquier instalación o actualización del software si las operaciones se realizan mediante Windows Installer.
Denegar el inicio de intérpretes de comandos sin comando para ejecutar	No aplicado.	Puede denegar el inicio de intérpretes de comandos sin comandos para ejecutar.
Inicio de la tarea	La primera ejecución no está programada.	La tarea de Control de inicio de aplicaciones no se inicia automáticamente cuando se inicia de Kaspersky Embedded Systems Security 2.2. Puede iniciar la tarea manualmente o configurar un inicio programado.

► *Para configurar las opciones generales de la tarea Control de inicio de aplicaciones, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Control de actividad local**, haga clic en el botón **Configurar** en la sección **Control de inicio de aplicaciones**.

   Se abre la ventana **Control de inicio de aplicaciones**.

4. En la pestaña **General**, seleccione la configuración siguiente en la sección **Modo**:

   En la lista desplegable **Modo de la Tarea**, especifique el modo de operación de la tarea.

   En esta lista desplegable, puede seleccionar un modo de la tarea de Control de inicio de aplicaciones:

   - **Activo**. Kaspersky Embedded Systems Security 2.2 usa las reglas especificadas para supervisar cualquier aplicación ejecutada.
   - **Solo estadísticas**. Kaspersky Embedded Systems Security 2.2 no usa las reglas especificadas para supervisar los inicios de aplicaciones, sino que solo registra la información sobre esos inicios en el registro de tareas. Se autoriza el inicio de todos los programas. Puede usar este modo para generar una lista de Reglas de Control de inicio de aplicaciones sobre la base de la información registrada en el registro de tareas.

   De forma predeterminada, la tarea Control de inicio de aplicaciones se ejecuta en el modo **Solo estadísticas**.

- Desactive o seleccione la casilla de verificación **Repetir la acción realizada durante el inicio del primer archivo en todos los inicios subsiguientes de este archivo**.

  La casilla de verificación habilita o deshabilita el control del inicio para los intentos segundos y subsecuentes de iniciar aplicaciones que se basan en la información sobre incidentes almacenada en el caché.

  Si la casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 autoriza o deniega un reinicio de la aplicación según la conclusión que la tarea había enviado en el primer inicio de esta aplicación. Por ejemplo, si las reglas autorizaron el primer inicio de la aplicación, la información sobre esta acción se almacenará en el caché, y el segundo intento y todos los intentos subsecuentes también se autorizarán, sin comprobaciones adicionales.

  Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 analiza una aplicación en cada intento de inicio.

  De forma predeterminada, la casilla está activada.

- Desactive o seleccione la casilla de verificación **Denegar los intérpretes de comandos sin comando para ejecutar**.

  Si se selecciona la casilla de verificación, Kaspersky Embedded Systems Security 2.2 deniega el inicio del intérprete de línea de comando aunque esté permitido el inicio del intérprete. La línea de comandos sin el comando solo se puede iniciar si se cumplen ambas condiciones:

  - Se autoriza el inicio del intérprete de línea de comando.
  - Se autoriza el comando ejecutado.

  Si se desactiva la casilla de verificación, Kaspersky Embedded Systems Security 2.2 solo considera las reglas de autorización para el inicio de la línea de comandos. El inicio se deniega si no se aplica ninguna regla de autorización o el proceso ejecutable no tiene el estado de confianza de KSN. Si se aplica la regla de autorización o el proceso tiene el estado de confianza de KSN, la línea de comandos se puede iniciar con o sin comandos para ejecutar.

Kaspersky Embedded Systems Security 2.2 reconoce los siguientes intérpretes de línea de comandos:

- cmd.exe
- powershell.exe
- python.exe
- perl.exe

5. En la sección **Reglas**, configure las opciones para aplicar reglas:

   a. Haga clic en el botón **Lista de reglas** para agregar reglas de permiso para el control del inicio de la tarea.

   Kaspersky Embedded Systems Security 2.2 no reconoce rutas de acceso que contengan barras invertidas "/". Use la barra invertida “\” para escribir la ruta de acceso correctamente.

   b. Seleccione el modo para aplicar reglas:

   - **Reemplazar las reglas locales con reglas de las directivas**.

     La aplicación aplica la lista de reglas especificada en la directiva para el control de inicio de aplicaciones centralizado de un grupo de equipos. Las listas de reglas locales no se pueden crear, modificar ni aplicar.

   - **Agregar reglas de la directiva a las reglas locales**.

     La aplicación aplica la lista de reglas especificada en una directiva junto con listas de reglas locales. Puede modificar las listas de reglas locales usando la tarea del Generador de reglas de control de inicio de aplicaciones.

   De forma predeterminada, Kaspersky Embedded Systems Security 2.2 aplica dos reglas predeterminadas que habilitan una lista de scripts, paquetes MSI y archivos de inicio basados en un certificado.

6. En la sección **Área de aplicación de las reglas**, especifique la siguiente configuración:

   - **Aplicar reglas a archivos ejecutables**.

     La casilla de verificación habilita y deshabilita el control del inicio de archivos ejecutables del programa.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 autoriza o bloquea el inicio de archivos ejecutables del programa mediante las reglas especificadas cuya configuración especifica archivos ejecutables como área.

     Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 no controla el inicio de los archivos ejecutables de programas mediante reglas especificadas. El inicio de archivos ejecutables del programa se autoriza.

     De forma predeterminada, la casilla está activada.

   - **Supervisar la carga de módulos DLL**.

     La casilla de verificación habilita y deshabilita la supervisión de la carga de módulos DLL

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 autoriza o bloquea las descargas de módulos DLL mediante las reglas especificadas cuya configuración especifica archivos ejecutables como área.

Si esta casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 no supervisa las descargas de módulos DLL mediante las reglas especificadas. La descarga de módulos DLL se autoriza.

La casilla de verificación se habilita si se selecciona la casilla de verificación Aplicar reglas a archivos ejecutables.

De forma predeterminada, la casilla está desactivada.

La supervisión de la descarga de módulos DLL puede afectar el rendimiento del sistema operativo.

- **Aplicar reglas a scripts y paquetes MSI**.

  La casilla de verificación habilita y deshabilita el inicio de scripts y paquetes MSI.

  Si se selecciona esta casilla de verificación, Kaspersky Embedded Systems Security 2.2 autoriza o bloquea la ejecución de scripts y paquetes MSI mediante las reglas especificadas cuya configuración especifica scripts y paquetes MSI como área.

  Si se desactiva la casilla de verificación, Kaspersky Embedded Systems Security 2.2 no controla el inicio de scripts y paquetes MSI mediante las reglas especificadas. Se autoriza el inicio de scripts y paquetes MSI.

  De forma predeterminada, la casilla está activada.

7. En la sección **Uso de KSN**, configure las siguientes opciones de inicio de aplicaciones:

   - **Denegar aplicaciones dudosas según KSN**.

     La casilla de verificación habilita o deshabilita el Control de inicio de aplicaciones según su reputación en KSN.

     Si esta casilla de verificación está seleccionada, Kaspersky Embedded Systems Security 2.2 bloquea la ejecución de cualquier aplicación si tiene estado dudoso en KSN. Las reglas de autorización del Control de inicio de aplicaciones que se aplican a las aplicaciones dudosas en KSN no se activarán. Si selecciona la casilla de verificación, se proporciona protección adicional contra el malware.

     Si se desactiva la casilla de verificación, Kaspersky Embedded Systems Security 2.2 no toma en cuenta la reputación de programas dudosos en KSN y autoriza o bloquea el inicio de acuerdo con las reglas que se aplican a tales programas.

     De forma predeterminada, la casilla está desactivada.

   - **Permitir aplicaciones de confianza según KSN**.

     La casilla de verificación habilita o deshabilita el Control de inicio de aplicaciones según su reputación en KSN.

     Si se selecciona esta casilla de verificación, Kaspersky Embedded Systems Security 2.2 permite que las aplicaciones se ejecuten si tienen estado de confianza según KSN. La denegación de reglas de control de inicio de aplicaciones que se aplican a las aplicaciones de confianza de KSN que tienen una prioridad más alta: si la aplicación se considera de confianza por los servicios de KSN, este inicio de aplicación se rechazará.

     Si se desactiva la casilla de verificación, Kaspersky Embedded Systems Security 2.2 no toma en cuenta la reputación de programas de confianza en KSN y autoriza o bloquea el inicio de acuerdo con las reglas que se aplican a tales programas.

     De forma predeterminada, la casilla está desactivada.

   - Los usuarios o grupos de usuarios permitieron lanzar aplicaciones de confianza en KSN.

8. En la pestaña **Control de distribución de software**, configure las opciones para control de distribución de software (consulte la sección “Configuración del Control de distribución de software”, en la página 185).
9. En la pestaña **Administración de tareas**, configure las opciones de programación de inicio de tareas (consulte la sección “Configuración de las opciones de programación de inicio de tareas”, en la página 123).
10. Haga clic en **Aceptar** en la ventana **Configuración de tareas**.

Kaspersky Embedded Systems Security 2.2 aplica inmediatamente los valores nuevos de configuración a la tarea en ejecución. La información sobre la fecha y la hora en que la configuración se modificó, así como los valores de configuración de la tarea antes y después de la modificación, se guardan en el registro de tareas.

Acerca del control de distribución de software

La generación de reglas de control de inicio de aplicaciones puede ser complicada si además necesita considerar el control de distribución de software en un equipo protegido. Por ejemplo, para equipos donde se realizan actualizaciones automáticas del software instalado. En este caso, se debe actualizar la lista de reglas de permiso después de cada actualización de software para que los archivos creados recientemente se consideren en la configuración de la tarea Control de inicio de aplicaciones. Para simplificar el control de inicio en situaciones de distribución de software, puede usar un subsistema de Control de inicio de aplicaciones.

Un *paquete de distribución de software* (también denominado “paquete”) representa una aplicación de software que se instala en un equipo. Cada paquete contiene al menos una aplicación, y también puede contener archivos individuales, actualizaciones o hasta un comando individuales, además de las aplicaciones, en particular cuando se instala una aplicación o una actualización de software.

El subsistema de Control de distribución de software se implementa como lista de exclusiones adicional. Cuando agrega un paquete de distribución de software a esta lista, la aplicación permitirá la descompresión de estos paquetes de confianza y el inicio automático del software creado o modificado por un paquete de confianza. Los archivos extraídos pueden heredar el atributo de confianza de un paquete de distribución principal. Un *paquete de distribución principal* es un paquete que el usuario añadió a la lista de exclusiones de Control de distribución de software y se convirtió en un paquete de confianza.

Kaspersky Embedded Systems Security 2.2 controla solo ciclos completos de distribución de software. La aplicación no puede procesar correctamente el inicio de archivos que modifica un paquete de confianza si, cuando el paquete se inicia por primera vez, se desactiva el control de distribución de software o no se instala el componente Control de inicio de aplicaciones.

El control de distribución de Software no está disponible si se desactiva la casilla de verificación **Aplicar reglas a archivos ejecutables** en la configuración de la tarea Control de inicio de aplicaciones.

Caché de distribución del software

Kaspersky Embedded Systems Security 2.2 establece una conexión entre paquetes de confianza y archivos creados durante el procedimiento de distribución del software con la ayuda de *caché de distribución del software* generado dinámicamente (denominado también “caché de distribución”). La primera vez que se ejecuta el paquete, Kaspersky Embedded Systems Security 2.2 detecta todos los archivos creados durante el proceso de distribución del software desde este paquete y almacena las sumas de comprobación y las rutas de acceso de los archivos en el caché de distribución. Después se permite de forma predeterminada el inicio de todos los archivos, que se almacenan en el caché de distribución.

No puede revisar, limpiar ni modificar manualmente el caché de distribución mediante la interfaz de usuario. Kaspersky Embedded Systems Security 2.2 completa y controla el caché.

Puede exportar el caché de distribución en el archivo de configuración (en formato XML) y también borrar el caché con opciones de la línea de comandos.

► *Para exportar el caché de distribución a un archivo de configuración, ejecute el siguiente comando:*

```
kavshell appcontrol /config /savetofile:<ruta de acceso completa> /sdc
```

► *Para borrar el caché de distribución, ejecute el siguiente comando:*

```
kavshell appcontrol /config /clearsdc
```

Kaspersky Embedded Systems Security 2.2 actualiza el caché de distribución cada 24 horas. Si se modifican la ruta de acceso entera o la suma de control de un archivo que se permitió anteriormente, la aplicación elimina este registro del archivo del caché de distribución. Si la tarea Control de inicio de aplicaciones se inicia en un modo activo, los inicios adicionales de este archivo se bloquearán.

Procesamiento de archivos extraídos

El atributo de confianza para todos los archivos extraídos del paquete de confianza se hereda la primera vez que se inicia el paquete. Si desactiva la casilla de verificación después del primer inicio, se mantendrá la herencia para todos los archivos extraídos de este paquete. Para reiniciar la herencia aplicada por primera vez para todos los archivos extraídos, debe borrar el caché de distribución y desactivar la casilla de verificación **Permitir el inicio de todos los archivos de la cadena de extracción de este paquete de distribución** antes de volver a iniciar el paquete de distribución de confianza.

Los archivos y los paquetes extraídos creados por un paquete de distribución principal adquieren el atributo de confianza, ya que sus sumas de comprobación se agregan al caché de distribución cuando el paquete de distribución del software de la lista de exclusiones se abre por primera vez. Por lo tanto, el propio paquete de distribución y todos los archivos extraídos de este paquete también serán de confianza. De forma predeterminada, el número de niveles para la herencia del atributo de confianza es ilimitado.

Los archivos extraídos mantendrán el atributo de confianza después del reinicio del sistema operativo.

El procesamiento de archivos se define en la Configuración de Control de distribución de software (consulte la sección “Configuración del Control de distribución de software”, en la página 185) mediante la selección o la desactivación de la casilla de verificación **Permitir el inicio de todos los archivos de la cadena de extracción de este paquete de distribución**.

Por ejemplo, agrega un paquete test.msi que contiene varios otros paquetes y aplicaciones a la lista de exclusiones y selecciona la casilla. En este caso, se permite la ejecución y la extracción de todos los paquetes y las aplicaciones que contiene el paquete test.msi, si contienen otros archivos. Esta situación funciona para archivos extraídos en todos los niveles anidados.

Si agrega un paquete test.msi a la lista de exclusiones y desactiva la casilla de verificación **Permitir el inicio de todos los archivos de la cadena de extracción de este paquete de distribución**, la aplicación asignará el atributo de confianza solo a los paquetes y los archivos ejecutables extraídos directamente de un paquete de confianza principal (anidados en el primer nivel). Las sumas de comprobación de estos archivos se almacenan en el caché de distribución. Todos los archivos anidados en el segundo nivel y superiores serán bloqueados por el principio de denegación predeterminada.

Interacción con la lista de reglas de control de inicio de aplicaciones

La lista de paquetes de confianza del subsistema de control de distribución de software es una lista de exclusiones que amplifica pero no reemplaza la lista general de reglas de control de inicio de aplicaciones.

Las reglas de denegación de control de inicio de aplicaciones tienen la prioridad más alta: se bloqueará la descompresión del paquete de confianza y el inicio de archivos nuevos o modificados si estos paquetes y archivos están afectados por las reglas de denegación de control del inicio de aplicaciones.

Las exclusiones de control de distribución de software se aplican tanto para paquetes de confianza como para archivos creados o modificados por estos paquetes si no se aplica ninguna regla de denegación en la lista de control de inicio de aplicaciones para esos paquetes y archivos.

Uso de las conclusiones de KSN

Las conclusiones de KSN dudosas tienen una prioridad más alta que las exclusiones de control de distribución de software: se bloqueará la descompresión de un paquete de confianza o el inicio de archivos creados y modificados por este paquete si se recibe de KSN la conclusión de que estos archivos no son de confianza.

Configuración del Control de distribución de software

► *Para agregar un paquete de distribución de confianza, realice las siguientes acciones:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Control de actividad local**, haga clic en el botón **Configurar** en la sección **Control de inicio de aplicaciones**.

   Se abre la ventana **Control de inicio de aplicaciones**.
4. En la pestaña seleccionada, seleccione la casilla de verificación **Permitir automáticamente la distribución de software para las aplicaciones y los paquetes mencionados**.

   La casilla de verificación habilita o deshabilita la creación automática de exclusiones para todos los archivos iniciados y utiliza los paquetes de distribución especificados en la lista.

   Si la casilla está marcada, la aplicación automáticamente permite que se inicien los archivos en los paquetes de distribución de confianza. La lista de aplicaciones y paquetes de distribución autorizadas para ser iniciados se puede editar.

   Si la casilla de verificación está desactivada, la aplicación no aplica las exclusiones especificadas en la lista.

   De forma predeterminada, la casilla está desactivada.

Puede seleccionar **Permitir automáticamente la distribución de software para las aplicaciones y los paquetes mencionados** si la casilla de verificación **Aplicar reglas a archivos ejecutables** está seleccionada en la configuración de la tarea **Control de inicio de aplicaciones**.

5. Desactive la casilla de verificación **Permitir siempre la distribución de software a través de Windows Installer** si es necesario.

   La casilla de verificación habilita o deshabilita la creación automática de exclusiones para todos los archivos ejecutados mediante Windows Installer.

   Si la casilla está seleccionada, la aplicación siempre permitirá que se inicien los archivos instalados mediante Windows Installer.

   Si la casilla de verificación está desactivada, la aplicación no estará autorizada incondicionalmente, aunque sea iniciada por medio de Windows Installer.

   De forma predeterminada, la casilla está activada.

   La casilla de verificación no se puede modificar si la casilla **Permitir la distribución automática de software para los paquetes de la lista** no está seleccionada.

Solo se recomienda desactivar la casilla **Permitir siempre la distribución de software a través de Windows Installer** si es absolutamente necesario. Desactivar esta función puede causar errores al actualizar archivos del sistema operativo y también impedir que se inicien archivos extraídos de un paquete de distribución.

6. Si es necesario, seleccione **Permitir siempre la distribución de software a través de SCCM mediante Background Intelligent Transfer Service**.

   La casilla activa o desactiva la distribución automática del software mediante el Administrador de configuración del Centro del sistema.

   Si se selecciona la casilla, Kaspersky Embedded Systems Security 2.2 permite automáticamente la implementación de Microsoft Windows mediante el Administrador de configuración de System Center. La aplicación permite a distribución del software únicamente mediante el Servicio de Transferencia Inteligente en Segundo Plano.

   Los controles de aplicaciones inician los objetos con las extensiones siguientes:

   - .exe
   - .msi

   De forma predeterminada, la casilla está desactivada.

La periodicidad de distribución del software de controles de aplicaciones en el equipo desde la entrega del paquete hasta la instalación/actualización. La aplicación no controla procesos si alguna de las etapas de distribución se realizara antes de la instalación de la aplicación en el equipo.

7. Para modificar la lista de paquetes de distribución de confianza, haga clic en **Modificar la lista de paquetes** y seleccione uno de los siguientes métodos en la ventana que se abre:

   - **Agregar un paquete de distribución**.

     a. Haga clic en el botón **Examinar** y seleccione el archivo ejecutable o el paquete de distribución.

        La sección **Criterios de confianza** se completa automáticamente con datos sobre el archivo seleccionado.

     b. Desactive o seleccione la casilla de verificación **Permitir el inicio de todos los archivos de la cadena de extracción de este paquete de distribución**.

c. Seleccione una de dos opciones disponibles para criterios para usar para determinar si un archivo o el paquete de distribución es de confianza:

- **Usar certificado digital**

  Si esta opción está seleccionada, se especifica la presencia de un certificado digital como el criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación ahora autorizará el inicio de programas que se inician mediante archivos con un certificado digital. Esta opción se recomienda si desea autorizar el inicio de alguna aplicación de confianza en el sistema operativo.

- **Usar hash SHA256**

  Si esta opción está seleccionada, el valor de la suma de control del archivo, que se usa para generar la regla, se especifica como el criterio de activación de la regla en la configuración de las reglas de autorización recientemente generadas para el Control de inicio de aplicaciones. La aplicación autorizará el inicio de programas que se inicien mediante archivos con el valor de suma de control especificado.

  Esta opción se recomienda para los casos en los que se requieren reglas generadas para cumplir el nivel de seguridad superior: La suma de control de SHA256 puede aplicarse como una Id. de archivo única. El uso de la suma de control de SHA256 como un criterio de activación de la regla limita el área de aplicación de la regla a un archivo.

  De forma predeterminada, esta opción está seleccionada.

- **Agregar varios paquetes por hash**.

  Puede seleccionar un número ilimitado de archivos de ejecutables y paquetes de distribución, y agregarlos a la lista al mismo tiempo. Kaspersky Embedded Systems Security 2.2 examina el hash y permite que el sistema operativo inicie los archivos especificados.

- **Cambiar el paquete seleccionado**.

  Use esta opción para seleccionar otro archivo de inicio o paquete de distribución, o bien para cambiar los criterios de confianza.

- **Importar lista de paquetes de distribución desde el archivo**.

  Puede importar la lista de paquetes de distribución de confianza desde el archivo de configuración. El archivo reconocido por Kaspersky Embedded Systems Security 2.2 debe cumplir con los siguientes parámetros:

  - El archivo tiene una extensión del texto.
  - El archivo contiene información estructurada como una lista de líneas, donde cada línea incluye datos para uno de los archivos de confianza.
  - El archivo debe contener una lista en uno de los formatos siguientes:
    - <nombre de archivo>: <hash SHA256>.
    - <hash SHA256> * <nombre de archivo>.

  En la ventana **Abrir**, especifique el archivo de configuración que contiene una lista de paquetes de distribución de confianza.

8. Si desea eliminar una aplicación o un paquete de distribución anteriormente agregados a la lista de confianza, haga clic en el botón **Eliminar paquetes de distribución**. Se podrán ejecutar los archivos extraídos.

   Para impedir que los archivos extraídos se inicien, desinstale la aplicación en el equipo protegido o cree una regla de denegación en la configuración de la tarea Control de inicio de aplicaciones.

9. Haga clic en **Aceptar**.

Se guardaron las opciones configuradas recientemente.

Habilitación del modo Habilitación predeterminada

El modo Habilitación predeterminada permite el inicio de todas las aplicaciones que no están bloqueadas por reglas o conclusiones de KSN dudosas. Para activar el modo Habilitación predeterminada, agregue reglas de permiso específicas. Puede activar Habilitación predeterminada solo para scripts o para todos los archivos ejecutables.

► *Para agregar una regla de Habilitación predeterminada:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.

3. En la sección **Control de actividad local**, haga clic en el botón **Configurar** en el bloque **Control de inicio de aplicaciones**.
4. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas de Control de inicio de aplicaciones**.
5. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione la opción **Agregar una regla**.

   Se abre la ventana **Configuración de regla**.
6. En el campo **Nombre**, ingrese el nombre de la regla.
7. En la lista desplegable **Tipo**, seleccione el tipo de regla **De autorización**.
8. En la lista desplegable **Área**, seleccione el tipo de archivos cuya ejecución será controlada por la regla:
   - **Archivos ejecutables** si desea que la regla controle el inicio de archivos ejecutables de aplicaciones.
   - **Scripts y paquetes MSI** si desea que la regla controle el inicio de scripts y paquetes MSI.

9. En la sección **Criterio de activación de la regla**, seleccione una opción para **Ruta de acceso al archivo**.
10. Escriba la siguiente máscara: **?:**
11. Haga clic en **Aceptar** en la ventana **Configuración de regla**.

Kaspersky Embedded Systems Security 2.2 aplica el modo de Habilitación predeterminada.

Acerca de la generación de reglas de Control de inicio de aplicaciones para todos los equipos en Kaspersky Security Center

Puede crear listas de reglas de Control de inicio de aplicaciones usando tareas y directivas de Kaspersky Security Center para todos los equipos y los grupos de equipos en la red corporativa a la vez. Esta situación se recomienda si la red corporativa no tiene una máquina de referencia y no puede crear una lista común de reglas usando una tarea para generar automáticamente reglas de permiso según las aplicaciones instaladas en la máquina de referencia.

El componente Control de inicio de aplicaciones se instala con dos reglas de permiso predefinidas:

- Regla de autorización para scripts y MSI con certificado de sistema operativo de confianza.
- Regla de autorización para archivos ejecutables con certificado de sistema operativo de confianza.

Puede crear listas de reglas de Control de inicio de aplicaciones del lado de Kaspersky Security Center de dos modos:

- Con una tarea de grupo de Generador de reglas de control de inicio de aplicaciones para el Control de inicio de aplicaciones.

  Cuando se utiliza este escenario, una tarea de grupo genera su propia lista de reglas de Control de inicio de aplicaciones para cada equipo en la red y guarda esas listas a un archivo XML en la carpeta de red compartida especificada. Luego, puede importar manualmente la lista creada de reglas en la tarea de Control de inicio de aplicaciones de la directiva de Kaspersky Security Center. Puede configurar una directiva de Kaspersky Security Center para el agregado automático de las reglas creadas a la lista de reglas de Control de inicio de aplicaciones cuando se completa la tarea de grupo del Generador de reglas de control de inicio de aplicaciones.

  Este escenario se recomienda cuando tiene que crear listas de la regla de Control de inicio de aplicaciones rápidamente. Se recomienda configurar el inicio planificado de la tarea de Generador de reglas de control de inicio de aplicaciones solo si el área de aplicación de las reglas de autorización incluye carpetas y archivos que usted sabe que están seguros.

  > Antes de usar la directiva de Control de inicio de aplicaciones en la red, asegúrese de que todos los equipos protegidos puedan acceder a una carpeta de red compartida. Si la directiva de la organización no asegura el uso de una carpeta de red compartida en la red, se recomienda iniciar la tarea Generadores automáticos de reglas para reglas de control del equipo del grupo del equipo de prueba o de una máquina modelo.

- Según un informe sobre los eventos de tareas generadas en Kaspersky Security Center para la operación de la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas**.

  Cuando se utiliza este escenario, Kaspersky Embedded Systems Security 2.2 no deniega inicios de aplicaciones, pero mientras el Control de inicio de aplicaciones se ejecuta en modo **Solo estadísticas**, informa todos los inicios de aplicaciones permitidos y denegados en todos los equipos de red en la sección **Eventos** de Kaspersky Security Center. Kaspersky Security Center genera una lista unificada de eventos de inicios de aplicaciones denegados según el registro de tareas.

Debe configurar el periodo de ejecución de tareas de modo que todos los escenarios de operación posibles de equipos protegidos y grupos de equipos y, al menos, un reinicio se realicen durante el periodo especificado. Luego, a medida que las reglas se agreguen a la tarea de Control de inicio de aplicaciones, puede importar datos en inicios de aplicaciones desde el archivo de informe de eventos de Kaspersky Security Center guardado (en formato TXT) y generar reglas de autorización de Control de inicio de aplicaciones para tales aplicaciones según estos datos.

Este escenario se recomienda si una red corporativa incluye una gran cantidad de equipos de tipos diferentes (consulte la sección “Acerca del uso d perfiles para configurar tareas de Control de inicio de aplicaciones en directivas de Kaspersky Security Center”, en la página 177) (con un conjunto de software diferente instalado).

- Según los eventos de inicios de aplicaciones denegados que se recibieron a través de Kaspersky Security Center, sin crear ni importar un archivo de configuración.

  Para usar esta función, la tarea Control de Inicio de aplicaciones en el equipo local se debe ejecutar bajo una directiva de Kaspersky Security Center activa. En este caso, todos los eventos en el equipo local se envían al Servidor de administración.

Se recomienda actualizar la lista de reglas cuando el conjunto de aplicaciones instaladas en equipos de red cambia (por ejemplo, cuando se instalan actualizaciones o se reinstalan sistemas operativos). Se recomienda usar la tarea Generador de reglas de control de inicio de aplicaciones o la directiva de Control de inicio de aplicaciones en el modo **Solo estadísticas**, se ejecuta en equipos en el grupo de administración de prueba, a fin de generar una lista actualizada de reglas. El grupo de administración de prueba incluye equipos requeridos para el inicio de prueba de aplicaciones nuevas antes de que se instalen en equipos de red.

Antes de agregar reglas de permiso, seleccione uno de los modos de aplicación de la regla disponibles (consulte la sección “Configuración de la tarea Control de inicio de aplicaciones”, en la página 178). La lista de reglas de la directiva de Kaspersky Security Center muestra solo esas reglas que son especificadas por la directiva, sin tener en cuenta el modo de aplicación de la regla. La lista de reglas locales muestra todas las reglas aplicadas, tanto reglas locales como reglas agregadas a través de una directiva.

En esta sección

Creación de reglas de autorización desde eventos de Kaspersky Security Center

► *Para generar reglas de permiso para aplicaciones con la opción ‘Crear reglas de autorización de aplicaciones desde los eventos de Kaspersky Security Center’ en el Control de inicio de aplicaciones, haga lo siguiente:*

1. En la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Amplíe el grupo de administración cuya configuración de la directiva desea configurar y seleccione la

pestaña **Directivas** en el panel de detalles.

3. Seleccione **Propiedades** en el menú contextual de la directiva que desea configurar.

   Se abre la ventana **Propiedades: <Nombre de la directiva>**.

4. En la sección **Control de actividad local**, haga clic en el botón **Configurar** en el bloque **Control de inicio de aplicaciones**.

5. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas de Control de inicio de aplicaciones**.

6. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Crear reglas de autorización de aplicaciones desde los eventos de Kaspersky Security Center**.

7. Seleccione el principio para agregar las reglas a la lista de reglas de control de inicio de aplicaciones:

   - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
   - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
   - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

   Se abre la ventana **Generación de reglas de Control de inicio de aplicaciones**.

8. Configure las siguientes opciones de solicitud:

   - **Dirección del servidor de administración**
   - **Puerto**
   - **Usuario**
   - **Contraseña**

9. Seleccione los tipos de eventos en los cuales desea basar la tarea de generación:

   - **Modo Solo estadísticas: inicio de aplicación denegado**.
   - **Inicio de la aplicación denegado**.

10. Seleccione el periodo en la lista desplegable **Eventos de solicitud generados dentro del periodo**.

11. Haga clic en el botón **Generar reglas**.

12. Haga clic en el botón **Guardar** en la ventana **Reglas de control de inicio de aplicaciones**.

    La lista de reglas en la directiva de Control de inicio de aplicaciones se completará con reglas nuevas generadas según un dato de sistema del equipo con la Consola de administración de Kaspersky Security Center instalada.

    Si la lista de reglas de control del inicio de aplicaciones ya se especificó en la directiva, Kaspersky Embedded Systems Security 2.2 agrega las reglas seleccionadas desde los eventos que bloquean las reglas ya especificadas. Las reglas con el mismo hash no se agregan, ya que todas las reglas de una lista deben ser únicas.

Importación de reglas de Control de inicio de aplicaciones desde un archivo XML

Puede importar informes generados después de la finalización de la tarea de grupo de Generador de reglas de

control de inicio de aplicaciones y aplicarlos como una lista de reglas de autorización en la directiva que está configurando.

Cuando la tarea de grupo de Generador de reglas de control de inicio de aplicaciones finaliza, la aplicación exporta las reglas de autorización creadas a archivos XML guardados en la carpeta de red compartida especificada. Cada archivo con la lista de reglas se crea según el análisis de los archivos ejecutados y las aplicaciones iniciadas en cada equipo independiente en la red corporativa. Las listas contienen reglas de autorización para archivos y aplicaciones cuyo tipo coincide con el tipo especificado en la tarea de grupo de Generador de reglas de control de inicio de aplicaciones.

El proceso de configurar las opciones de los componentes funcionales de Kaspersky Embedded Systems Security 2.2 en Kaspersky Security Center es similar al de la configuración local de estos componentes en la Consola de la aplicación. Se proporcionan instrucciones detalladas sobre cómo establecer la configuración de tareas y las funciones de aplicaciones en las secciones relevantes de la *Guía del usuario de Kaspersky Embedded Systems Security 2.2*.

► *Para especificar reglas de autorización para el inicio de la aplicación para un grupo de equipos según una lista de reglas de autorización generada automáticamente, siga estos pasos.*

1. En la pestaña **Tareas** en el panel de control del grupo de equipos que está configurando, cree una tarea de grupo de Generador de reglas de control de inicio de aplicaciones o seleccione una tarea existente.
2. En las propiedades de la tarea de grupo de Generador de reglas de control de inicio de aplicaciones creada o en el asistente de tareas, especifique la siguiente configuración:
   - En la sección **Notificación**, configure las opciones para guardar el informe de ejecución de la tarea.

     Para obtener instrucciones detalladas sobre la configuración de opciones en esta sección, consulte la *Ayuda de Kaspersky Security Center*.

   - En la sección **Configuración**, especifique los tipos de aplicaciones cuyo inicio será autorizado por las reglas que se crean. Puede modificar el contenido de las carpetas que contienen aplicaciones autorizadas: excluya carpetas predeterminadas del área de la tarea o agregue carpetas nuevas manualmente.
   - En la sección **Opciones**, especifique las operaciones de la tarea mientras se está ejecutando y después de que se complete. Especifique el criterio según el cual se generarán las reglas y el nombre del archivo al cual estas reglas se exportarán.
   - En la sección **Programación**, configure las opciones de programación de inicio de tareas.
   - En la sección **Cuenta**, especifique la cuenta de usuario conforme a la cual se ejecutará la tarea.
   - En la sección **Exclusiones del área de la tarea**, especifique los grupos de equipos que deben excluirse del área de la tarea.

     Kaspersky Embedded Systems Security 2.2 no crea reglas de autorización para las aplicaciones iniciadas en los equipos excluidos.

3. En la pestaña **Tareas** en el panel de control del grupo de equipos configurados, en la lista de tareas de grupo, seleccione el Generador de reglas de control de inicio de aplicaciones que creó y haga clic en el

botón **Iniciar** para iniciar la tarea.

Cuando la tarea se completa, las listas de reglas de autorización generadas automáticamente se guardan en una carpeta de red compartida en archivos XML.

> Antes de usar la directiva de Control de inicio de aplicaciones en la red, asegúrese de que todos los equipos protegidos puedan acceder a una carpeta de red compartida. Si la directiva de la organización no asegura el uso de una carpeta de red compartida en la red, se recomienda iniciar la tarea Generadores automáticos de reglas para reglas de control del equipo del grupo del equipo de prueba o de una máquina modelo.

4. Agregue las listas de reglas de autorización generadas a la tarea de Control de inicio de aplicaciones. Para hacerlo, en las propiedades de la directiva configurada, en la configuración de la tarea de Control de inicio de aplicaciones, realice lo siguiente:
   a. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

      Se abre la ventana **Reglas de Control de inicio de aplicaciones**.
   b. Haga clic en el botón **Agregar** y, en la lista que se abre, seleccione **Importar reglas desde archivo XML**.
   c. Seleccione el principio para agregar las reglas de autorización generadas automáticamente a la lista de reglas de Control de inicio de aplicaciones creadas anteriormente:
      - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
      - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
      - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.
   d. En la ventana estándar de Microsoft Windows que se abre, seleccione archivos de XML creados después de la finalización de la tarea de grupo de Generador de reglas de control de inicio de aplicaciones.
   e. Haga clic en **Aceptar** en las ventanas **Reglas de Control de inicio de aplicaciones** y **Configuración de tareas**.
5. Si desea aplicar las reglas creadas para controlar el inicio de aplicaciones, en la directiva en las propiedades de la tarea Control de inicio de aplicaciones, seleccione el modo de ejecución de la tarea **Activo**.

Las reglas de autorización generadas automáticamente según ejecuciones de la tarea en cada equipo independiente se aplican a todos los equipos de red abarcados por la directiva configurada. En estos equipos, la aplicación permitirá iniciar solo las aplicaciones para las cuales se crearon reglas de autorización.

Importación de reglas desde el archivo de informe de Kaspersky Security Center sobre aplicaciones bloqueadas

Puede importar datos de inicios de la aplicación bloqueada desde el informe generado en Kaspersky Security Center después de la finalización de la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas** y usar estos datos para generar una lista de reglas de autorización de Control de inicio de aplicaciones en la directiva configurada.

Al generar el informe sobre eventos que ocurren durante una tarea de Control de inicio de aplicaciones, puede

hacer un seguimiento de las aplicaciones cuyo inicio se bloquea.

Al importar datos del informe sobre aplicaciones bloqueadas en la configuración de la directiva, asegúrese de que la lista que está usando solo contenga aplicaciones cuyo inicio desea autorizar.

► *Para especificar reglas de autorización para el inicio de la aplicación para un grupo de equipos según el informe de aplicaciones bloqueadas de Kaspersky Security Center, siga estos pasos:*

1. En las propiedades de la directiva, en la configuración de la tarea de Control de inicio de aplicaciones, seleccione el modo de operación **Solo estadísticas**.
2. En las propiedades de la directiva, en la sección **Eventos**, asegúrese de que:
   - La pestaña **Eventos críticos** del evento de Inicio de la aplicación denegado muestra un tiempo de almacenamiento del evento que supera el tiempo planificado de la operación de la tarea en el modo **Solo estadísticas** (el valor predeterminado es 30 días).
   - La pestaña **Advertencia** del evento *Solo estadísticas: inicio de aplicación denegado* muestra un tiempo de almacenamiento del evento que supera el tiempo planificado de la operación de la tarea en el modo **Solo estadísticas** (el valor predeterminado es 30 días).

   Cuando el periodo especificado en la columna **Tiempo de almacenamiento** se agota, la información sobre los eventos registrados se elimina y no se refleja en el archivo del informe. Antes de ejecutar la tarea de Control de inicio de aplicaciones en el modo **Solo estadísticas**, asegúrese de que el tiempo de ejecución de la tarea no supere el tiempo de almacenamiento configurado para los eventos especificados.
3. Cuando la tarea se haya completado, exporte los eventos registrados a un archivo TXT:
   a. Para hacerlo, en las propiedades de la tarea Control de Inicio de aplicaciones, expanda el nodo **Registros y notificaciones**.
   b. En el nodo secundario **Eventos**, cree una selección de eventos basada en el criterio *Bloqueado* para ver las aplicaciones cuyo inicio bloqueará la tarea Control de inicio de aplicaciones.
   c. En el panel de detalles de la selección, haga clic en la lista **Exportar eventos a archivo** para guardar el informe sobre inicios de la aplicación bloqueados a un archivo TXT.

   Antes de importar y aplicar el informe generado en una directiva, asegúrese de que el informe solo contenga datos de las aplicaciones cuyo inicio desea autorizar.
4. Importe datos sobre inicios de aplicación bloqueados en la tarea de Control de inicio de aplicaciones. Para hacerlo, en las propiedades de la directiva en la configuración de la tarea de Control de inicio de aplicaciones, realice lo siguiente:
   a. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

      Se abre la ventana **Reglas de Control de inicio de aplicaciones**.
   b. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Importar datos sobre aplicaciones bloqueadas del informe de Kaspersky Security Center**.
   c. Seleccione el principio para agregar reglas desde la lista creada sobre la base del informe de Kaspersky Security Center a la lista de reglas de Control de inicio de aplicaciones configuradas anteriormente:
      - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes.

Las reglas con configuración idéntica se duplican.

- **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
- **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

d. En la ventana estándar de Microsoft Windows que se abre, seleccione el archivo TXT al cual se exportaron los eventos del informe de inicios de aplicación bloqueados.

e. Haga clic en **Aceptar** en las ventanas Reglas de Control de inicio de aplicaciones y **Configuración de tareas**.

Las reglas creadas sobre la base del informe de Kaspersky Security Center sobre aplicaciones bloqueadas se agregan a la lista de reglas de Control de inicio de aplicaciones.

Administración de conexiones de dispositivos mediante Kaspersky Security Center

Puede autorizar o restringir conexiones de unidades flash y otros dispositivos de almacenamiento masivo a todos los equipos de red mediante la generación de listas de control del equipo unificadas mediante Kaspersky Security Center para los grupos de equipos.

En esta sección

Acerca de la tarea Control de dispositivos

Kaspersky Embedded Systems Security 2.2 controla el registro y el uso de dispositivos de almacenamiento masivo y unidades de CD/DVD para proteger el equipo contra amenazas de la seguridad informática, que pueden ocurrir en el proceso de intercambio de archivos con unidades flash u otro tipo de dispositivos externos conectados mediante USB. Los dispositivos de almacenamiento masivo son dispositivos externos que pueden estar conectados a un equipo para copiar o almacenar archivos.

Kaspersky Embedded Systems Security 2.2 controla las siguientes conexiones de dispositivos externos de USB:

- Unidades flash conectadas mediante USB
- Unidades CD-ROM
- Unidades de discos flexibles conectadas mediante USB

- Dispositivos móviles MTP conectados mediante USB

Kaspersky Embedded Systems Security 2.2 le informa sobre todos los dispositivos conectados mediante USB con el correspondiente evento en los registros de tareas y eventos. Los detalles de los eventos incluyen el tipo de dispositivo y la ruta de acceso de la conexión. Cuando se inicia la tarea de control de dispositivos, Kaspersky Embedded Systems Security 2.2 comprueba y enumera todos los dispositivos conectados mediante USB. Puede configurar las notificaciones en la sección de configuración de la notificación de Kaspersky Security Center.

La tarea Control de dispositivos supervisa todos los intentos de conexiones de dispositivos externos a un equipo protegido mediante USB y bloquea la conexión si no hay reglas de autorización para tales dispositivos. Después de que se bloquea la conexión, el dispositivo no está disponible.

La aplicación asigna uno de los siguientes estados a cada dispositivo de almacenamiento masivo conectado:

- *Confiable*. Dispositivo para el cual desea permitir el intercambio de archivos. Después de la generación de la lista de reglas, el valor de la ruta de acceso a la instancia del dispositivo se incluye en el área de uso para al menos una regla.
- *Dudoso*. Dispositivo para el cual desea restringir el intercambio de archivos. La ruta de acceso a la instancia del dispositivo no se incluye en ninguna área de aplicación de las reglas de autorización.

Puede crear reglas de autorización para que el dispositivo externo autorice el intercambio de datos a través del uso de la tarea de Generador de reglas para Control de dispositivos. También puede ampliar el área de aplicación de las reglas ya especificadas. No puede crear reglas de autorización manualmente.

Kaspersky Embedded Systems Security 2.2 identifica dispositivos de almacenamiento masivo registrados en el sistema con el valor *Ruta de acceso a la instancia del dispositivo*. La ruta de acceso a la instancia del dispositivo es una función predeterminada especificada únicamente para cada dispositivo externo. El valor de la ruta de acceso a la instancia del dispositivo se especifica para cada dispositivo externo en sus propiedades de Windows, y Kaspersky Embedded Systems Security 2.2 lo determina automáticamente durante la generación de reglas.

La tarea de Control de dispositivos puede funcionar en dos modos:

- **Activo**. Kaspersky Embedded Systems Security 2.2 aplica reglas para controlar la conexión de unidades flash y otros dispositivos externos, y autoriza o bloquea el uso de todos los dispositivos según el principio de denegación predeterminada y las reglas de autorización especificadas. Se autoriza el uso de dispositivos externos de confianza. El uso de dispositivos externos dudosos se bloquea de forma predeterminada.

  Si un dispositivo externo que se considera dudoso se conecta a un equipo protegido antes de que la tarea Control de dispositivos se ejecute en modo Activo, la aplicación no bloquea el dispositivo. Se recomienda desconectar el dispositivo dudoso manualmente o reiniciar el equipo. De lo contrario, el principio Denegar por defecto no se aplicará al dispositivo.

- **Solo estadísticas**. Kaspersky Embedded Systems Security 2.2 no controla la conexión de unidades flash ni otros dispositivos externos, sino que solo registra la información sobre la conexión y el registro de dispositivos externos en un equipo protegido y sobre las reglas de autorización de Control de dispositivos que activan los dispositivos conectados. Se autoriza el uso de todos los dispositivos externos. Este modo está configurado de forma predeterminada.

  Puede aplicar este modo para la generación de reglas basadas en la información registrada durante la

ejecución de la tarea.

Acerca de la generación de reglas de Control de dispositivos para todos los equipos mediante Kaspersky Security Center

Puede crear listas de reglas de Control de dispositivos usando tareas de Kaspersky Security Center para todos los equipos y los grupos de equipos en la red corporativa a la vez.

Puede crear listas de reglas de Control de dispositivos del lado de Kaspersky Security Center de dos modos:

- Con la tarea de grupo de Generador de reglas para Control de dispositivos.

  Según este escenario, la tarea de grupo genera listas de reglas basadas en datos del sistema de cada equipo sobre todos los dispositivos de almacenamiento masivo que alguna vez se hayan conectado a equipos protegidos. La tarea también autoriza todos los dispositivos de almacenamiento masivo que están conectados en el momento de ejecución de la tarea. Después de la finalización de la tarea de grupo, Kaspersky Embedded Systems Security 2.2 genera listas de reglas de autorización para todos los dispositivos de almacenamiento masivo registrados en la red y guarda estas listas en un archivo XML en una carpeta especificada. Luego, puede importar manualmente las reglas generadas en la configuración de la directiva de Control de dispositivos. A diferencia de una tarea en un equipo local, la directiva no permite configurar la adición automática de las reglas creadas a la lista de reglas de Control de dispositivos cuando se completa la tarea de grupo de Generador de reglas de control de inicio de aplicaciones.

  Este escenario se recomienda para generar la lista de reglas de autorización antes del primer inicio de la directiva de Control de dispositivos en el modo de aplicación de reglas activa.

  > Antes de usar la directiva de Control de dispositivos en la red, asegúrese de que todos los equipos protegidos puedan acceder a una carpeta de red compartida. Si la directiva de la organización no asegura el uso de una carpeta de red compartida en la red, se recomienda iniciar la tarea Generadores automáticos de reglas para reglas de control del equipo del grupo del equipo de prueba o de una máquina modelo.

- Según un informe sobre los eventos de tareas generadas en Kaspersky Security Center para la operación de la tarea de Control de dispositivos en el modo **Solo estadísticas**.

  Según este escenario, Kaspersky Embedded Systems Security 2.2 no restringe las conexiones de dispositivos de almacenamiento masivo, sino que registra información sobre todas las conexiones de dispositivos y registro de dispositivos de almacenamiento masivo en todos los equipos de red durante la tarea de Control de dispositivos que se ejecutan en el modo **Solo estadísticas**; la información registrada se puede encontrar en la sección **Eventos** de Kaspersky Security Center. Kaspersky Security Center genera una lista unificada de eventos de autorización y restricción de dispositivos de almacenamiento masivo según el registro de tareas.

  Debe configurar el periodo de la tarea en ejecución de modo que todas las conexiones de dispositivos de almacenamiento masivo se realicen durante el periodo establecido. Luego, a medida que las reglas se agreguen a la tarea de Control de dispositivos, puede importar datos en conexiones de dispositivos desde el archivo de informe de eventos de Kaspersky Security Center guardado (en formato TXT) y generar reglas de autorización de Control de dispositivos para tales dispositivos según estos datos. El tipo de eventos, en los que se basa un registro importado, no influye en el tipo de reglas generado; solo se generan reglas de autorización.

  Este escenario se recomienda para agregar reglas de autorización para un gran número de dispositivos de almacenamiento masivo nuevos, así como para generar reglas para los dispositivos móviles de confianza

conectados a MTP.

- Sobre la base de datos de sistema acerca de dispositivos de almacenamiento masivo conectados (con la opción Generar reglas basadas en datos del sistema en la configuración de la directiva de Control de dispositivos).

  Según este escenario, Kaspersky Embedded Systems Security 2.2 genera reglas de autorización para los dispositivos de almacenamiento masivo que alguna vez se hayan conectado o que estén conectados en ese momento a un equipo con Kaspersky Security Center instalado.

  Este escenario se recomienda para generar reglas para un número pequeño de dispositivos de almacenamiento masivo nuevos en los que desee confiar en todos los equipos en la red.

- En base a datos sobre los dispositivos actualmente conectados (con **Generar reglas basadas en los dispositivos conectados**).

  En esta situación, Kaspersky Embedded Systems Security 2.2 genera reglas de autorización solo para dispositivos conectados actualmente. Puede seleccionar uno o varios dispositivos para los cuales desea generar reglas de autorización.

  Kaspersky Embedded Systems Security 2.2 no accede a datos del sistema sobre los dispositivos móviles conectados mediante MTP. No puede generar reglas de autorización para dispositivos móviles de confianza conectados a MTP con escenarios para el llenado de listas de reglas sobre la base de datos del sistema sobre todos los dispositivos conectados.

Generación de reglas basadas en los datos del sistema sobre dispositivos externos conectados a equipos de red

Puede generar reglas (consulte la sección “Acerca de la generación de reglas de Control de dispositivos para todos los equipos mediante Kaspersky Security Center”, en la página 197) basadas en datos de Windows sobre todos los almacenamiento masivos que se han conectado históricamente o están conectados actualmente según tres escenarios:

- Con la tarea de grupo de Generador de reglas para Control de dispositivos. Use este escenario durante el proceso de generación de reglas para tener en cuenta todos los dispositivos de almacenamiento masivo que alguna vez se hayan conectado y que estén registrados por los sistemas en todos los equipos de red.
- Con la opción **Generar reglas basadas en datos del sistema** en la configuración de la directiva Control de dispositivos. Use este escenario durante el proceso de generación de reglas para tener en cuenta todos los dispositivos de almacenamiento masivo que alguna vez se hayan conectado y que estén registrados por el sistema de un equipo con la Consola de administración de Kaspersky Security Center.
- Usar **Generar reglas basadas en los dispositivos conectados** en la configuración de la directiva del Control de dispositivos y la configuración de la tarea del Generador de reglas para Control de dispositivos. Use este método si desea solo considerar datos sobre dispositivos actualmente conectados al equipo protegido al generar el permiso de reglas.

Kaspersky Embedded Systems Security 2.2 no accede a datos del sistema sobre los dispositivos móviles conectados mediante MTP. No puede generar reglas de autorización para dispositivos móviles de confianza conectados a MTP con escenarios para el llenado de listas de reglas sobre la base de datos del sistema sobre todos los dispositivos conectados.

En esta sección

Creación de reglas con la tarea Generador de reglas para Control de dispositivos

► *Para especificar reglas de control de dispositivos para un grupo de equipos mediante la tarea de Generador de reglas para Control de dispositivos, siga estos pasos.*

1. En la pestaña **Tareas** en el panel de control del grupo de equipos que está configurando, cree una tarea de grupo de Generador de reglas para Control de dispositivos o seleccione una tarea existente.
2. En las propiedades de la tarea de grupo de Generador de reglas de control de inicio de aplicaciones creada o en el asistente de tareas, especifique la siguiente configuración:
   - En la sección **Notificaciones**, configure las opciones para guardar el informe de ejecución de la tarea.
   - En la sección **Configuración**, especifique las operaciones de la tarea después de que se complete. Especifique el nombre del archivo donde se exportarán las reglas generadas.
   - En la sección **Programación**, establezca la configuración de las opciones de programación de inicio de tareas.
3. En la pestaña **Tareas** en el panel de control del grupo de equipos configurados, en la lista de tareas de grupo, seleccione el Generador de reglas para Control de dispositivos que creó y haga clic en el botón **Iniciar** para iniciar la tarea.

   Cuando la tarea se completa, las listas de reglas de autorización generadas automáticamente se guardan en una carpeta de red compartida en archivos XML.

   Antes de usar la directiva de Control de dispositivos en la red, asegúrese de que todos los equipos protegidos puedan acceder a una carpeta de red compartida. Si la directiva de la organización no asegura el uso de una carpeta de red compartida en la red, se recomienda iniciar la tarea Generadores automáticos de reglas para reglas de control del equipo del grupo del equipo de prueba o de una máquina modelo.

4. Agregue las listas de reglas de autorización generadas a la tarea de Control de dispositivos. Para hacerlo, en las propiedades de la directiva configurada, en la configuración de la tarea de Control de dispositivos, realice lo siguiente:
   a. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

      Se abre la ventana **Reglas de control de dispositivos**.

   b. Haga clic en el botón **Agregar** y, en la lista que se abre, seleccione **Importar reglas desde archivo XML**.

   c. Seleccione el principio para agregar las reglas de autorización generadas automáticamente a la lista de reglas de Control de dispositivos creadas anteriormente:
      - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes.

Las reglas con configuración idéntica se duplican.

- **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
- **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

d. En la ventana estándar de Microsoft Windows que se abre, seleccione archivos XML creados después de la finalización de la tarea de grupo de Generador de reglas para Control de dispositivos.

e. Haga clic en **Aceptar** en las ventanas Reglas de control de dispositivos y **Configuración de tareas**.

5. Si desea aplicar reglas generadas de Control de dispositivos, seleccione el modo de la tarea **Activo** en la configuración de la directiva **Control de dispositivos**.

Las reglas de autorización generadas automáticamente según datos del sistema en cada equipo independiente se aplican a todos los equipos de red abarcados por la directiva configurada. En estos equipos, la aplicación permitirá la conexión de solo las dispositivos para los cuales se crearon reglas de autorización.

Creación de reglas de autorización sobre la base de datos de sistema en una directiva de Kaspersky Security Center

► *Para especificar reglas de autorización con la opción **Generar reglas basadas en datos del sistema** en la directiva de Control de dispositivos, siga estos pasos:*

1. Si es necesario, conecte un dispositivo de almacenamiento masivo nuevo en el que desee confiar a un equipo con la Consola de administración de Kaspersky Security Center instalada.
2. En la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
3. Amplíe el grupo de administración cuya configuración de la directiva desea configurar y seleccione la pestaña **Directivas** en el panel de detalles.
4. Seleccione **Propiedades** en el menú contextual de la directiva que desea configurar.
5. Se abre la ventana **Propiedades: <Nombre de la directiva>**.
6. En la configuración de la directiva, abra la configuración de la tarea de Control de dispositivos y siga estos pasos:

   a. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

      Se abre la ventana **Reglas de control de dispositivos**.

   b. Haga clic en el botón **Agregar** y, en el menú contextual que se abre, seleccione la opción **Generar reglas basadas en datos del sistema**.

   c. Seleccione el principio para agregar las reglas de autorización a la lista de reglas de Control de dispositivos creadas anteriormente:

      - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
      - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.
      - **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos

un parámetro de la regla es único.

7. Haga clic en **Aceptar** en las ventanas **Reglas de Control de dispositivos** y **Configuración de tareas**.

La lista de reglas en la directiva de Control de dispositivos se completará con reglas nuevas generadas según un dato de sistema del equipo con la Consola de administración de Kaspersky Security Center instalada.

Generación de reglas para dispositivos conectados

► *Para especificar reglas de autorización con la opción **Generar reglas basadas en datos del sistema** en la directiva de Control de dispositivos, siga estos pasos:*

1. En la Consola de administración de Kaspersky Security Center, expanda el nodo **Dispositivos administrados**.
2. Amplíe el grupo de administración cuya configuración de la directiva desea configurar y seleccione la pestaña **Directivas** en el panel de detalles.
3. Seleccione **Propiedades** en el menú contextual de la directiva que desea configurar.
4. Se abre la ventana **Propiedades: <Nombre de la directiva>**.
5. En la sección **Control de actividad local**, haga clic en el botón **Configurar** en la sección **Control de dispositivos**.
6. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

   Se abre la ventana **Reglas de control de dispositivos**.
7. Haga clic en el botón **Agregar** y, en el menú contextual, seleccione **Generar reglas basadas en los dispositivos conectados**.

   Se abre la ventana **Generar reglas basadas en datos del sistema**.
8. En la lista de dispositivos detectados conectados al equipo protegido, seleccione los dispositivos para los cuales desea generar reglas de autorización.
9. Haga clic en el botón **Agregar reglas para los dispositivos seleccionados**.
10. Haga clic en el botón **Guardar** en la ventana **Control de dispositivos**.

La lista de reglas en la directiva de Control de dispositivos se completará con reglas nuevas generadas según un dato de sistema del equipo con la Consola de administración de Kaspersky Security Center instalada.

Importación de reglas desde el archivo de informe de Kaspersky Security Center sobre dispositivos restringidos

Puede importar datos sobre conexiones de dispositivos restringidos desde el informe generado en Kaspersky Security Center después de la finalización de la tarea de Control de dispositivos en el modo **Solo estadísticas** y usar estos datos para generar una lista de reglas de autorización de Control de dispositivos en la directiva configurada.

Al generar el informe sobre eventos que ocurren durante la tarea de Control de dispositivos, puede hacer un seguimiento de los dispositivos cuya conexión se restringe.

Al importar datos del informe sobre dispositivos restringidos en la configuración de la directiva, asegúrese de que la lista que está usando solo contenga dispositivos cuya conexión desea autorizar.

► *Para especificar reglas de autorización para la conexión de dispositivos para un grupo de equipos según el informe de Kaspersky Security Center sobre dispositivos restringidos, siga estos pasos:*

1. En las propiedades de la directiva, en la configuración de la tarea de Control de dispositivos, seleccione el modo **Solo estadísticas**.
2. En las propiedades de la directiva, en la sección **Eventos**, asegúrese de que:
   - La pestaña **Eventos críticos** del evento *Dispositivos de almacenamiento masivo restringidos* muestra un tiempo de almacenamiento del evento que supera el tiempo planificado de la operación de la tarea en el modo **Solo estadísticas** (el valor predeterminado es 30 días).
   - La pestaña **Advertencia** del evento *Solo estadísticas: dispositivos de almacenamiento masivo dudosos detectados* muestra un tiempo de almacenamiento del evento que supera el tiempo planificado de la operación de la tarea en el modo **Solo estadísticas** (el valor predeterminado es 30 días).

   Cuando el periodo especificado en la columna **Tiempo de almacenamiento** se agota, la información sobre los eventos registrados se elimina y no se refleja en el archivo del informe. Antes de ejecutar la tarea de Control de dispositivos en el modo **Solo estadísticas**, asegúrese de que el tiempo de ejecución de la tarea no supere el tiempo de almacenamiento configurado para los eventos especificados.
3. Cuando la tarea se haya completado, exporte los eventos registrados a un archivo TXT. Para hacerlo, amplíe el nodo **Registros y notificaciones** y, en el nodo secundario **Eventos**, cree una selección de eventos según el criterio *Denegado* para ver los dispositivos cuyo inicio restringirá la tarea de Control de dispositivos. En el panel de detalles de la selección, haga clic en la lista **Exportar eventos a archivo** para guardar el informe sobre inicios de la aplicación bloqueados a un archivo TXT.

   Antes de importar y aplicar el informe generado en una directiva, asegúrese de que el informe solo contenga datos de los dispositivos cuya conexión desea autorizar.
4. Importe datos sobre conexiones de dispositivos restringidos a la directiva de Control de dispositivos. Para hacerlo, en las propiedades de la directiva configurada, en la configuración de la tarea de Control de dispositivos, siga estos pasos:
   a. En la pestaña **General**, haga clic en el botón **Lista de reglas**.

      Se abre la ventana **Reglas de control de dispositivos**.
   b. Haga clic en el botón **Agregar** y, en el menú contextual del botón, seleccione **Importar datos sobre dispositivos bloqueados del informe de Kaspersky Security Center**.
   c. Seleccione el principio para agregar reglas desde la lista creada sobre la base del informe de Kaspersky Security Center a la lista de reglas de Control de dispositivos configuradas anteriormente:
      - **Agregar a reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con configuración idéntica se duplican.
      - **Reemplazar reglas existentes** si desea reemplazar las reglas existentes con las reglas importadas.

- **Combinar con reglas existentes** si desea agregar las reglas importadas a la lista de reglas existentes. Las reglas con una configuración idéntica no se agregan; la regla se agrega si al menos un parámetro de la regla es único.

d. En la ventana estándar de Microsoft Windows que se abre, seleccione el archivo TXT al cual se exportaron los eventos del informe sobre dispositivos restringidos.

e. Haga clic en **Aceptar** en las ventanas **Reglas de Control de dispositivos** y **Configuración de tareas**.

Las reglas creadas sobre la base del informe de Kaspersky Security Center sobre los dispositivos restringidos se agregan a la lista de reglas de Control de dispositivos.

Control de actividad de red

Esta sección contiene la información sobre la tarea de administración de firewall.

Administración de firewall

Esta sección contiene información acerca de la tarea Administración de firewall y cómo configurarla.

En esta sección

Acerca de la tarea Administración de firewall

Kaspersky Embedded Systems Security 2.2 proporciona una solución de confianza y ergonómica para proteger las conexiones de red mediante la tarea Administración de firewall.

La tarea Administración de firewall no realiza un filtrado de tráfico de red independiente, pero permite administrar el firewall de Windows por medio de la interfaz gráfica de Kaspersky Embedded Systems Security 2.2. Durante la tarea Administración de firewall, Kaspersky Embedded Systems Security 2.2 controla la administración de la configuración y de las directivas del firewall del sistema operativo y bloquea cualquier posibilidad de configuración externa del firewall.

Durante la instalación de la aplicación, el componente de Administración de firewall lee y copia el estado del firewall de Windows y todas las reglas especificadas. Después de esto, solo es posible cambiar el conjunto de reglas y los parámetros de reglas, y activar o desactivar el firewall mediante Kaspersky Embedded Systems Security 2.2.

Si el firewall de Windows está desactivado durante la instalación de Kaspersky Embedded Systems Security 2.2, la tarea Administración de firewall no se ejecuta después de que finaliza la instalación. Si el firewall de Windows está activado durante la instalación de la aplicación, la tarea de Administración de firewall se ejecuta después de que la instalación finaliza. De esta manera, se bloquean todas las conexiones de red que las reglas especificadas no autorizan.

El componente de Administración de firewall no se instala de forma predeterminada, ya que no se incluye en el conjunto de componentes para la instalación recomendada.

La tarea de Administración de firewall aplica el bloqueo de todas las conexiones de entrada y de salida que no autorizan las reglas especificadas de la tarea.

La tarea sondea el firewall de Windows periódicamente y supervisa su estado. De forma predeterminada, el intervalo de sondeo está configurado en 1 minuto y no se puede cambiar. Si durante el sondeo, Kaspersky Embedded Systems Security 2.2 descubre diferencias entre la configuración del firewall de Windows y la configuración de la tarea Administración de firewall, la aplicación implementa la configuración de la tarea en el firewall del sistema operativo.

Con el sondeo minuto a minuto del Firewall de Windows, Kaspersky Embedded Systems Security 2.2 supervisa lo siguiente:

- Estado operativo del Firewall de Windows
- Estado de reglas añadidas después de la instalación de Kaspersky Embedded Systems Security 2.2 por otras aplicaciones o herramientas (por ejemplo, la adición de una nueva regla de aplicación para un puerto/aplicación mediante wf.msc).

Al aplicar las nuevas reglas al Firewall de Windows, Kaspersky Embedded Systems Security 2.2 crea un conjunto de reglas de Kaspersky Security Group en el complemento **Firewall de Windows**. Este conjunto de reglas une todas las reglas creadas por Kaspersky Embedded Systems Security 2.2 usando la tarea Administración de firewall. Las reglas de grupo de Kaspersky Security no son supervisadas por la aplicación durante el sondeo cada minuto y no se sincronizan automáticamente con la lista de reglas especificadas en la configuración de la tarea de Administración de firewall.

► *Para actualizar las reglas de grupo de Kaspersky Security manualmente,*

reinicie la tarea Administración de firewall de Kaspersky Embedded Systems Security 2.2.

También puede corregir las reglas de Kaspersky Security Group manualmente mediante el complemento **Firewall de Windows**.

Si el firewall de Windows está controlado por la directiva de grupo de Kaspersky Security Center, la tarea de Administración de firewall no se puede iniciar.

Acerca de las reglas de firewall

La tarea de Administración de firewall controla el filtrado del tráfico de red de entrada y de salida mediante reglas de autorización que se aplican en el firewall de Windows durante la ejecución de la tarea.

La primera vez que la tarea se inicia, Kaspersky Embedded Systems Security 2.2 lee y copia todas las reglas de tráfico de red de entrada especificadas en la configuración del firewall de Windows en la configuración de la tarea Administración de firewall. Luego, la aplicación funciona según las reglas siguientes:

- Si se crea una nueva regla en la configuración del firewall de Windows (de forma manual o automática durante una nueva instalación de aplicación), Kaspersky Embedded Systems Security 2.2 elimina la regla.
- Si se elimina una regla existente de la configuración del firewall de Windows, Kaspersky Embedded Systems Security 2.2 restaura la regla.
- Si se cambian los parámetros de una regla existente en la configuración del firewall de Windows, Kaspersky Embedded Systems Security 2.2 revierte los cambios.
- Si se crea una nueva regla en la configuración de Administración de firewall, Kaspersky Embedded Systems Security 2.2 aplica la regla al firewall de Windows.
- Si se elimina una regla existente de la configuración de Administración de firewall, Kaspersky Embedded Systems Security 2.2 elimina la regla de la configuración del firewall de Windows.

Kaspersky Embedded Systems Security 2.2 no trabaja con reglas de bloqueo ni reglas que controlen el tráfico de red saliente. Cuando se inicia la tarea de Administración de firewall, Kaspersky Embedded Systems Security 2.2 elimina todas reglas de ese tipo de la configuración del firewall de Windows.

Puede configurar, eliminar y editar las reglas de filtrado para el tráfico de red de entrada.

No puede especificar una nueva regla para controlar el tráfico de red saliente en la configuración de la tarea de Administración de firewall. Todas las reglas de firewall especificadas en Kaspersky Embedded Systems Security 2.2 controlan solo el tráfico de red de entrada.

Puede administrar los siguientes tipos de reglas de firewall:

- Reglas de aplicación.
- Reglas de puerto.

Reglas de aplicación

Este tipo de regla permite conexiones de red específicas para aplicaciones determinadas. El criterio de activación para estas reglas se basa en una ruta de acceso a un archivo ejecutable.

Puede administrar las reglas de aplicación:

- Agregar reglas nuevas.
- Eliminar reglas existentes.
- Habilitar y deshabilitar reglas específicas.
- Editar los parámetros de las reglas especificadas: especificar el nombre de la regla, la ruta de acceso del archivo ejecutable y el área de aplicación de la regla.

Reglas de puerto

Este tipo de regla permite las conexiones de red para los puertos y los protocolos especificados (TCP/UDP). Los criterios de activación para estas reglas se basan en el número de puerto y en el tipo de protocolo.

Puede administrar las reglas de puerto:

- Agregar reglas nuevas.
- Eliminar reglas existentes.
- Habilitar y deshabilitar reglas específicas.
- Editar los parámetros de las reglas especificadas: configurar el nombre de regla, el número de puerto, el tipo del protocolo y el área de aplicación de la regla.

Las reglas de puerto implican un área de aplicación más amplia que la de las reglas de aplicación. Al permitir conexiones basadas en las reglas de puerto, se baja el nivel de seguridad del equipo protegido.

Habilitación y deshabilitación de Reglas de firewall

► *Para habilitar o deshabilitar una regla existente para filtrar el tráfico de red de entrada, realice las*

siguientes acciones:

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** en el bloque **Administración de firewall.**
4. Haga clic en el botón **Lista de reglas** en la ventana que se abre.

   Se abre la ventana **Lista de reglas**.
5. Según el tipo de regla cuyo estado desee modificar, seleccione **Aplicaciones** o **Puertos**.
6. En la lista de reglas, seleccione la regla cuyo estado desee modificar y realice una de las acciones siguientes:
   - Si desea habilitar una regla deshabilitada, seleccione la casilla de verificación ubicada a la izquierda del nombre de la regla.

     La regla seleccionada se habilitará.
   - Si desea deshabilitar una regla habilitada, desactive la casilla de verificación ubicada a la izquierda del nombre de la regla.

     La regla seleccionada se deshabilitará.
7. Haga clic en **Guardar** en la ventana **Lista de reglas**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Cómo agregar manualmente reglas de firewall

Solo puede agregar y editar reglas para aplicaciones y para puertos. No puede agregar reglas de grupo nuevas ni editar las existentes.

► *Para agregar una regla nueva o editar una existente para filtrar el tráfico de red de entrada, realice lo siguiente:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección "Configuración de directivas", en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección "Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center", en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** en el bloque **Administración de firewall**.
4. Haga clic en el botón **Lista de reglas** en la ventana que se abre.

   Se abre la ventana **Lista de reglas**.
5. Según el tipo de regla que desee agregar, seleccione la pestaña **Aplicaciones** o **Puertos** y realice una de las acciones siguientes:
   - Para editar una regla existente, seleccione la regla que desee editar en la lista de reglas y haga clic en **Editar**.
   - Para agregar una nueva regla, haga clic en **Agregar**.

     Según el tipo de regla que se vaya a configurar, se abre la ventana **Regla de puerto** o la de **Regla de aplicación**.
6. En la ventana que se abre, realice las siguientes operaciones:
   - Si está trabajando con una regla de aplicación, realice lo siguiente:
     a. Ingrese el **Nombre de regla** de la regla editada.
     b. Especifique la **Ruta de acceso de la aplicación** del archivo ejecutable de la aplicación para la cual se está autorizando una conexión mediante la modificación de esta regla.

        Puede configurar la ruta de acceso manualmente o mediante el botón **Examinar**.
     c. En el campo **Área de aplicación de la regla**, especifique las direcciones de red para las cuales se aplicará la regla modificada.

        Solo puede usar direcciones IP de tipo IPv4.

- Si está trabajando con una regla de puerto, realice lo siguiente:
  a. Ingrese el **Nombre de regla** de la regla editada.
  b. Especifique el **Número de puerto** para el cual la aplicación autorizará las conexiones.
  c. Seleccione el tipo de protocolo (TCP/UDP) para el cual la aplicación autorizará las conexiones.
  d. En el campo **Área de aplicación de la regla**, especifique las direcciones de red para las cuales se aplicará la regla modificada.

  > Solo puede usar direcciones IP de tipo IPv4.

7. Haga clic en **Aceptar** en la ventana **Regla de Aplicación** o **Regla de puerto**.
8. Haga clic en **Guardar** en la ventana **Reglas de firewall**.

Se guarda la configuración de la tarea especificada. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Eliminación de reglas de firewall

> Solo puede eliminar reglas de puerto y de aplicación. No puede eliminar reglas de grupo existentes.

► *Para eliminar una regla existente para filtrar el tráfico de red de entrada, realice las siguientes acciones:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

   > Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Control de actividad de red**, haga clic en el botón **Configurar** en el bloque **Administración de firewall.**
4. Haga clic en el botón **Lista de reglas** en la ventana que se abre.

   Se abre la ventana **Lista de reglas**.
5. Según el tipo de regla cuyo estado desee modificar, seleccione la pestaña **Aplicaciones** o **Puertos**.

6. En la lista de reglas, seleccione la regla que desee eliminar.
7. Haga clic en el botón **Eliminar**.

   La regla seleccionada se elimina.
8. Haga clic en **Guardar** en la ventana **Reglas de firewall**.

Se guardará la configuración especificada para la tarea de Administración de firewall. Los nuevos parámetros de regla se enviarán al firewall de Windows.

Inspección del sistema

Esta sección contiene la información sobre la tarea del Monitor de integridad de archivos y funciones para inspeccionar el registro del sistema operativo.

En este capítulo

Monitor de integridad de archivos

Esta sección contiene información sobre el inicio y la configuración de la tarea Monitor de integridad de archivos.

En esta sección

Acerca de la tarea del Monitor de integridad de archivos

La tarea Monitor de integridad de archivos se diseña para realizar un seguimiento de las acciones realizadas con los archivos y las carpetas especificados en las áreas de aplicación especificadas en la configuración de la tarea. Puede usar la tarea de detectar los cambios en el archivo que podrían indicar una violación de la seguridad en el equipo protegido. También puede configurar que se realice un seguimiento de los cambios en el archivo durante periodos en los cuales la supervisión se interrumpe.

Una *interrupción de supervisión* ocurre cuando el área de supervisión temporalmente queda fuera del área de la tarea, por ejemplo, si la tarea se detiene o si un dispositivo protegido no está físicamente presente en un equipo protegido. Kaspersky Embedded Systems Security 2.2 informa las operaciones con archivos detectadas en el área de supervisión tan pronto como un dispositivo de almacenamiento masivo se conecta de nuevo.

Si las tareas dejan de ejecutarse en el área de supervisión especificada debido a una nueva instalación del componente Monitor de integridad de archivos, esto no constituye una interrupción de supervisión. En este caso, la tarea del Monitor de integridad de archivos no se ejecuta.

Requisitos en el entorno

Para iniciar la tarea del Monitor de integridad de archivos, se deben cumplir las siguientes condiciones:

- Un dispositivo de almacenamiento que admite ReFS y sistemas de archivos NTFS se deben instalar en el equipo protegido.
- Se debe habilitar el diario de USN de Windows. El componente le solicita a este diario recibir la información sobre operaciones con archivos.

Si habilita el diario de USN después de que una regla se haya creado para un volumen y la tarea del Monitor de integridad de archivos se ha iniciado, la tarea se debe reiniciar. Si no, la regla no se aplicará durante la supervisión.

Áreas de supervisión excluidas

Puede crear exclusiones para el área de supervisión (consulte la sección “Configuración de reglas de supervisión”, en la página 216). Las exclusiones se especifican para cada regla independiente y funcionan solo para el área de supervisión indicada. Puede especificar un número ilimitado de exclusiones para cada regla.

Las exclusiones tienen mayor prioridad que el área de supervisión y no son supervisadas por la tarea, aun si una carpeta o el archivo indicado están dentro del área de supervisión. Si la configuración para una de las reglas especifica un área de supervisión a un nivel inferior que una carpeta especificada en exclusiones, el área de supervisión no se considera cuando la tarea se ejecuta.

Para especificar exclusiones, puede usar las mismas máscaras que se usan para especificar áreas de supervisión.

Acerca de las reglas de supervisión de las operaciones con archivos

El Monitor de integridad de archivos se ejecuta según reglas de supervisión de operación con archivos. Puede usar los criterios de activación de la regla para configurar las condiciones que desencadenan la tarea y ajustan el nivel de importancia de eventos para operaciones con archivos detectadas y registradas en el registro de tareas.

Una regla de supervisión de operación con archivos se especifica para cada área de supervisión.

Puede configurar los siguientes criterios de activación de la regla:

- Usuarios de confianza.
- Marcadores de operaciones con archivos.

Usuarios de confianza

De forma predeterminada, la aplicación trata todas las acciones del usuario como posible violación de la seguridad. La lista del usuarios de confianza está vacía. Puede configurar el nivel de importancia del evento al crear una lista de usuarios de confianza en la operación con archivos que supervisa la configuración de la regla.

Usuario dudoso: cualquier usuario no indicado en la lista de usuarios de confianza en la configuración de la regla del área de supervisión. Si Kaspersky Embedded Systems Security 2.2 detecta una operación con archivos realizada por un usuario dudoso, la tarea Monitor de integridad de archivos registra un Evento crítico en el registro de tareas.

Usuario de confianza: un usuario o el grupo de usuarios autorizados para realizar operaciones con archivos en el área de supervisión especificada. Si Kaspersky Embedded Systems Security 2.2 detecta operaciones con archivos realizadas por un usuario de confianza, la tarea Monitor de integridad de archivos registra un Evento informativo en el registro de tareas.

Kaspersky Embedded Systems Security 2.2 no puede determinar a los usuarios que inician operaciones durante los periodos de interrupción de la supervisión. En este caso, el estado del usuario está determinado como desconocido.

Usuario desconocido: este estado se asigna a un usuario si Kaspersky Embedded Systems Security 2.2 no puede

recibir la información sobre un usuario debido a una interrupción de la tarea o una omisión del controlador de sincronización de datos o un diario de USN. Si Kaspersky Embedded Systems Security 2.2 detecta una operación con archivos realizada por un usuario desconocido, la tarea Monitor de integridad de archivos registra un evento de *Advertencia* en el registro de tareas.

Marcadores de operaciones con archivos

Cuando se ejecuta la tarea Monitor de integridad de archivos se ejecuta, Kaspersky Embedded Systems Security 2.2 usa marcadores de operaciones con archivos para decidir que una acción se ha realizado en un archivo.

Un marcador de operaciones con archivos es un descriptor único que puede caracterizar una operación con archivos.

Cada operación con archivos puede ser una sola acción o una cadena de acciones con archivos. Cada acción de esta clase se compara con un marcador de operaciones con archivos. Si el marcador que especifica como criterio de activación de la regla se detecta en una cadena de operaciones con archivos, la aplicación registra un evento que indica que la operación con archivos dada se realizó.

El nivel de importancia de los eventos registrados no depende de los marcadores de operaciones con archivos seleccionados o el número de eventos.

De forma predeterminada, Kaspersky Embedded Systems Security 2.2 considera todos los marcadores de operaciones con archivos disponibles. Puede seleccionar marcadores de operaciones con archivos manualmente en la configuración de la regla de la tarea.

Table 36. Marcadores de operaciones con archivos

ID de operación con archivos	Marcador de operaciones con archivos	Sistemas de archivos admitidos
BASIC_INFO_CHANGE	Los atributos o los marcadores del tiempo de un archivo o carpeta cambiaron.	NTFS, ReFS
COMPRESSION_CHANGE	La compresión de un archivo o carpeta cambió.	NTFS, ReFS
DATA_EXTEND	El tamaño de archivo o carpeta aumentó.	NTFS, ReFS
DATA_OVERWRITE	El dato en un archivo o carpeta se sobreescribió.	NTFS, ReFS
DATA_TRUNCATION	Archivo o carpeta truncados.	NTFS, ReFS
EA_CHANGE	Los atributos de la carpeta o el archivo ampliado cambiaron.	Solo NTFS
ENCRYPTION_CHANGE	El estado del cifrado del archivo o la carpeta cambió.	NTFS, ReFS
FILE_CREATE	Archivo o carpeta creada por primera vez	NTFS, ReFS
FILE_DELETE	El archivo o la carpeta eliminados de forma permanente con la combinación SHIFT+DEL	NTFS, ReFS
HARD_LINK_CHANGE	Vínculo físico creado o eliminado del archivo o la carpeta	Solo NTFS
INDEXABLE_CHANGE	El estado del índice de archivo o carpeta cambió.	NTFS, ReFS

ID de operación con archivos	Marcador de operaciones con archivos	Sistemas de archivos admitidos
INTEGRITY_CHANGE	El atributo de integridad cambió para un determinado flujo de archivos.	Solo ReFS
NAMED_DATA_EXTEND	El tamaño de un determinado flujo de archivos aumentó.	NTFS, ReFS
NAMED_DATA_OVERWRITE	Determinado flujo de archivos sobreescrito	NTFS, ReFS
NAMED_DATA_TRUNCATION	Determinado flujo de archivos truncado	NTFS, ReFS
OBJECT_ID_CHANGE	El identificador de archivo o carpeta cambió.	NTFS, ReFS
RENAME_NEW_NAME	Nombre nuevo asignado a archivo o carpeta	NTFS, ReFS
REPARSE_POINT_CHANGE	Nuevo punto de reanálisis creado o existente cambiado para un archivo o carpeta	NTFS, ReFS
SECURITY_CHANGE	Los derechos de acceso del archivo o la carpeta cambiaron.	NTFS, ReFS
STREAM_CHANGE	Determinado flujo de archivos nuevo creado o flujo de archivos existentes modificado	NTFS, ReFS
TRANSACTED_CHANGE	Flujo de archivos determinado modificado por transacción TxF	Solo ReFS

Configuración de la tarea Monitor de integridad de archivos

Puede cambiar las configuraciones predeterminadas de la tarea del Monitor de Integridad de archivos (ver la siguiente tabla).

Table 37. Configuración de la tarea del Monitor de integridad de archivos predeterminada

Configuración	Valor predeterminado	Descripción
Área de supervisión	No configurado	Puede especificar las carpetas y los archivos para los cuales las acciones se supervisarán. Los eventos de supervisión se generarán para las carpetas y los archivos en el área especificada.
Lista de usuarios de confianza	No configurado	Puede especificar a usuarios o grupos de usuarios cuyas acciones en los directorios especificados serán tratadas como seguras por el componente.
Supervise operaciones con archivos cuando la tarea no se ejecute	Utilizado	Puede habilitar o deshabilitar el registro de operaciones con archivos realizadas en el área de supervisión indicado durante los periodos en los que no se ejecuta la tarea.

Configuración	Valor predeterminado	Descripción
Tener en cuenta el área de supervisión excluida	No aplicado	Puede examinar el uso de exclusiones para ver carpetas donde las operaciones con archivos no se tienen que supervisar. Cuando se ejecuta la tarea Monitor de integridad de archivos, Kaspersky Embedded Systems Security 2.2 omitirá las áreas de supervisión especificadas como exclusiones.
Cálculo de la suma de control	No aplicado	Puede configurar el cálculo de la suma de control del archivo después de aplicar los cambios en el archivo.
Considerar los marcadores de operaciones con archivos	Todos los marcadores de operaciones con archivos disponibles se consideran.	Puede especificar el conjunto de marcadores de operaciones con archivos. Si una operación con archivos realizada en un área de supervisión es caracterizada por uno o varios marcadores especificados, Kaspersky Embedded Systems Security 2.2 genera un evento de auditoría.
Programación del inicio de la tarea	La primera ejecución no está programada	Puede configurar las opciones del inicio programado de la tarea.

► *Para configurar los parámetros generales del Monitor de integridad de archivos, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Inspección del sistema** en el bloque **Monitor de integridad de archivos**, haga clic en el botón **Configurar**.

   Se abre la ventana **Monitor de integridad de archivos**.
4. En la pestaña **Configuración de supervisión de operaciones de archivos** en la ventana que se abre, ajuste la configuración del área de supervisión:
   a. Seleccionar o desactivar la casilla de verificación **Registrar la información sobre las operaciones de los archivos que aparece durante el período de interrupción de monitoreo**.

      La casilla habilita o deshabilita la supervisión de las operaciones con archivos especificadas en la configuración de la tarea del Monitor de integridad de archivos cuando la tarea no se está ejecutando por ningún motivo (la eliminación de un disco duro, la tarea fue detenida por usuario, error de software).

Si la casilla se selecciona, Kaspersky Embedded Systems Security 2.2 registrará eventos en todas las áreas de supervisión cuando la tarea Monitor de integridad de archivos no esté en ejecución.

Si la casilla se desactiva, la aplicación no registrará las operaciones con archivos en las áreas de supervisión cuando la tarea no se esté ejecutando.

De forma predeterminada, la casilla está activada.

b. Agregue las áreas de supervisión (consulte la sección “Configuración de reglas de supervisión”, en la página 216) que la tarea debe supervisar.

5. En la ficha **Administración de tareas**, inicie la tarea en base a una programación (consulte la sección “Administración de programaciones de tareas”, en la página 123).
6. Haga clic en **Aceptar** para guardar los cambios.

Configuración de reglas de supervisión

De forma predeterminada, un área de supervisión no se especifica y la tarea no supervisa las operaciones con archivos en ningún directorio.

► *Para agregar un área de supervisión, siga estos pasos:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Inspección del sistema** en el bloque **Monitor de integridad de archivos**, haga clic en el botón **Configurar**.

   Se abre la ventana **Propiedades: Monitor de integridad de archivos**.
4. En la sección **Área de supervisión**, haga clic en el botón **Agregar**.

   Se abre la ventana **Área de supervisión**.
5. Agregue un área de supervisión de una de las siguientes maneras:
   - Si desea seleccionar carpetas a través del diálogo estándar de Microsoft Windows:
     a. Haga clic en el botón **Examinar**.

        Se abre la ventana estándar Buscar carpeta de Microsoft Windows.

     b. En la ventana que se abre, seleccione la carpeta para la cual desea supervisar operaciones y haga clic en el botón **Aceptar**.

- Si desea especificar un área de supervisión manualmente, agregue una ruta mediante una máscara admitida:
  - <*.ext>: todos los archivos con la extensión <ext>, sin tener en cuenta su ubicación;
  - <*\name.ext>: todos los archivos con nombre <nombre> y extensión <ext>, sin tener en cuenta su ubicación;
  - <\Dir*>: todos los archivos en el directorio <\dir>;
  - <\dir*\name.ext>: todos los archivos con el nombre <nombre> y la extensión <ext> en el directorio <\dir> y todos sus subdirectorios.

Al especificar un área de supervisión manualmente, asegúrese de que la ruta esté en el formato siguiente: <letra del volumen>: \<máscara>. Si la letra del volumen falta, Kaspersky Embedded Systems Security 2.2 no agregará el área de supervisión especificada.

6. En la pestaña **Usuarios de confianza**, haga clic en el botón **Agregar**.

   Se abre la ventana estándar **Seleccionar usuarios o grupos** de Microsoft Windows.

7. Seleccione los usuarios o los grupos de usuarios para los que están autorizadas las operaciones con archivos en el área de supervisión seleccionada y haga clic en el botón **Aceptar**.

   De forma predeterminada, Kaspersky Embedded Systems Security 2.2 trata a todos los usuarios que no figuran en la lista de usuarios de confianza como dudosos (consulte la sección “Acerca de las reglas de supervisión de las operaciones con archivos”, en la página 212), y genera eventos críticos para ellos.

8. Seleccione la pestaña **Marcadores de operación de los archivos**.
9. Si es necesario, realice las siguientes acciones para seleccionar varios marcadores:
   a. Seleccione la opción **Detectar las operaciones de archivos sobre la base de los siguientes marcadores**.
   b. En la lista de operaciones con archivos disponibles (consulte la sección “Acerca de las reglas de supervisión de operaciones con archivos”, en la página 212), seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.

   De manera predeterminada, Kaspersky Embedded Systems Security 2.2 detecta todos los marcadores de operaciones con archivos, ya que está seleccionada la opción **Detectar las operaciones de archivos sobre la base de todos los marcadores reconocibles**.

10. Si desea que Kaspersky Embedded Systems Security 2.2 calcule la suma de control de los archivos después de se realiza la operación, haga lo siguiente:
    a. En la sección **Cálculo de la suma de control**, seleccione la casilla de verificación **Calcular suma de control para la versión final de un archivo luego de que se haya modificado el archivo, si es posible**.

       Si se selecciona la casilla, Kaspersky Embedded Systems Security 2.2 calcula la suma de control del archivo modificado donde se detectó la operación con archivos con al menos un marcador.

       Si la operación con archivos es detectada por varios marcadores, solo se calcula la suma de control del archivo final después de que todas las modificaciones.

Si se desactiva la casilla de verificación, Kaspersky Embedded Systems Security 2.2 no calcula la suma de control para los archivos modificados.

Ningún cálculo de la suma de control se realiza en los casos siguientes:

- Si el archivo se volviera no disponible (por ejemplo, debido al cambio de permisos de acceso).
- Si la operación con archivos se detecta en el archivo que se ha eliminado después.

De forma predeterminada, la casilla está desactivada.

b. En la lista desplegable **Calcular la suma de control que usa el algoritmo**, seleccione una de las opciones:

- **Hash MD5**
- **Hash SHA256**

11. Si no desea supervisar todas las operaciones con archivos en la lista de operaciones con archivos disponibles (consulte la sección “Acerca de las reglas de supervisión de operación de archivos”, en la página 212) y seleccione las casillas de verificación ubicadas junto a las operaciones que desea supervisar.
12. Si es necesario, agregue áreas de supervisión excluidas al realizar los pasos siguientes:
    a. Seleccione la pestaña **Exclusiones**.
    b. Seleccione la casilla de verificación **Tener en cuenta el área de supervisión excluida**.

    La casilla deshabilita el uso de exclusiones para carpetas donde las operaciones con archivos no se tienen que supervisar.

    Si la casilla se selecciona, Kaspersky Embedded Systems Security 2.2 omite los alcances de monitoreo especificados en la lista de exclusiones cuando se ejecuta la tarea Monitor de integridad de archivos.

    Si la casilla de verificación está desactivada, Kaspersky Embedded Systems Security 2.2 registra los eventos de todos los alcances del monitoreo especificados.

    De forma predeterminada, la casilla se desactiva y la lista de exclusión aparece vacía.

    c. Haga clic en el botón **Agregar**.

    La ventana **Seleccionar carpeta para agregar** se abre.

    d. En la ventana que se abre, especifique el objeto que desea excluir del área de supervisión.

    e. Haga clic en **Aceptar**.

    La carpeta especificada se añade a la lista de áreas excluidas.
13. Haga clic en **Aceptar** en la ventana **Área de supervisión**.

La configuración de la regla especificada se aplicará al área de supervisión seleccionada de la tarea del Monitor de integridad de archivos.

Inspección de registros

Esta sección contiene la información sobre la tarea Inspección de registros y los parámetros de la tarea.

En esta sección

Acerca de la tarea Inspección de registros

Cuando se ejecuta la tarea Inspección de registros, Kaspersky Embedded Systems Security 2.2 supervisa la integridad del entorno protegido según los resultados de una inspección de registros de Eventos de Windows. La aplicación notifica al administrador cuando detecta comportamiento anormal en el sistema, que puede ser una indicación de intentos de ataques cibernéticos.

Kaspersky Embedded Systems Security 2.2 considera que el evento de Windows registra e identifica incumplimientos según las reglas especificadas por un usuario o por la configuración del Analizador heurístico, que la tarea utiliza para inspeccionar registros.

Reglas predefinidas y análisis heurístico

Puede usar la tarea Inspección de registros para supervisar el estado del sistema protegido aplicando reglas predefinidas que se basan en la heurística existente. El Analizador heurístico identifica la actividad anormal en el equipo protegido, que pueden ser pruebas de intentos de ataque. Las plantillas para identificar el comportamiento anormal se incluyen en las reglas disponibles, en la configuración de reglas predefinidas.

Se incluyen siete reglas en la lista de reglas para la tarea Inspección de registros. Puede habilitar o deshabilitar el uso de cualquiera de estas reglas. No puede eliminar las reglas existentes ni crear reglas nuevas.

Puede configurar los criterios de activación para las reglas que supervisan eventos para las siguientes operaciones:

- Detección de la fuerza bruta de la contraseña
- Detección del inicio de sesión de la red

También puede configurar exclusiones en la configuración de la tarea. El Analizador heurístico no se activa cuando un inicio de sesión es realizado por un usuario de confianza o desde una dirección IP de confianza.

> Kaspersky Embedded Systems Security 2.2 no usa los parámetros heurísticos para inspeccionar registros de Windows si la tarea no utiliza el Analizador heurístico. De forma predeterminada, el Analizador heurístico está habilitado.

Cuando se aplican las reglas, la aplicación registra un *Evento crítico* en el registro de tareas de Inspección de registros.

Reglas personalizadas para la tarea de Inspección de registros

Puede usar la configuración de la regla de la tarea para especificar y cambiar los criterios para desencadenar reglas al detectar los eventos seleccionados en el registro de Windows especificado. De manera predeterminada, la lista

de reglas de la tarea de Inspección de registros contiene cuatro reglas. Puede habilitar y deshabilitar el uso estas reglas, eliminar reglas y modificar la configuración de la regla.

Puede configurar los siguientes criterios de activación de la regla en cada regla:

- Lista de identificadores de registro en Registro de Eventos de Windows.

  La regla se desencadena cuando un registro nuevo se crea en el Registro de Eventos de Windows, si las propiedades del evento incluyen un identificador del evento especificado para la regla. También puede agregar y eliminar identificadores para cada regla especificada.

- Fuente del evento.

  Para cada regla, puede definir un subregistro del Registro de Eventos de Windows. La aplicación buscará registros con los identificadores del evento especificados solo en este subregistro. Puede seleccionar uno de los subregistros estándar (Aplicación, Seguridad o Sistema) o especificar un subregistro personalizado ingresando el nombre en el campo Selección de origen.

  La aplicación no verifica que el subregistro especificado realmente exista en el Registro de Eventos de Windows.

Cuando se activa la regla, Kaspersky Embedded Systems Security 2.2 registra un evento crítico en el registro de tareas de Inspección de registros.

De manera predeterminada, la tarea Inspección de registros no aplica reglas personalizadas.

Antes de iniciar la tarea Inspección de registros, asegúrese d que la directiva de auditoría del sistema esté configurada correctamente. Consulte el artículo de Microsoft https://technet.microsoft.com/en-us/library/cc952128.aspx para obtener detalles.

Configuración de reglas de tareas predefinidas

► *Realice las siguientes acciones para configurar las reglas predefinidas para la tarea Inspección de registros:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

     Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Inspección del sistema**, haga clic en el botón **Configurar** en el bloque **Inspección de registros**.

Se abre la ventana **Configuración de inspección de registros**.

4. Seleccione la pestaña **Reglas predefinidas**.
5. Seleccione o desactive la casilla de verificación **Aplicar reglas predefinidas para la inspección de registros**.

   Si esta casilla se selecciona, Kaspersky Embedded Systems Security 2.2 aplica el analizador heurístico para detectar actividad anormal en el equipo protegido.

   Si esta casilla se desactiva, el analizador heurístico no se ejecuta y Kaspersky Embedded Systems Security 2.2 aplica reglas predeterminadas o personalizadas para detectar la actividad anormal.

   De forma predeterminada, la casilla está activada.

   Para que la tarea se ejecute, debe seleccionarse al menos una regla de inspección de registros.

6. Seleccione las reglas que desea aplicar en la lista de reglas predefinidas:
   - Hay patrones de un posible ataque de fuerza bruta en el sistema.
   - Hay patrones de un posible abuso del registro de eventos de Windows.
   - Se detectaron acciones atípicas por parte de un servicio nuevo instalado.
   - Se detectó un inicio de sesión atípico que utiliza credenciales explícitas.
   - Hay patrones de un posible ataque PAC (MS14-068) falsificado de Kerberos en el sistema.
   - Se detectaron acciones atípicas dirigidas a administradores de un grupo integrado con privilegiados.
   - Hay una actividad atípica detectada durante un inicio de sesión en la red.
7. Para configurar las reglas seleccionadas, haga clic en el botón **Configuración avanzada**.

   Se abrirá la ventana **Inspección de registros**.
8. En la sección **Detección de ataques de fuerza bruta**, configure el número de intentos y el periodo en el que se produjeron estos intentos, que se considerarán como desencadenadores para el analizador heurístico.
9. En la sección **Detección de inicio de sesión en la red**, indique el inicio y el final del intervalo de tiempo durante el cual los intentos de inicio de sesión en Kaspersky Embedded Systems Security 2.2 se consideraron como amenazas y como actividad anormal.
10. Seleccione la pestaña **Exclusiones**.
11. Realice las siguientes acciones para agregar a usuarios de confianza:
    a. Haga clic en el botón **Examinar**.
    b. Seleccione a un usuario.
    c. Haga clic en **Aceptar**.

       Un usuario seleccionado se añade a la lista de usuarios de confianza.
12. Realice las siguientes acciones para agregar Direcciones IP de confianza:
    a. Escriba la Dirección IP.
    b. Haga clic en el botón **Agregar**.
13. Una Dirección IP indicada se añade a la lista de Direcciones IP de confianza.

14. En la pestaña **Administración de tareas**, configure la programación de inicio de tareas (consulte la sección “Configuración de las opciones de programación de inicio de tareas”, en la página 123).
15. Haga clic en **Aceptar**.

La configuración de la tarea Inspección de registros se guardó.

Configuración de las reglas de inspección de registros

► *Realice las siguientes acciones para agregar y configurar una nueva regla personalizada de Inspección de registros:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. En el panel de detalles del grupo de administración seleccionado, realice una de las siguientes acciones:
   - Para establecer la configuración de la aplicación para un grupo de equipos, seleccione la pestaña **Directivas** y abra la ventana **Propiedades: <Nombre de la directiva>** (consulte la sección “Configuración de directivas”, en la página 91).
   - Para configurar la aplicación para un solo equipo, seleccione la pestaña **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).

   > Si un dispositivo es administrado por una directiva activa de Kaspersky Security Center, y esta directiva no permite cambiar la configuración de la aplicación, esta configuración no se puede modificar a través de la ventana **Configuración de la aplicación**.
3. En la sección **Inspección del sistema**, haga clic en el botón **Configurar** en el bloque **Inspección de registros**.

   Se abrirá la ventana **Inspección de registros**.
4. En la pestaña **Reglas de inspección de registros**, seleccione o desmarque la casilla de verificación **Aplicar reglas personalizadas para la inspección de registros**.

   Si la casilla está seleccionada, Kaspersky Embedded Systems Security 2.2 aplica reglas personalizadas para la inspección de registros según cada configuración de reglas. Puede agregar, eliminar o configurar reglas de Inspección de registros.

   Si la casilla está desactivada, no puede agregar ni modificar las reglas personalizadas. Kaspersky Embedded Systems Security 2.2 aplica la configuración de reglas predeterminada.

   De forma predeterminada, la casilla está activada. Solo la regla Detección de aplicaciones emergentes está activa.

   > Puede controlar si las reglas predeterminadas se aplican para la Inspección de registros. Seleccione las casillas correspondientes a las reglas desea aplicar a la Inspección de registros.
5. Para agregar una nueva regla personalizada, haga clic en el botón **Agregar**.

   Se abre la ventana **Reglas de inspección de registros**.

6. En la sección **General**, ingrese la siguiente información sobre la regla nueva:
   - **Nombre**
   - **Origen**

     Seleccione un registro de fuentes para usar los eventos registrados para el análisis. Los siguientes tipos de registros de eventos de Windows están disponibles:

     - Aplicación
     - Seguridad
     - Sistema

     Puede agregar un nuevo registro personalizado ingresando el nombre del registro en el campo **Origen**.
7. En la sección **Id. de eventos activados**, especifique los Id. de los elementos que activarán la regla tras la detección:
   a. Escriba el valor numérico de un ID.
   b. Haga clic en el botón **Agregar**.

      El ID de la regla seleccionado se añade a la lista. Puede agregar un número ilimitado de identificadores para cada regla.
   c. Haga clic en **Aceptar**.

   La regla de inspección de registros se añade a la lista de reglas.

Informes en Kaspersky Security Center

Los informes en Kaspersky Security Center contienen información sobre el estado de dispositivos administrados. Los informes se basan en información almacenada en el Servidor de administración.

A partir de Kaspersky Security Center 11, los siguientes tipos de informes están disponibles para Kaspersky Embedded Systems Security 2.2:

- Informe sobre el estado de componentes de la aplicación
- Informe sobre aplicaciones prohibidas
- Informe sobre aplicaciones prohibidas en modo de prueba

Consulte la *Ayuda de Kaspersky Security Center* para obtener información detallada sobre todos los informes de Kaspersky Security Center y cómo configurarlos.

Informe sobre el estado de componentes de la aplicación

Puede supervisar el estado de protección de todos los dispositivos de red y acceder a un panorama estructurado del conjunto de componentes en cada dispositivo.

El informe muestra uno de los siguientes estados para cada componente: *En ejecución, En pausa, Detenido, Mal funcionamiento, No instalado, Iniciando*.

El estado *No instalado* hace referencia al componente, no a la aplicación. Si la aplicación no se instala, Kaspersky Security Center asigna el estado N/D (No disponible).

Puede crear selecciones de componentes y utilizar filtros para mostrar dispositivos de red con el conjunto definido de componentes y su estado.

Consulte la *Ayuda de Kaspersky Security Center* para acceder a información detallada sobre la creación y el uso de selecciones.

► *Para revisar los estados de componentes en la configuración de la aplicación:*

1. Expanda el nodo **Dispositivos administrados** en el árbol de la Consola de administración de Kaspersky Security Center y seleccione el grupo de administración para el cual desea configurar la aplicación.
2. Seleccione la ficha **Dispositivos** y abra la ventana **Configuración de la aplicación** (consulte la sección “Configuración de tareas locales en la ventana Configuración de la aplicación de Kaspersky Security Center”, en la página 103).
3. Seleccione la sección **Componentes**.
4. Revise la tabla de estado.

► *Para revisar un informe estándar de Kaspersky Security Center:*

1. Seleccione el nodo **Servidor de administración <nombre del equipo>** en el árbol de la Consola de administración.
2. Abra la pestaña **Informes**.
3. Haga doble clic en el elemento de la lista **Informe sobre el estado de los componentes de la aplicación**.

   Se genera un informe.
4. Revise los siguientes detalles del informe:
   - Un diagrama gráfico.
   - Una tabla con un resumen de los componentes y los números sumados de los dispositivos de red donde se instala cada uno de los componentes, y los grupos a los que pertenecen.
   - Una tabla detallada donde se especifica estado, versión, dispositivo y grupo del componente.

Informes sobre aplicaciones bloqueadas en los modos Activo y Solo estadísticas

En base a los resultados de la ejecución de la tarea Control de inicio de aplicaciones (consulte la sección “Administración de inicio de aplicaciones desde Kaspersky Security Center”, en la página 177), pueden generarse dos tipos de informes: un informe sobre las aplicaciones prohibidas (si la tarea se inicia en el modo **Activo**) y un informe de las aplicaciones prohibidas en modo de prueba (si la tarea se inició en el modo **Solo estadísticas**). Estos informes muestran información sobre las aplicaciones bloqueadas en los servidores protegidos de la red. Cada informe se genera para todos los grupos de administración y acumula datos de todas las aplicaciones de Kaspersky Lab instaladas en los dispositivos protegidos.

► *Para revisar un informe sobre aplicaciones prohibidas en modo de prueba:*

1. Inicie la tarea Control de aplicaciones en el modo Solo estadísticas (consulte la sección “Configuración de la tarea Control de inicio de aplicaciones”, en la página 178).
2. Seleccione el nodo **Servidor de administración <nombre del equipo>** en el árbol de la Consola de administración.
3. Abra la pestaña **Informes**.
4. Haga doble clic en el elemento de la lista **Informe sobre aplicaciones prohibidas en modo de prueba**.

   Se genera un informe.
5. Revise los siguientes detalles del informe:
   - Un diagrama gráfico que muestra las diez primeras aplicaciones con la mayor cantidad de inicios bloqueados.
   - Una tabla que resume los bloques de aplicaciones ocurridos, donde se especifican el nombre del archivo ejecutable, el motivo, el tiempo de bloqueo y el número de dispositivos donde ocurrió.
   - Una tabla detallada donde se especifican datos sobre el dispositivo, la ruta de acceso del archivo y el criterio para el bloqueo.

► *Para revisar un informe sobre aplicaciones prohibidas en modo Activo:*

1. Inicie la tarea Control de aplicaciones en el modo Activo (consulte la sección “Configuración de la tarea Control de inicio de aplicaciones”, en la página 178).
2. Seleccione el nodo **Servidor de administración <nombre del equipo>** en el árbol de la Consola de

administración.

3. Abra la pestaña **Informes**
4. Haga doble clic en el elemento de la lista **Informe sobre aplicaciones prohibidas**.

   Se genera un informe.

Este informe consiste en los mismos bloques de datos que el informe sobre aplicaciones prohibidas en el modo de prueba.

Cómo utilizar Kaspersky Embedded Systems Security 2.2 desde la línea de comandos

Esta sección describe cómo utilizar Kaspersky Embedded Systems Security 2.2 desde la línea de comandos.

En este capítulo

Comandos de la línea de comandos

Puede ejecutar comandos básicos de administración de Kaspersky Embedded Systems Security 2.2 desde la línea de comandos del equipo protegido, si incluye el componente Utilidad de línea de comandos en la lista de funciones instaladas durante la instalación de Kaspersky Embedded Systems Security 2.2.

Si utiliza comandos de la línea de comandos, puede administrar solo aquellas funciones a las que tiene acceso según los permisos que se le asignaron en Kaspersky Embedded Systems Security 2.2.

Ciertos comandos de Kaspersky Embedded Systems Security 2.2 se ejecutan en los siguientes modos:

- Modo síncrono: la administración regresa a la Consola solo después de que la ejecución del comando se ha completado.
- Modo asíncrono: la administración regresa a la Consola inmediatamente después de que el comando se ejecuta.

► *Para interrumpir la ejecución del comando en modo síncrono*

presione el acceso directo del teclado **Ctrl+C**.

Siga las siguientes reglas al introducir comandos de Kaspersky Embedded Systems Security 2.2:

- Introduzca modificadores y comandos utilizando mayúsculas y minúsculas.
- Delimite los modificadores con el carácter de espacio.
- Si el nombre del archivo o de la carpeta cuya ruta se especifica como valor de clave contiene un espacio, especifique la ruta del archivo o de la carpeta entre comillas, por ejemplo: `"C:\TEST\test cpp.exe"`
- Si es necesario, use marcadores de posición en las máscaras de ruta de acceso o el nombre de archivo, por ejemplo: “`C:\Temp\Temp*\`”, “`C:\Temp\Temp???.doc`”, “`C:\Temp\Temp*.doc`”

Se puede usar la línea de comandos para todo el rango de operaciones requeridas para la administración de Kaspersky Embedded Systems Security 2.2 (consulte la tabla a continuación).

Table 38. Comandos de Kaspersky Embedded Systems Security 2.2

Comando	Descripción
KAVSHELL APPCONTROL (consulte la sección “Cómo completar la lista de reglas de Control de inicio de aplicaciones KAVSHELL APPCONTROL”, en la página 240)	Renueva la lista de reglas especificadas según el principio de adición seleccionado.
KAVSHELL APPCONTROL /CONFIG (consulte la sección “Administración de la tarea Control de inicio de aplicaciones KAVSHELL APPCONTROL /CONFIG”, en la página 237)	Controla el modo de operación de la tarea Control de inicio de aplicaciones
KAVSHELL APPCONTROL /GENERATE (consulte la sección “Generador de reglas de control de inicio de aplicaciones KAVSHELL APPCONTROL /GENERATE”, en la página 237)	Inicia la tarea de Generador de reglas de control de inicio de aplicaciones.
KAVSHELL VACUUM (consulte la sección “Desfragmentación de archivos de registro de Kaspersky Embedded Systems Security 2.2. KAVSHELL VACUUM”, en la página 248)	Desfragmenta los archivos de registro de Kaspersky Embedded Systems Security 2.2.
KAVSHELL PASSWORD	Administra la configuración de protección con contraseña.
KAVSHELL HELP (consulte la sección “Visualización de la ayuda de comandos de Kaspersky Embedded Systems Security 2.2. KAVSHELL HELP”, en la página 229)	Muestra la ayuda de comandos de Kaspersky Embedded Systems Security 2.2.
KAVSHELL START (consulte la sección “Inicio y detención del servicio de Kaspersky Security KAVSHELL START, KAVSHELL STOP”, en la página 230)	Inicia el servicio de Kaspersky Embedded Systems Security 2.2.
KAVSHELL STOP (consulte la sección “Inicio y detención del servicio de Kaspersky Security KAVSHELL START, KAVSHELL STOP”, en la página 230)	Detiene el servicio de Kaspersky Embedded Systems Security 2.2.
KAVSHELL SCAN (consulte la sección “Análisis del área seleccionada. KAVSHELL SCAN”, en la página 230)	Crea e inicia una tarea de Análisis a pedido temporal con la configuración de seguridad y de área del análisis determinada por los modificadores de comando.
KAVSHELL SCANCRITICAL (consulte la sección “Inicio de la tarea Análisis de áreas críticas. KAVSHELL SCANCRITICAL”, en la página 234)	Inicia la tarea del sistema Análisis de áreas críticas.
KAVSHELL TASK (consulte la sección “Administración de tarea especificada de manera asíncrona. KAVSHELL TASK”, en la página 235)	Inicia/pausa/reanuda/detiene la tarea seleccionada de manera asíncrona/muestra el estado de tarea actual/muestra estadísticas.
KAVSHELL RTP (consulte la sección “Inicio y detención de tareas de protección en tiempo real. KAVSHELL RTP”, en la página 236)	Inicia o detiene todas las tareas de protección en tiempo real.
KAVSHELL UPDATE (consulte la sección “Inicio de la tarea de actualización de bases de datos de Kaspersky Embedded Systems Security 2.2. KAVSHELL UPDATE”, en la página 241)	Inicia la tarea de actualización de las bases de datos de Kaspersky Embedded Systems Security 2.2 con la configuración especificada mediante modificadores de comando.

Comando	Descripción
KAVSHELL ROLLBACK (consulte la sección “Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK”, en la página 244)	Revierte las bases de datos a la versión anterior.
KAVSHELL LICENSE (consulte la sección “Activación de la aplicación KAVSHELL LICENSE”, en la página 245)	Administra claves.
KAVSHELL TRACE (consulte la sección “Habilitación, configuración y deshabilitación del registro de rastreo. KAVSHELL TRACE”, en la página 247)	Habilita o deshabilita el registro de rastreo, administra la configuración del registro de rastreo.
KAVSHELL DUMP (consulte la sección “Habilitación y deshabilitación de la creación de archivos de volcado. KAVSHELL DUMP”, en la página 249)	Habilita o deshabilita los archivos de volcado de memoria de Kaspersky Embedded Systems Security 2.2 en caso de interrupción anormal de los procesos.
KAVSHELL IMPORT (consulte la sección “Importación de la configuración. KAVSHELL IMPORT”, en la página 251)	Importa valores de configuración, funciones y tareas generales de Kaspersky Embedded Systems Security 2.2 de un archivo de configuración creado con antelación.
KAVSHELL EXPORT (consulte la sección “Exportación de configuración. KAVSHELL EXPORT”, en la página 251)	Exporta todos los valores de configuración de Kaspersky Embedded Systems Security 2.2 y tareas existentes a un archivo de configuración.
KAVSHELL DEVCONTROL (consulte la sección “Cómo completar la lista de reglas de Control de dispositivos. KAVSHELL DEVCONTROL”, en la página 241)	Agrega a la lista de reglas de control de dispositivos generadas según el método seleccionado.

Visualización de la ayuda de comandos de Kaspersky Embedded Systems Security 2.2. KAVSHELL HELP

Para obtener la lista de todos los comandos de Kaspersky Embedded Systems Security 2.2, ejecute uno de los comandos siguientes:

```
/KAVSHELL

KAVSHELL HELP

KAVSHELL /?
```

Para obtener una descripción de un comando y su sintaxis, ejecute uno de los siguientes comandos:

```
KAVSHELL HELP <comando>

KAVSHELL <comando> /?
```

Ejemplos de comandos de KAVSHELL HELP

Para ver información detallada sobre el comando KAVSHELL SCAN, ejecute el siguiente comando:

```
KAVSHELL HELP SCAN
```

Inicio y detención del servicio de Kaspersky Security KAVSHELL START, KAVSHELL STOP

Para ejecutar el servicio de Kaspersky Security, ejecute el comando

```
KAVSHELL START
```

De manera predeterminada, cuando se inicia el servicio de Kaspersky Security, se inician las tareas Protección de archivos en tiempo real y Análisis cuando arranca el sistema, así como las demás tareas cuyo inicio esté programado **Al inicio de la aplicación**.

Para detener el servicio de Kaspersky Security, ejecute el comando

```
KAVSHELL STOP
```

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Análisis del área seleccionada. KAVSHELL SCAN

Para iniciar una tarea de análisis de áreas específicas del equipo protegido, utilice el comando `KAVSHELL SCAN`. Los modificadores del comando especifican el área del análisis y la configuración de seguridad del nodo seleccionado.

La tarea Análisis a pedido iniciada con el comando `KAVSHELL SCAN` es una tarea temporal. Se muestra en Consola de la aplicación solo al ejecutarse (no se puede ver la configuración de la tarea en la Consola de la aplicación). Al mismo tiempo, se genera el registro de rendimiento de tareas. Se muestra en los **Registros de tareas** de la Consola de la aplicación.

Al especificar las rutas de acceso en las tareas de análisis de áreas específicas, se pueden utilizar las variables del entorno. Si se utilizan las variables del entorno especificadas para el usuario, ejecute el comando `KAVSHELL SCAN` con los permisos para ese usuario.

El comando `KAVSHELL SCAN` se ejecuta en el modo síncrono.

Para iniciar una tarea Análisis a pedido desde la línea de comandos, use el comando KAVSHELL TASK (consulte la sección “Administración de la tarea especificada de manera asíncrona. KAVSHELL TASK”, en la página 235).

Sintaxis del comando KAVSHELL SCAN

```
KAVSHELL SCAN <área del análisis>
[/MEMORY|/SHARED|/STARTUP|/REMDRIVES|/FIXDRIVES|/MYCOMP] [/L:< ruta de acceso al
archivo con la lista de áreas del análisis >] [/F<A|C|E>] [/NEWONLY]
[/AI:<DISINFECT|DISINFDEL|DELETE|REPORT|AUTO>]
[/AS:<QUARANTINE|DELETE|REPORT|AUTO>] [/DISINFECT|/DELETE] [/E:<ABMSPO>]
[/EM:<”masks”>] [/ES:<tamaño>] [/ET:<cantidad de segundos>] [/TZOFF]
[/OF:<SKIP|RESIDENT|SCAN[=<días>] [NORECALL]>]
[/NOICHECKER][/NOISWIFT][/ANALYZERLEVEL][/NOCHECKMSSIGN][/W:<ruta de acceso al
```

```
archivo de registro de tareas>] [/ANSI] [/ALIAS:<alias de la tarea>]
```

El comando KAVSHELL SCAN tiene claves obligatorias y opcionales (consulte la tabla a continuación).

Ejemplos del comando KAVSHELL SCAN

```
KAVSHELL SCAN Folder56 D:\Folder1\Folder2\Folder3\ C:\Folder1\ C:\Folder2\3.exe
"\\another server\Shared\" F:\123\*.fgb /SHARED /AI:DISINFDEL /AS:QUARANTINE /FA
/E:ABM /EM:"*.xtx;*.fff;*.ggg;*.bbb;*.info" /NOICHECKER /ANALYZERLEVEL:1
/NOISWIFT /W:log.log
```

```
KAVSHELL SCAN /L:scan_objects.lst /W:c:\log.log
```

Table 39. Modificadores del comando KAVSHELL SCAN

Clave	Descripción
Área del análisis. Modificador obligatorio.	
<archivos> <carpetas> <ruta de red>	Especifica el área del análisis: lista de archivos, carpetas, rutas de red y áreas predefinidas. Especifique rutas de red en el formato UNC (convención de nomenclatura universal). En el siguiente ejemplo, la carpeta Folder4 se especifica sin una ruta de acceso y está ubicada en la carpeta desde la cual se ejecuta el comando KAVSHELL: KAVSHELL SCAN Folder4 Si el nombre del objeto a comprobar tiene espacios, se debe colocar entre signos de interrogación. Cuando se selecciona una carpeta, Kaspersky Embedded Systems Security 2.2 también comprueba todas las subcarpetas de esa carpeta. Los símbolos * o ? se pueden utilizar para analizar un grupo de archivos.
/MEMORY	Analizar objetos en RAM
/SHARED	Analizar carpetas compartidas en el equipo
/STARTUP	Analizar objetos de inicio
/REMDRIVES	Analizar unidades extraíbles
/FIXDRIVES	Analizar unidades de disco duro
/MYCOMP	Analizar todas las áreas del equipo protegido
/L:<ruta del archivo con la lista de áreas del análisis>	Nombre de archivo con la lista de áreas de análisis incluida la ruta completa para el archivo. Delimite áreas de análisis en los archivos utilizando saltos de línea. Puede especificar áreas de análisis predefinidas como se muestra a continuación en este ejemplo de un archivo con una lista de áreas del análisis: C:\ D:\Docs*.doc E:\Mis documentos /STARTUP /SHARED
Objetos analizados (tipos de archivos). Si no especifica valores para este modificador, Kaspersky Embedded Systems Security 2.2 analizará los objetos por formato.	

Clave	Descripción
/FA	Analizar todos los objetos
/FC	Analizar los objetos por formato (de manera predeterminada). Kaspersky Embedded Systems Security 2.2 analiza solo objetos cuyos formatos figuran en la lista de formatos de objetos infectables.
/FE	Analizar los objetos por extensión Kaspersky Embedded Systems Security 2.2 analiza solo objetos con extensiones que figuran en la lista de extensiones de objetos infectables.
/NEWONLY	Analizar solo los archivos nuevos y modificados. Si no indica este modificador, Kaspersky Embedded Systems Security 2.2 analizará todos los objetos.
Acción que se realizará con los objetos infectados y otros objetos. Si no se especificaron valores para este modificador, Kaspersky Embedded Systems Security 2.2 ejecutará la acción **Omitir**.	
DISINFECT	Desinfectar, omitir si la desinfección es imposible
DISINFDEL	Desinfectar, eliminar si la desinfección es imposible
DELETE	Eliminar Los valores de configuración DISINFECT y DELETE se guardan en la versión actual de Kaspersky Embedded Systems Security 2.2 a fin de asegurar compatibilidad con versiones anteriores. Esos valores se pueden utilizar en lugar de los comandos de modificador /AI: y /AS: En ese caso, Kaspersky Embedded Systems Security 2.2 no procesará objetos probablemente infectados.
REPORT	Enviar un informe (de manera predeterminada)
AUTO	Ejecutar la acción recomendada
/AS: **Acción que se realizará con los objetos probablemente infectados**/ Si no se especificaron valores para este modificador, Kaspersky Embedded Systems Security 2.2 ejecutará la acción **Omitir**.	
CUARENTENA	Cuarentena
DELETE	Eliminar
REPORT	Enviar un informe (de manera predeterminada)
AUTO	Ejecutar la acción recomendada
Exclusiones	
/E:ABMSPO	Excluye objetos compuestos de los siguientes tipos: A: archivos (se analizan solo los archivos SFX) B: bases de datos de correo electrónico M: correo electrónico sin formato S: archivos y archivos SFX P: objetos empaquetados O: objetos OLE integrados
/EM:<″masks″>	Excluir archivos por máscara Se pueden especificar varias máscaras, por ejemplo: EM:″*.txt; *.png; C\Videos*.avi″.

Clave	Descripción
/ET:<cantidad de segundos>	Detener el procesamiento de un objeto si demora más tiempo que la cantidad de segundos especificada en el valor <cantidad de segundos>. No hay restricciones de tiempo de manera predeterminada.
/ES:<tamaño>	No analizar objetos compuestos que superan el tamaño (en MB) especificado por el valor <tamaño>. Kaspersky Embedded Systems Security 2.2 analiza objetos de todo tamaño de manera predeterminada.
/TZOFF	Deshabilitar exclusiones de zonas de confianza
Configuración avanzada (Opciones)	
/NOICHECKER	Deshabilitar la utilización de iChecker (habilitada de forma predeterminada).
/NOISWIFT	Deshabilitar la utilización de iSwift (habilitada de forma predeterminada).
/ANALYZERLEVEL: <intensidad del análisis>	Habilitar el Analizador heurístico, configurar el nivel de análisis. Los siguientes niveles de análisis heurístico están disponibles: 1: ligero 2: medio 3: profundo Si se omite el modificador, Kaspersky Embedded Systems Security 2.2 no utilizará el analizador heurístico.
/ALIAS:<alias de la tarea>	Permite asignar un nombre temporal a una tarea de Análisis a pedido por el cual se puede acceder a la tarea durante su ejecución; por ejemplo, para ver sus estadísticas con el comando TASK. El alias de tarea debe ser único entre los alias de tarea de todos los componentes funcionales de Kaspersky Embedded Systems Security 2.2. Si no se especificó este modificador, se utiliza el nombre temporal scan_<pid_de_kavshell>, por ejemplo scan_1234. En la Consola de la aplicación, se asigna a la tarea el nombre Analizar objetos (<fecha y hora>), por ejemplo, Analizar objetos 16/08/2007 5:13:14 p. m.
Configuración de registros de tareas (configuración de informes)	

Clave	Descripción
/W:<ruta del archivo de registro de tareas>	Si se especifica esta clave, Kaspersky Embedded Systems Security 2.2 guardará el archivo de registro de tareas con el nombre definido por el valor de la clave. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos producidos en ella. El registro se utiliza para registrar eventos definidos por la configuración de los registros de tareas y el registro de eventos de Kaspersky Embedded Systems Security 2.2 en el "Visor de eventos". Se puede especificar la ruta relativa o absoluta del archivo de registro. Si se especifica solo el nombre de un archivo sin especificar la ruta correspondiente, el archivo de registro se creará en la carpeta actual. Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo Registros de tareas de la Consola de la aplicación. Si se produce un error en Kaspersky Embedded Systems Security 2.2 al crear el archivo de registro, esto no evitará que el comando se ejecute, pero se mostrará un mensaje de error.
/ANSI	La opción permite la grabación de los eventos en el registro de tareas en la codificación ANSI. La opción ANSI no se aplicará si la opción W no está definida. Si no se especificó la opción ANSI, el registro de tareas se genera con la codificación UNICODE.

Iniciar la tarea Análisis de áreas críticas. KAVSHELL SCANCRITICAL

Use el comando `KAVSHELL SCANCRITICAL` para iniciar el Análisis de áreas críticas de la tarea de Análisis a pedido del sistema con la configuración definida en la Consola de la aplicación.

Sintaxis del comando KAVSHELL SCANCRITICAL

```
KAVSHELL SCANCRITICAL [/W:<ruta del archivo del registro de tareas>]
```

Ejemplos del comando KAVSHELL SCANCRITICAL

Para ejecutar la tarea Análisis a pedido de Análisis de áreas críticas y guardar el registro de tareas scancritical.log en la carpeta actual, ejecute el siguiente comando:

```
KAVSHELL SCANCRITICAL /W:scancritical.log
```

Según la sintaxis del modificador /W, se puede configurar la ubicación del registro de tareas (consulte la tabla a continuación).

Table 40. Sintaxis del modificador /W para el comando KAVSHELL SCANCRITICAL

Clave	Descripción
/W:<ruta del archivo de registro de tareas>	Si se especifica esta clave, Kaspersky Embedded Systems Security 2.2 guardará el archivo de registro de tareas con el nombre definido por el valor de la clave. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos producidos en ella. El registro se utiliza para registrar eventos definidos por la configuración de los registros de tareas y el registro de eventos de la aplicación en el Visor de eventos. Se puede especificar la ruta relativa o absoluta del archivo de registro. Si se especifica solo el nombre de un archivo sin especificar la ruta correspondiente, el archivo de registro se creará en la carpeta actual. Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo **Registros de tareas** de la Consola de la aplicación. Si se produce un error en Kaspersky Embedded Systems Security 2.2 al crear el archivo de registro, esto no evitará que el comando se ejecute, pero se mostrará un mensaje de error.

Administración de una tarea especificada asíncronamente. KAVSHELL TASK

La utilización del comando `KAVSHELL TASK` le permite administrar la tarea especificada: ejecutar, pausar, reanudar y detener la tarea especificada y ver el estado y estadísticas de la tarea actual. El comando se ejecuta en modo asíncrono.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL TASK

```
KAVSHELL TASK [<alias de nombre de tarea> </START | /STOP | /PAUSE | /RESUME | /STATE | /STATISTICS >]
```

Ejemplos del comando KAVSHELL TASK

```
KAVSHELL TASK

KAVSHELL TASK on-access /START

KAVSHELL TASK user-task_1 /STOP

KAVSHELL TASK scan-computer /STATE
```

El comando `KAVSHELL TASK` se puede ejecutar sin modificadores o con uno o varios modificadores (consulte la tabla a continuación).

Table 41. Modificadores del comando KAVSHELL TASK

Clave	Descripción
Sin claves	Devuelve la lista de todas las tareas existentes de Kaspersky Embedded Systems Security 2.2. La lista contiene los campos: nombre alternativo de la tarea, categoría de la tarea (del sistema o personalizada) y estado de la tarea actual.
<alias de tarea>	En lugar del nombre de la tarea, en el comando SCAN TASK use el alias de tarea, un nombre corto adicional que Kaspersky Embedded Systems Security 2.2 asigna a las tareas. Para ver los alias de tarea de Kaspersky Embedded Systems Security 2.2, introduzca el comando KAVSHELL TASK sin ningún modificador
/START	Inicia la tarea especificada en modo asíncrono.
/STOP	Detiene la tarea especificada.
/PAUSE	Pone en pausa la tarea especificada.
/RESUME	Reanuda la tarea especificada en modo asíncrono.
/STATE	Muestra el estado de la tarea actual (por ejemplo, **En ejecución**, **Completada**, **En pausa**, **Detenida**, **Error**, **Iniciando** o **Recuperando**).
/STATISTICS	Recupera las estadísticas de la tarea: información acerca de la cantidad de objetos procesados desde el inicio de la tarea hasta la actualidad.

Códigos de devolución para el comando KAVSHELL TASK (consulte la sección “Códigos de devolución para el comando KAVSHELL TASK”, en la página 254).

Inicio y detención de tareas de protección en tiempo real. KAVSHELL RTP

El comando `KAVSHELL RTP` se puede utilizar para iniciar o detener todas las tareas de Protección en tiempo real.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL RTP

```
KAVSHELL RTP {/START | /STOP}
```

Ejemplo del comando KAVSHELL RTP

Para iniciar todas las tareas de Protección en tiempo real, ejecute el siguiente comando:

```
KAVSHELL RTP /START
```

El comando `KAVSHELL RTP` puede incluir cualquiera de los dos modificadores obligatorios (consulte la tabla a continuación).

Table 42. Modificadores del comando KAVSHELL RTP

Clave	Descripción
/START	Inicia todas las tareas de Protección en tiempo real: Protección de archivos en tiempo real y Uso de KSN.
/STOP	Detiene todas las tareas de Protección en tiempo real.

Administración de la tarea Control de inicio de aplicaciones KAVSHELL APPCONTROL /CONFIG

Puede usar el comando `KAVSHELL APPCONTROL /CONFIG` para configurar el modo en el cual la tarea Control de inicio de aplicaciones se ejecuta y supervisa la carga de módulos DLL.

Sintaxis del comando KAVSHELL APPCONTROL /CONFIG

```
/config /mode:<applyrules|statistics> [/dll:<no|yes>] | /config
/savetofile:<ruta completa al archivo XML>
```

Ejemplos del comando KAVSHELL APPCONTROL /CONFIG

► *Para ejecutar la tarea Control de inicio de aplicaciones en el modo **Activo** sin cargar DLL y guardar la configuración de la tarea después de la finalización, ejecute el siguiente comando:*

```
KAVSHELL APPCONTROL /CONFIG /mode:applyrules /dll:<no>
/savetofile:c:\appcontrol\config.xml
```

Puede ajustar la configuración de la tarea de Control de inicio de aplicaciones usando los parámetros de la línea de comandos (ver la tabla a continuación).

Table 43. Modificadores de comando KAVSHELL APPCONTROL /GENERATE

Clave	Descripción
`/mode:<applyrules|statistics>`	Modo de operación de la tarea Control de inicio de aplicaciones. Puede seleccionar uno de los siguientes modos: • active: aplicar reglas de Control de inicio de aplicaciones; • statistics: solo estadísticas.
`/dll:<no|yes>`	Habilitar o deshabilitar la supervisión de la carga de DLL.
`/savetofile: <ruta de acceso al archivo XML>`	Exportar determinadas reglas en el archivo indicado en formato XML.
`/savetofile: <el nombre completo al archivo xml>`	Guardar la lista de reglas en el archivo.
`/savetofile: <el nombre completo al archivo xml> /sdc`	Guardar la lista de reglas de Control de distribución de software en el archivo.
`/clearsdc`	Eliminar todas las reglas de control de distribución de software de la lista.

Generador de reglas de control de inicio de aplicaciones KAVSHELL APPCONTROL /GENERATE

Con el comando `KAVSHELL APPCONTROL /GENERATE` puede generar listas de reglas de Control de inicio de aplicaciones.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL APPCONTROL /GENERATE

```
KAVSHELL APPCONTROL /GENERATE <ruta de acceso a la carpeta> | /source:<ruta de acceso a archivos con lista de carpetas> [/masks:<edms>] [/runapp] [/rules:<ch|cp|h>] [/strong] [/user:<usuario o grupo de usuarios>] [/export:<ruta de acceso a archivo XML>] [/import:<a|r|m>] [/prefix:<prefijo para nombres de reglas>] [/unique]
```

Ejemplos del comando KAVSHELL APPCONTROL /GENERATE

- *Para generar reglas para archivos desde carpetas especificadas, ejecute el siguiente comando:*

  ```
  KAVSHELL APPCONTROL /GENERATE /source:c\folderslist.txt
  /export:c:\rules\appctrlrules.xml
  ```

- *Para generar reglas para archivos ejecutables de todas las extensiones disponibles en la carpeta especificada y, después de la finalización de la tarea, guardar las reglas generadas en el archivo XML del archivo especificado, ejecute el siguiente comando:*

  ```
  KAVSHELL APPCONTROL /GENERATE c:\folder /masks:edms
  /export:c\rules\appctrlrules.xml
  ```

Según la sintaxis de las claves, puede configurar la generación automática de reglas para la tarea Control de inicio de aplicaciones (consulte la tabla a continuación).

Table 44. Claves del comando KAVSHELL APPCONTROL /GENERATE

Clave	Descripción
Área de aplicación de las reglas de autorización	
<ruta de acceso a la carpeta>	Especifica la ruta de acceso a la carpeta con los archivos ejecutables que requieren reglas de autorización generadas automáticamente.
/source: <ruta de acceso al archivo con la lista de carpetas>	Especifica la ruta de acceso al archivo TXT con la lista de carpetas que contienen archivos ejecutables que requieren reglas de autorización generadas automáticamente.
/masks: <edms>	Especifica extensiones de archivos ejecutables que requieren reglas de autorización generadas automáticamente. Puede incluir archivos del área de aplicación de las reglas con las siguientes extensiones: • e: archivos EXE • d: archivos DLL • m: archivos MSI • s: scripts
/runapp	Al generar reglas de autorización, tenga en cuenta aplicaciones que se ejecuten en un equipo protegido en el momento de la realización de la tarea.

Clave	Descripción
Acciones al generar automáticamente reglas de autorización	
/rules: <ch|cp|h>	Especifica acciones para realizar durante la generación de reglas de autorización del Control de inicio de aplicaciones: • ch: usar un certificado digital. De no haber un certificado, usar hash SHA256. • cp: usar un certificado digital. De no haber un certificado, usar la ruta al archivo ejecutable. • h: usar hash SHA256.
/strong	Use el asunto y la huella del certificado digital al generar automáticamente las reglas de autorización de Control de inicio de aplicaciones. El comando se ejecuta si se especifica la clave /rules: <ch|cp>.
/user: <usuario o grupo de usuarios>	Especifica el nombre de usuario o un grupo de usuarios para los cuales se aplicarán las reglas. La aplicación supervisará las aplicaciones ejecutadas por el usuario especificado o el grupo de usuarios.
Acciones después de la finalización de Generador de reglas de control de inicio de aplicaciones	
/export: <ruta de acceso al archivo XML>	Guarda las reglas generadas en un archivo XML.
/unique	Agrega información sobre el equipo con aplicaciones instaladas que son la base para la generación de reglas de autorización del Control de inicio de aplicaciones.
/prefix: <prefijo para nombres de reglas>	Especifica el prefijo del nombre para generar reglas de autorización del control de inicios de aplicaciones.
/import: <a|r|m>	Importa las reglas generadas a la lista de reglas de control de inicio de aplicaciones especificadas según el principio de adición seleccionado. : • a: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican) • r: **Reemplazar reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un parámetro de la regla es único) • m: **Combinar con reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un parámetro de la regla es único)

Cómo completar la lista de reglas de Control de inicio de aplicaciones KAVSHELL APPCONTROL

Mediante `KAVSHELL APPCONTROL`, se pueden agregar reglas del archivo XML a la lista de reglas de la tarea de Control de inicio de aplicaciones según el principio seleccionado y también se pueden eliminar todas las reglas definidas de la lista.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL APPCONTROL

```
KAVSHELL APPCONTROL /append <ruta de acceso al archivo XML> | /replace <ruta de acceso al archivo XML> | /merge <ruta de acceso al archivo XML> | /clear
```

Ejemplo del comando KAVSHELL APPCONTROL

► *Para agregar reglas de un archivo XML a reglas ya especificadas para la tarea Control de inicio de aplicaciones según el principio Agregar a reglas existentes, ejecute el siguiente comando:*

```
KAVSHELL APPCONTROL /append c:\rules\appctrlrules.xml
```

Según la sintaxis de las claves, puede seleccionar el principio para agregar reglas nuevas a un archivo XML especificado para una lista de reglas definidas de Control de inicio de aplicaciones (consulte la tabla a continuación).

Table 45. Claves del comando `KAVSHELL SCAN`

Clave	Descripción
/append <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de inicio de aplicaciones según un archivo XML especificado. Principio de adición: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican).
/replace <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de inicio de aplicaciones según un archivo XML especificado. Principio de adición: **Reemplazar reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un parámetro de la regla es único).
/merge <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de inicio de aplicaciones según un archivo XML especificado. Principio de adición: **Combinar con reglas existentes** (las nuevas reglas no duplican reglas ya definidas).
/clear	Vacía la lista de reglas de Control de inicio de aplicaciones.

Llenado de la lista de reglas de Control de dispositivos. KAVSHELL DEVCONTROL

Mediante `KAVSHELL DEVCONTROL` se pueden agregar reglas del archivo XML a la lista de reglas de la tarea de Control de dispositivos según el principio seleccionado y también se pueden eliminar todas las reglas definidas de la lista.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis del comando KAVSHELL DEVCONTROL

```
KAVSHELL DEVCONTROL /append <ruta de acceso al archivo XML> | /replace <ruta de acceso al archivo XML> | /merge <ruta de acceso al archivo XML> | /clear
```

Ejemplo del comando KAVSHELL DEVCONTROL

► *Para agregar reglas de un archivo XML a reglas ya especificadas para la tarea de Control de dispositivos según **Agregar a reglas existentes**, ejecute el siguiente comando:*

```
KAVSHELL DEVCONTROL /append :c:\rules\devctrlrules.xml
```

Según la sintaxis de las claves, puede seleccionar el principio para agregar reglas nuevas de un archivo XML especificado a una lista de reglas definidas de Control de dispositivos (consulte la tabla a continuación).

Table 46. Claves del comando `KAVSHELL DEVCONTROL`

Clave	Descripción
/append <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de dispositivos según un archivo XML especificado. Principio de adición: **Agregar a reglas existentes** (las reglas con la configuración idéntica se duplican).
/replace <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de dispositivos según un archivo XML especificado. Principio de adición: **Reemplazar reglas existentes** (las reglas con parámetros idénticos no se agregan; la regla se agrega si al menos un parámetro de la regla es único).
/merge <ruta de acceso al archivo XML>	Renueva la lista de reglas de Control de dispositivos según un archivo XML especificado. Principio de adición: **Combinar con reglas existentes** (las nuevas reglas no duplican reglas ya definidas).
/clear	Vacía la lista de reglas de Control de dispositivos.

Inicio de la tarea de actualización de bases de datos de Kaspersky Embedded Systems Security 2.2. KAVSHELL UPDATE

El comando `KAVSHELL UPDATE` se puede utilizar para iniciar el comando de actualización de bases de datos de Kaspersky Embedded Systems Security 2.2 en modo sincrónico.

La tarea de actualización de bases de datos de Kaspersky Embedded Systems Security 2.2 ejecutada mediante un comando `KAVSHELL UPDATE` es una tarea temporal. Solo se muestra en la Consola de la aplicación mientras está en ejecución. Al mismo tiempo, se genera el registro de tareas. Se muestra en los **Registros de tareas** de la

Consola de la aplicación. Se pueden aplicar directivas de Kaspersky Security Center para actualizar tareas creadas e iniciadas mediante el comando `KAVSHELL UPDATE` y para actualizar tareas creadas en la Consola de la aplicación. Para obtener información sobre administrar Kaspersky Embedded Systems Security 2.2 en equipos con Kaspersky Security Center, consulte la sección “Administrar Kaspersky Embedded Systems Security 2.2 con Kaspersky Security Center".

Se pueden usar variables del entorno al especificar la ruta al origen de actualizaciones en esta tarea. Si se utilizan las variables del entorno de un usuario, ejecute el comando `KAVSHELL UPDATE` con los permisos de dicho usuario.

Sintaxis de comandos para KAVSHELL UPDATE

```
KAVSHELL UPDATE < Ruta al origen de actualizaciones | /AK | /KL> [/NOUSEKL]
[/PROXY:<dirección>:<puerto>] [/AUTHTYPE:<0-2>] [/PROXYUSER:<nombre de
usuario>] [/PROXYPWD:<contraseña>] [/NOPROXYFORKL] [/USEPROXYFORCUSTOM]
[/NOFTPPASSIVE] [/TIMEOUT:<segundos>] [/REG:<código iso3166>] [/W:<ruta del
archivo del registro de ejecución de la tarea>] [/ALIAS:<alias de la tarea>]
```

El comando KAVSHELL UPDATE tiene claves obligatorias y opcionales (consulte la tabla a continuación).

Ejemplos del comando KAVSHELL UPDATE

- *Para iniciar una tarea de actualización de bases de datos personalizada, ejecute el comando siguiente:*

```
KAVSHELL UPDATE
```

- *Para iniciar una tarea de actualización de bases de datos mediante los archivos de actualizaciones en la carpeta de red \\server\databases, ejecute el siguiente comando:*

```
KAVSHELL UPDATE \\server\databases
```

- *Para iniciar una tarea de actualización usando el servidor FTP ftp://dnl-ru1.kaspersky-labs.com/ y registrar todos los eventos de tareas al archivo de registro c:\update_report.log, ejecute el comando:*

```
KAVSHELL UPDATE ftp://dnl-ru1.kaspersky-labs.com /W:c:\update_report.log
```

- *Para descargar actualizaciones de la base de datos de Kaspersky Embedded Systems Security 2.2 del servidor de actualizaciones de Kaspersky Lab, conéctese con el origen de actualizaciones a través de un servidor proxy (dirección del servidor proxy: proxy.company.com, puerto: 8080), para acceder al equipo con la autenticación NTLM incorporada de Microsoft Windows con el nombre de usuario: inetuser, contraseña: 123456, y ejecute el siguiente comando:*

```
KAVSHELL UPDATE /KL /PROXY:proxy.company.com:8080 /AUTHTYPE:1
/PROXYUSER:inetuser /PROXYPWD:123456
```

Table 47. Claves del comando KAVSHELL UPDATE

Clave	Descripción
Origen de actualizaciones (clave obligatoria). Especifique una o varias fuentes. Kaspersky Embedded Systems Security 2.2 accederá a las fuentes en el orden en que están enumeradas. Delimite las fuentes con un espacio.	
<ruta en formato UNC>	Origen de actualizaciones definido por el usuario. Ruta a la carpeta de actualizaciones de red en formato UNC.

Clave	Descripción
<URL>	Origen de actualizaciones definido por el usuario. Dirección del servidor HTTP o FTP en que se ubica la carpeta de actualización.
<Carpeta local>	Origen de actualizaciones definido por el usuario. Carpeta en el equipo protegido.
/AK	El servidor de administración de Kaspersky Security Center como el origen de actualizaciones.
/KL	Los servidores de actualización de Kaspersky Lab como origen de actualizaciones.
/NOUSEKL	No utilice los servidores de actualización de Kaspersky Lab si no hay otros orígenes de actualizaciones disponibles (se utiliza de manera predeterminada).
Configuración del servidor proxy	
/PROXY:<dirección>:<puerto>	Nombre de red o dirección IP del servidor proxy y su puerto. Si no se especifica esta clave, Kaspersky Embedded Systems Security 2.2 detectará automáticamente la configuración del servidor proxy utilizado en la red de área local.
/AUTHTYPE:<0-2>	Esta clave especifica el método de autenticación para acceder al servidor proxy. Puede tener los valores siguientes: **0**: autenticación NTLM integrada de Microsoft Windows; Kaspersky Embedded Systems Security 2.2 se comunicará con el servidor proxy en la cuenta **Sistema local** (**SYSTEM**) **1**: autenticación NTLM integrada de Microsoft Windows; Kaspersky Embedded Systems Security 2.2 se comunicará con el servidor proxy en la cuenta con el nombre de inicio de sesión y la contraseña especificados por las claves /PROXYUSER y /PROXYPWD **2**: autenticación por el nombre de inicio de sesión y la contraseña especificados por las claves /PROXYUSER y /PROXYPWD (autenticación básica) Si no se requiere autenticación para acceder al servidor proxy, no es necesario especificar una clave.
/PROXYUSER:<nombre de usuario>	Nombre de usuario que se utilizará para acceder al servidor proxy. Si se especifica el valor de la clave /AUTHTYPE:0, se ignorarán las claves /PROXYUSER:<nombre de usuario> y /PROXYPWD:<contraseña>.
/PROXYPWD:<contraseña>	Contraseña de usuario que se utilizará para acceder al servidor proxy. Si se especifica el valor de la clave /AUTHTYPE:0, se ignorarán las claves /PROXYUSER:<nombre de usuario> y /PROXYPWD:<contraseña>. Si se especifica la clave /PROXYUSER y se omite /PROXYPWD, la contraseña se considerará en blanco.
/NOPROXYFORKL	No use la configuración del servidor proxy para establecer conexión con los servidores de actualización de Kaspersky Lab (se utiliza de manera predeterminada)
/USEPROXYFORCUSTOM	Utilice la configuración del servidor proxy para establecer conexión con los orígenes de actualizaciones definidos por el usuario (no se utiliza de manera predeterminada).
/USEPROXYFORLOCAL	Utilice la configuración del servidor proxy para establecer conexión con los orígenes de actualizaciones locales. Si no se especifica, se aplicará el valor **No usar el servidor proxy para las direcciones locales**.
Configuración general de los servidores FTP y HTTP	

Clave	Descripción
/NOFTPPASSIVE	Si se especifica esta clave, Kaspersky Embedded Systems Security 2.2 usará el modo de equipo FTP activo para establecer conexión con el equipo protegido. Si no se especifica esta clave, Kaspersky Embedded Systems Security 2.2 usará el modo de equipo FTP pasivo, si es posible.
/TIMEOUT:<cantidad de segundos>	Tiempo de espera de conexión del servidor FTP o HTTP. Si no especifica esta clave, Kaspersky Embedded Systems Security 2.2 usará el valor predeterminado: 10 seg. El valor de la clave debe ser un número entero.
/REG:<código iso3166>	Configuración regional. Esta clave se utiliza cuando se reciben actualizaciones de los servidores de actualización de Kaspersky Lab. Kaspersky Embedded Systems Security 2.2 optimiza la carga de actualización en el equipo protegido, ya que selecciona el servidor de actualizaciones más cercano. Como el valor de esta clave, especifique el código de letra del país de ubicación para el equipo protegido de acuerdo con ISO 3166-1, por ejemplo, /REG: gr o /REG:RU. Si esta clave se omite o se especifica un código del país inexistente, Kaspersky Embedded Systems Security 2.2 detectará la ubicación del equipo protegido según la configuración regional del equipo donde está instalada la Consola de la aplicación.
/ALIAS:<alias de la tarea>	Esta clave le permitirá asignar un nombre temporal a la tarea que se utilizará para acceder a la tarea durante su ejecución. Por ejemplo, se pueden ver las estadísticas de la tarea mediante el comando TASK. El alias de tarea debe ser único entre los alias de tarea de todos los componentes funcionales de Kaspersky Embedded Systems Security 2.2. Si no se especifica esta clave, se utilizará update_<kavshell_pid>, por ejemplo, update_1234. En la Consola de la aplicación, la tarea Update-databases (<fecha hora>) se asignará automáticamente, por ejemplo, Update-databases 16/08/2007 05:41:02 p. m.
/W:<ruta del archivo de registro de tareas>	Si se especifica esta clave, Kaspersky Embedded Systems Security 2.2 guardará el archivo de registro de tareas con el nombre definido por el valor de la clave. El archivo de registro contiene las estadísticas de ejecución, la hora de inicio y finalización (detención) de la tarea, e información sobre los eventos producidos en ella. El registro se utiliza para registrar eventos definidos por la configuración de los registros de tareas y el registro de eventos de Kaspersky Embedded Systems Security 2.2 en el "Visor de eventos". Se puede especificar la ruta relativa o absoluta del archivo de registro. Si se especifica solo el nombre de archivo sin la ruta, el archivo de registro se creará en la carpeta actual. Si se reinicia el comando con la misma configuración de registro, se sobrescribirá el archivo de registro existente. Se puede visualizar el archivo de registro mientras se ejecuta una tarea. El registro se muestra en el nodo **Registros de tareas** de la Consola de la aplicación. Si se produce un error en Kaspersky Embedded Systems Security 2.2 al crear el archivo de registro, esto no evita que el comando se ejecute o que se muestre un mensaje de error.

Códigos de devolución para el comando KAVSHELL UPDATE (en la página 255).

Reversión de actualizaciones de bases de datos de Kaspersky Embedded Systems Security 2.2. KAVSHELL ROLLBACK

El comando `KAVSHELL ROLLBACK` se puede utilizar para realizar una tarea del sistema Reversión de las bases de datos de Kaspersky Embedded Systems Security 2.2 (reversión de las bases de datos de Kaspersky Embedded

Systems Security 2.2 a la versión anteriormente instalada). El comando se realiza sincrónicamente.

Sintaxis del comando:

```
KAVSHELL ROLLBACK
```

Códigos de devolución para el comando KAVSHELL ROLLBACK (en la página 256).

Administración de inspección de registros. KAVSHELL TASK LOG-INSPECTOR

El comando `KAVSHELL TASK LOG-INSPECTOR` puede usarse para supervisar la integridad del entorno en base al análisis del registro de eventos de Windows.

Sintaxis del comando

```
KAVSHELL TASK LOG-INSPECTOR
```

Ejemplos del comando

```
KAVSHELL TASK LOG-INSPECTOR /stop
```

Table 48. Modificadores del comando KAVSHELL TASK LOG-INSPECTOR

Clave	Descripción
/START	Inicia la tarea especificada en modo asíncrono.
/STOP	Detiene la tarea especificada.
/STATE	Muestra el estado de la tarea actual (por ejemplo, *En ejecución, Completada, En pausa, Detenida, Error, Iniciando o Recuperando*).
/STATISTICS	Recupera las estadísticas de la tarea: información acerca de la cantidad de objetos procesados desde el inicio de la tarea hasta la actualidad.

Códigos de devolución para el comando KAVSHELL TASK LOG-INSPECTOR (consulte la sección “Códigos de devolución para el comando KAVSHELL TASK LOG-INSPECTOR”, en la página 254).

Activación de la aplicación KAVSHELL LICENSE

Las claves y los códigos de activación de Kaspersky Embedded Systems Security 2.2 se pueden administrar con el comando `KAVSHELL LICENSE`.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis de comandos para KAVSHELL FULLSCAN

```
KAVSHELL LICENSE [/ADD:<archivo de clave | código de activación> [/R] | /DEL:<clave | número de código de activación>]
```

Ejemplos del comando KAVSHELL SCAN

► *Para activar la aplicación, ejecute el comando:*

```
KAVSHELL.EXE LICENSE / ADD: <código de activación o clave>
```

► *Para ver información sobre las claves agregadas, ejecute el comando:*

```
KAVSHELL LICENSE
```

► *Para eliminar una clave agregada con el número de serie 0000-000000-00000001, ejecute el comando:*

```
KAVSHELL LICENSE /DEL:0000-000000-00000001
```

El comando `KAVSHELL LICENSE` se puede ejecutar con o sin claves (consulte la tabla a continuación).

Table 49. Claves del comando KAVSHELL LICENSE

Clave	Descripción
Sin claves	El comando devuelve la siguiente información sobre las claves agregadas: • Clave. • Tipo de licencia (comercial). • Duración de la licencia asociada con la clave. • Estado de la clave (activa o adicional). Si el valor especificado es *, la clave se ha agregado como clave adicional.
/ADD: <nombre del archivo de clave o código de activación>	Agrega la clave a través del archivo especificado o el código de activación. Se pueden usar variables del entorno del sistema al especificar la ruta al archivo de clave; no se permiten variables del entorno del usuario.
/R	El código de activación o la clave /R son una adición al código de activación o clave ADD/ e indican que el código de activación o la clave que se agregan son un código de activación o clave adicional.
/DEL:<clave o código de activación>	Elimina la clave con el número especificado o el código de activación seleccionado.

Códigos de devolución para el comando KAVSHELL LICENSE (consulte la sección “Código de devolución para el comando KAVSHELL LICENSE”, en la página 256).

Cómo habilitar, configurar y deshabilitar el registro de rastreo. KAVSHELL TRACE

El comando `KAVSHELL TRACE` se puede utilizar para habilitar y deshabilitar el registro de rastreo para todos los subsistemas de Kaspersky Embedded Systems Security 2.2 y para establecer el nivel de detalle del registro.

Kaspersky Embedded Systems Security 2.2 escribe la información en los archivos de rastreo y el archivo de volcado de memoria en formato no cifrado.

Sintaxis de comandos para KAVSHELL TRACE

```
KAVSHELL TRACE </ON /F:<ruta de la carpeta de archivo del registro de rastreo>
[/S:<tamaño máximo del registro en megabytes>]
[/LVL:debug|info|warning|error|critical] | /OFF>
```

Si se mantiene el registro de seguimiento y desea cambiar su configuración, introduzca el comando `KAVSHELL TRACE` con la clave /ON y especifique la configuración del registro con los valores de las claves /S y /LVL (consulte la tabla a continuación).

Table 50. Claves del comando KAVSHELL TRACE

Clave	Descripción
/ON	Habilita el registro de rastreo.
/F:<carpeta con archivos de registro de rastreo>	Esta clave especifica la ruta completa a la carpeta en la que se guardarán los archivos de registro de rastreo (obligatorio). Si se especifica la ruta de una carpeta inexistente, no se creará ningún archivo de registro. Se pueden utilizar las rutas de red en formato UNC (convención de nomenclatura universal), pero las rutas a carpetas en unidades de red del equipo protegido no se pueden especificar. Si el nombre de la carpeta de la que se especifica la ruta de acceso como el valor de la clave contiene un carácter de espacio, escriba la ruta de esta carpeta entre comillas, por ejemplo: /F:"C\Carpeta de rastreo". Se pueden usar variables del entorno del sistema al especificar la ruta a los archivos de registro de rastreo; no se permiten variables del entorno del usuario.
/S: <tamaño máximo de archivo de registro en megabytes>	Esta clave establece el tamaño máximo de un único archivo de registro de rastreo. Tan pronto como el archivo de registro alcanza el nivel máximo, Kaspersky Embedded Systems Security 2.2 comenzará a registrar información en un archivo nuevo; y el archivo de registro anterior se guardará. Si no se especifica el valor de esta clave, el tamaño máximo de un archivo de registro será 50 MB.
/LVL:debug|info|warning|error|critical	Esta clave define el nivel de detalle de registro desde máximo (**Toda la información de depuración**) en el que todos los eventos se graban en el registro, hasta mínimo (**Eventos críticos**) en el que solo se registran los eventos críticos. Si no se especifica esta clave, los eventos con el nivel de detalle **Toda la información de depuración** se registrarán en el registro de rastreo.
/OFF	Esta clave deshabilita el registro de rastreo.

Ejemplos del comando KAVSHELL TRACE

► *Para habilitar el registro de rastreo mediante el nivel de detalle **Toda la información de depuración** y el tamaño máximo del registro de 200 MB, y para guardar el archivo de registro en la carpeta C:\Trace Folder, ejecute el comando:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /S:200
```

► *Para habilitar el registro de seguimiento mediante el nivel de detalle **Eventos importantes** y para guardar el archivo de registro en la carpeta C:\Trace Folder, ejecute el comando:*

```
KAVSHELL TRACE /ON /F:"C:\Trace Folder" /LVL:warning
```

► *Para deshabilitar el registro de rastreo, ejecute el comando:*

```
KAVSHELL TRACE /OFF
```

Códigos de devolución para el comando KAVSHELL TRACE (consulte la sección “Códigos de devolución para el comando KAVSHELL TRACE”, en la página 256).

Desfragmentación de archivos de registro de Kaspersky Embedded Systems Security 2.2. KAVSHELL VACUUM

Con el comando `KAVSHELL VACUUM` puede desfragmentar los archivos de registro de aplicaciones. Le permite evitar errores del sistema o errores durante el trabajo de Kaspersky Embedded Systems Security 2.2 que estén relacionados con un almacenamiento de registros duros.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Se recomienda aplicar el comando `KAVSHELL VACUUM` para optimizar el almacenamiento de archivos de registro en caso de Análisis a pedido frecuentes e inicios de tareas de actualización. Al ejecutar el comando, Kaspersky Embedded Systems Security 2.2 renueva una estructura lógica para los archivos de registros de aplicación que se almacenan en un equipo protegido por la ruta especificada.

De forma predeterminada, los archivos de registro de aplicación se almacenan en C:\ProgramData\Kaspersky Lab\Kaspersky Embedded Systems Security 2.2\2.2\Reports. Si ha especificado manualmente otra ruta para el almacenamiento de registros, el comando `KAVSHELL VACUUM` ejecuta la desfragmentación para archivos en la carpeta que se especifica en la configuración de registros de Kaspersky Embedded Systems Security 2.2.

El tamaño grande de desfragmentación de archivos aumenta el periodo de ejecución del comando `KAVSHELL VACUUM`.

Las tareas de Protección en tiempo real y Control del equipo no están disponibles para realizarse durante la ejecución del comando `KAVSHELL VACUUM`. El proceso de desfragmentación en curso restringe el acceso al registro de Kaspersky Embedded Systems Security 2.2 y rechaza el registro de eventos. Para evitar la disminución del nivel de seguridad, se recomienda planificar la ejecución del comando `KAVSHELL VACUUM` en el tiempo inactivo con antelación.

► *Para desfragmentar archivos de registros de Kaspersky Embedded Systems Security 2.2, ejecute el comando siguiente:*

```
KAVSHELL VACUUM
```

La ejecución del comando es posible si se inicia con los derechos de la cuenta del administrador local.

Limpieza de la base de iSwift. KAVSHELL FBRESET

Kaspersky Embedded Systems Security 2.2 emplea la tecnología iSwift, que permite que la aplicación evite que se vuelvan a analizar los archivos que no se modificaron desde el último análisis (**Usar la tecnología iSwift**).

Kaspersky Embedded Systems Security 2.2 crea en el directorio %SYSTEMDRIVE%\System Volume Information los archivos klamfb.dat y klamfb2.dat, que contienen información sobre objetos limpios que ya se han analizado. El archivo klamfb.dat (klamfb2.dat) aumenta con la cantidad de archivos que analiza Kaspersky Embedded Systems Security 2.2. El archivo solo contiene información actual sobre la existencia de archivos en el sistema: si un archivo se elimina, Kaspersky Embedded Systems Security 2.2 purga la información sobre esto de fidbox.dat.

Para limpiar un archivo, utilice el comando `KAVSHELL FBRESET`.

Tenga en cuenta las siguientes especificaciones para ejecutar el comando `KAVSHELL FBRESET`:

- Durante la limpieza del archivo klamfb.dat mediante el comando KAVSHELL FBRESET, Kaspersky Embedded Systems Security 2.2 no pausa la protección (a diferencia de los casos de la eliminación manual de klamfb.dat).
- Kaspersky Embedded Systems Security 2.2 puede aumentar la carga de trabajo del equipo después de que los datos se borran en klamfb.dat. En este caso, el antivirus analiza todos los archivos a los que se accede por primera vez luego de borrar klamfb.dat. Después del análisis, Kaspersky Embedded Systems Security 2.2 vuelve a agregar a klamfb.dat la información sobre cada objeto analizado. Si se realizan nuevos intentos para acceder al objeto, la tecnología iSwift impedirá un nuevo análisis del archivo siempre que no se haya modificado.

La ejecución del comando `KAVSHELL FBRESET` solo está disponible si la línea de comandos se inicia mediante la cuenta de SYSTEM.

Cómo habilitar y deshabilitar la creación del archivo de volcado. KAVSHELL DUMP

La creación de instantáneas (archivo de volcado) para los procesos de Kaspersky Embedded Systems Security 2.2 en casos de interrupción anormal se puede habilitar o deshabilitar mediante el comando `KAVSHELL DUMP` (consulte la tabla a continuación). Además, se pueden tomar instantáneas de memoria de procesos en curso de Kaspersky Embedded Systems Security 2.2 en cualquier momento.

Para que el archivo de volcado se cree correctamente, el comando `KAVSHELL DUMP` se debe ejecutar mediante la cuenta de sistema local (SYSTEM).

Sintaxis de comandos para KAVSHELL DUMP

```
KAVSHELL DUMP </ON /F:<carpeta con el archivo de volcado>|/SNAPSHOT /F:< carpeta con el archivo de volcado> / P:<pid> | /OFF>
```

Ejemplos del comando KAVSHELL DUMP

► *Para habilitar la creación de un archivo de volcado; para guardar el archivo de volcado en la carpeta C:\Dump Folder, ejecute el comando:*

```
KAVSHELL DUMP /ON /F:"C:\Dump Folder"
```

► *Para realizar un volcado para el proceso con el Id. 1234 a la carpeta C:/Dumps, ejecute el comando:*

```
KAVSHELL DUMP /SNAPSHOT /F: C:\Dumps /P:1234
```

► *Para deshabilitar la generación del archivo de volcado, ejecute el comando:*

```
KAVSHELL DUMP /OFF
```

Table 51. Claves del comando KAVSHELL DUMP

Clave	Descripción
/ON	Habilita la creación del archivo de volcado de memoria de proceso en casos de interrupción anormal.
/F:<ruta de la carpeta con archivos de volcado>	Esta clave es obligatoria. Especifica la ruta a la carpeta en la cual se guardará el archivo de volcado. Si se especifica la ruta de una carpeta inexistente, no se creará el archivo de volcado. Las rutas de red se pueden utilizar en formato UNC (convención de nomenclatura universal), pero las rutas a carpetas en unidades de red del equipo protegido no se pueden especificar. Se pueden usar variables del entorno del sistema al especificar la ruta a la carpeta con el archivo de volcado de memoria; no se permiten variables del entorno del usuario.
/SNAPSHOT	Toma una instantánea de la memoria del proceso de Kaspersky Embedded Systems Security 2.2 en curso especificado y guarda el archivo de volcado en la carpeta de la ruta que está especificada por la clave /F.
/P	El identificador de proceso PID se muestra en el Administrador de tareas de Microsoft Windows.
/OFF	Deshabilita la creación del archivo de volcado de memoria de procesos en casos de interrupción anormal.

Códigos de devolución para el comando KAVSHELL DUMP (consulte la sección "Códigos de devolución para el comando KAVSHELL DUMP", en la página 257).

Importación de la configuración. KAVSHELL IMPORT

El comando `KAVSHELL IMPORT` permite importar la configuración de Kaspersky Embedded Systems Security 2.2, sus funciones y tareas de un archivo de configuración a una copia de Kaspersky Embedded Systems Security 2.2 en el equipo protegido. Se puede crear un archivo de configuración mediante el comando `KAVSHELL EXPORT`.

Es posible que se requiera una contraseña para ejecutar el comando. Para introducir la contraseña actual, utilice la clave `[/pwd:<contraseña>]`.

Sintaxis de comandos para KAVSHELL IMPORT

```
KAVSHELL IMPORT <nombre del archivo de configuración y ruta del archivo>
```

Ejemplos del comando KAVSHELL IMPORT

```
KAVSHELL IMPORT Host1.xml
```

Table 52. Claves del comando KAVSHELL IMPORT

Clave	Descripción
<nombre del archivo de configuración y ruta del archivo>	Nombre del archivo de configuración utilizado como el origen de importación de la configuración. Se pueden usar variables del entorno del sistema al especificar la ruta al archivo; no se permiten variables del entorno del usuario.

Códigos de devolución para el comando KAVSHELL IMPORT (consulte la sección “Códigos de devolución para el comando KAVSHELL IMPORT”, en la página 258).

Exportación de la configuración. KAVSHELL EXPORT

El comando `KAVSHELL EXPORT` permite exportar todos los valores de configuración de Kaspersky Embedded Systems Security 2.2 y sus tareas actuales a un archivo de configuración, a fin de importarlos más tarde a copias de Kaspersky Embedded Systems Security 2.2 instaladas en otros equipos.

Sintaxis de comandos para KAVSHELL EXPORT

```
KAVSHELL EXPORT <nombre del archivo de configuración y ruta del archivo>
```

Ejemplos del comando KAVSHELL EXPORT

```
KAVSHELL EXPORT Host1.xml
```

Table 53. Claves del comando KAVSHELL EXPORT

Clave	Descripción
<nombre del archivo de configuración y ruta del archivo>	Nombre del archivo de configuración que contendrá la configuración. Se puede asignar cualquier extensión al archivo de configuración. Se pueden usar variables del entorno del sistema al especificar la ruta al archivo; no se permiten variables del entorno del usuario.

Códigos de devolución para el comando KAVSHELL EXPORT (consulte la sección “Códigos de devolución para el comando KAVSHELL EXPORT”, en la página 258).

Integración con Microsoft Operations Management Suite. KAVSHELL OMSINFO

Con el comando KAVSHELL OMSINFO, puede revisar el estado de la aplicación, además de información sobre amenazas detectadas por bases de datos antivirus y el servicio KSN. Los datos sobre amenazas se toman desde los registros de eventos disponibles.

Sintaxis del comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO <ruta de acceso completa al archivo generado con nombre de archivo>
```

Ejemplos del comando KAVSHELL OMSINFO

```
KAVSHELL OMSINFO C:\Users\Admin\Desktop\omsinfo.json
```

Table 54. Claves del comando KAVSHELL OMSINFO

Clave	Descripción
<ruta de acceso al archivo generado con nombre de archivo>	El nombre del archivo generado, que contendrá información sobre el estado de aplicación y las amenazas detectadas.

Códigos de devolución de la línea de comandos

En esta sección

Código de devolución para los comandos KAVSHELL START y KAVSHELL STOP

Table 55. Código de devolución para los comandos KAVSHELL START y KAVSHELL STOP

Código de devolución	Descripción
0	Operación finalizada correctamente
-3	Error de permisos
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, el servicio de Kaspersky Embedded Systems Security 2.2 ya está en ejecución o detenido)
-7	Servicio no registrado
-8	El inicio de Servicio automático está deshabilitado.
-9	Error en el intento de inicio del equipo desde otra cuenta de usuario (de manera predeterminada, el servicio de Kaspersky Embedded Systems Security 2.2 se ejecuta desde la cuenta de usuario Sistema local)
-99	Error desconocido

Código de devolución para los comandos KAVSHELL SCAN y KAVSHELL SCANCRITICAL

Table 56. Código de devolución para los comandos KAVSHELL SCAN y KAVSHELL SCANCRITICAL

Código de devolución	Descripción
0	La operación se completó correctamente (no se detectaron amenazas)
1	Operación cancelada
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró el archivo con la lista de áreas de análisis)
-5	Sintaxis de comando no válida o área del análisis sin definir
-80	Objetos infectados y otros objetos detectados
-81	Objetos probablemente infectados detectados
-82	Errores de proceso detectados
-83	Objetos sin comprobar detectados
-84	Objetos dañados detectados
-85	Error de creación de archivo de registro de tareas

Código de devolución	Descripción
-99	Error desconocido
-301	Clave no válida

Códigos de devolución para el comando KAVSHELL TASK LOG-INSPECTOR

Table 57. Código de devolución para el comando KAVSHELL TASK LOG-INSPECTOR

Código de devolución	Descripción
0	Operación finalizada correctamente
-6	Operación no válida (por ejemplo, el servicio de Kaspersky Embedded Systems Security 2.2 ya está en ejecución o detenido)
402	La tarea ya se está ejecutando (para el modificador /STATE)

Códigos de devolución para el comando KAVSHELL TASK

Table 58. Códigos de devolución para el comando KAVSHELL TASK

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (tarea no encontrada)
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, la tarea no se está ejecutando, ya se está ejecutando o no se puede pausar)
-99	Error desconocido
-301	Clave no válida
401	La tarea no se está ejecutando (para el modificador /STATE)
402	La tarea ya se está ejecutando (para el modificador /STATE)
403	La tarea ya está en pausa (para el modificador /STATE)
-404	Error al ejecutar la operación (el cambio de estado de tarea provocó una interrupción del funcionamiento)

Códigos de devolución para el comando KAVSHELL RTP

Table 59. Códigos de devolución para el comando KAVSHELL RTP

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (una de las tareas de Protección en tiempo real o todas las tareas de Protección en tiempo real no han sido encontradas)
-5	Sintaxis de comando no válida
-6	Operación no válida (por ejemplo, la tarea ya está en ejecución o detenida)
-99	Error desconocido
-301	Clave no válida

Códigos de devolución para el comando KAVSHELL UPDATE

Table 60. Códigos de devolución para el comando KAVSHELL UPDATE

Código de devolución	Descripción
0	Operación finalizada correctamente
200	Todos los objetos están actualizados (base de datos o componentes del programa actuales)
-2	El servicio no está en ejecución
-3	Error de permisos
-5	Sintaxis de comando no válida
-99	Error desconocido
-206	Faltan archivos de extensión en la fuente especificada o estos tienen un formato desconocido
-209	Error al conectarse al origen de actualizaciones
-232	Error de autenticación al conectarse al servidor proxy
-234	Error al conectarse a Kaspersky Security Center
-235	Kaspersky Embedded Systems Security 2.2 no fue autenticado al conectarse con el origen de actualizaciones
-236	La base de datos de la aplicación está dañada
-301	Clave no válida

Códigos de devolución para el comando KAVSHELL ROLLBACK

Table 61. Códigos de devolución para el comando KAVSHELL ROLLBACK

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-99	Error desconocido
-221	Copia de seguridad de la base de datos no encontrada o dañada
-222	Copia de seguridad de la base de datos dañada

Códigos de devolución para el comando KAVSHELL LICENSE

Table 62. Códigos de devolución para el comando KAVSHELL LICENSE

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Privilegios insuficientes para administrar claves
-4	No se encontró la clave con el número especificado
-5	Sintaxis de comando no válida
-6	Operación no válida (clave ya agregada)
-99	Error desconocido
-301	Clave no válida
-303	La licencia se aplica a una aplicación diferente

Códigos de devolución para el comando KAVSHELL TRACE

Table 63. Códigos de devolución para el comando KAVSHELL TRACE

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos

Código de devolución	Descripción
-4	No se encontró el objeto (no se encontró la ruta especificada de la carpeta Registros de rastreo)
-5	Sintaxis de comando no válida
-6	Operación no válida (intento de ejecución del comando KAVSHELL TRACE /OFF si la creación de registros de rastreo ya está deshabilitada)
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL FBRESET

Table 64. Códigos de devolución para el comando KAVSHELL FBRESET

Código de devolución	Descripción
0	Operación finalizada correctamente
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL DUMP

Table 65. Códigos de devolución para el comando KAVSHELL DUMP

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró la ruta especificada de la carpeta del archivo de volcado; no se encontró el proceso con el PID especificado)
-5	Sintaxis de comando no válida
-6	Operación no válida (intento de ejecución del comando KAVSHELL DUMP/OFF si la creación de archivos de volcado ya está deshabilitada)
-99	Error desconocido

Códigos de devolución para el comando KAVSHELL IMPORT

Table 66. Códigos de devolución para el comando KAVSHELL IMPORT

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-4	No se encontró el objeto (no se encontró el archivo de configuración para importación)
-5	Sintaxis no válida
-99	Error desconocido
501	La operación finalizó correctamente. Sin embargo, se produjo un error/comentario durante la ejecución del comando, por ejemplo, Kaspersky Embedded Systems Security 2.2 no importó los parámetros de algunos componentes funcionales
-502	Falta el archivo que se está importando o el formato no se reconoce
-503	Configuración incompatible (archivo de configuración exportado desde un programa diferente o desde una versión posterior e incompatible de Kaspersky Embedded Systems Security 2.2)

Códigos de devolución para el comando KAVSHELL EXPORT

Table 67. Códigos de devolución para el comando KAVSHELL EXPORT

Código de devolución	Descripción
0	Operación finalizada correctamente
-2	El servicio no está en ejecución
-3	Error de permisos
-5	Sintaxis no válida
-10	No es posible crear el archivo de configuración (por ejemplo, no hay acceso a la carpeta especificada en la ruta del archivo)
-99	Error desconocido
501	La operación finalizó correctamente. Sin embargo, se produjo un error/comentario durante la ejecución del comando, por ejemplo, Kaspersky Embedded Systems Security 2.2 no exportó los parámetros de algunos componentes funcionales

Integración con sistemas de terceros

Esta sección describe la integración de Kaspersky Embedded Systems Security 2.2 con funciones y tecnologías de terceros.

En este capítulo

Control del rendimiento. Contadores de Kaspersky Embedded Systems Security 2.2

Esta sección brinda información sobre los contadores de Kaspersky Embedded Systems Security 2.2: Contadores de rendimiento del Supervisor del sistema y contadores y capturas de SNMP.

En este capítulo

Contadores de rendimiento para el supervisor del sistema

Esta sección contiene información sobre contadores de rendimiento para el supervisor del sistema de Microsoft Windows que Kaspersky Embedded Systems Security 2.2 registra durante la instalación.

En esta sección

Acerca de los contadores SNMP de Kaspersky Embedded Systems Security 2.2

El componente **Contadores de rendimiento** está incluido en los componentes instalados de Kaspersky Embedded Systems Security 2.2 de forma predeterminada. Kaspersky Embedded Systems Security 2.2 registra sus propios contadores de rendimiento en el supervisor del sistema de Microsoft Windows durante la instalación.

Mediante contadores de Kaspersky Embedded Systems Security 2.2, puede supervisar el rendimiento de la aplicación mientras se ejecutan tareas de Protección en tiempo real. Puede descubrir lugares estrechos cuando se ejecuta con otras aplicaciones y escasez de recursos. Puede diagnosticar la configuración no deseada de Kaspersky Embedded Systems Security 2.2, así como interrupciones en su funcionamiento.

Puede ver los contadores de rendimiento de Kaspersky Embedded Systems Security 2.2 si abre la consola **Rendimiento** en el elemento **Administración** del Panel de control de Windows.

Las siguientes secciones enumeran definiciones de contadores, intervalos recomendados para obtener lecturas, valores de umbral y recomendaciones para la configuración de Kaspersky Embedded Systems Security 2.2 si los valores del contador los superan.

Cantidad total de solicitudes denegadas

Table 68. Cantidad total de solicitudes denegadas

Nombre	Cantidad total de solicitudes denegadas
Definición	Cantidad total de solicitudes del controlador de interceptación de archivos para procesar los objetos que no fueron aceptados por procesos de la aplicación, obtenida desde el último inicio de Kaspersky Embedded Systems Security 2.2. La aplicación omite objetos para los cuales las solicitudes del procesamiento son denegadas por procesos de Kaspersky Embedded Systems Security 2.2.
Objetivo	Este contador puede ayudarlo a detectar: • Protección en tiempo real de menor calidad a raíz del atascamiento de los procesos de trabajo de Kaspersky Embedded Systems Security 2.2. • Interrupciones en la Protección en tiempo real debido a errores de distribuidor para la interceptación de archivos.
Valor umbral/ normal	0 / 1.
Intervalo de lectura recomendado	1 hora.

Recomendaciones para la configuración si el valor supera el umbral	La cantidad de solicitudes del proceso denegadas corresponde a la cantidad de objetos omitidos. Las siguientes situaciones son posibles según el comportamiento del contador: • El contador muestra varias solicitudes denegadas durante el periodo extendido: todos los procesos de Kaspersky Embedded Systems Security 2.2 se cargan totalmente para que Kaspersky Embedded Systems Security 2.2 no pueda analizar objetos. Para evitar que se omitan objetos, aumente el número de procesos de la aplicación para las tareas de Protección en tiempo real. Puede usar configuraciones de Kaspersky Embedded Systems Security 2.2 como **Número máximo de procesos activos** y **Número de procesos para la protección en tiempo real**. • La cantidad de solicitudes denegadas supera de manera considerable el umbral crítico y aumenta rápidamente: el distribuidor para la interceptación de archivos dejó de funcionar. Kaspersky Embedded Systems Security 2.2 no está analizando objetos durante el acceso. Reinicie Kaspersky Embedded Systems Security 2.2.

Cantidad total de solicitudes omitidas

Table 69. Cantidad total de solicitudes omitidas

Nombre	Cantidad total de solicitudes omitidas
Definición	La cantidad total de solicitudes del controlador de interceptación de archivos para procesar objetos que recibió Kaspersky Embedded Systems Security 2.2 pero que no generaron eventos de finalización de procesamiento. Esta cantidad se cuenta desde el momento en que la aplicación se inició por última vez. Si una solicitud para procesar ese objeto aceptada por uno de los procesos de trabajo no envió un evento para que finalice el procesamiento, el controlador transferirá dicha solicitud a otro proceso y el valor del contador **Cantidad total de solicitudes omitidas** se incrementará en 1. Si el controlador revisó todos los procesos en ejecución y ningún proceso recibió la solicitud de procesamiento (por estar ocupados) ni envió ningún evento de finalización de proceso, Kaspersky Embedded Systems Security 2.2 omitirá dicho objeto, y el valor del contador **Cantidad total de solicitudes omitidas** se incrementará en 1.
Objetivo	Este contador le permite detectar bajas en el rendimiento debido a errores del distribuidor para la interceptación de archivos.
Valor umbral/ normal	0 / 1
Intervalo de lectura recomendado	1 hora
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador es distinto de cero, significa que uno o varios flujos del distribuidor para la interceptación de archivos está interrumpido y no funciona. El valor del contador corresponde a la cantidad de flujos actualmente inactivos. Si la velocidad del análisis no es satisfactoria, reinicie Kaspersky Embedded Systems Security 2.2 a fin de restaurar los flujos fuera de línea.

Cantidad de solicitudes sin procesar por falta de recursos del sistema

Table 70. Cantidad de solicitudes sin procesar por falta de recursos del sistema

Nombre	Cantidad de solicitudes sin procesar por falta de recursos.
Definición	Cantidad total de solicitudes del controlador de interceptación de archivos que no se procesaron por falta de recursos del sistema (por ejemplo, de memoria RAM), calculada desde el último inicio de Kaspersky Embedded Systems Security 2.2. Kaspersky Embedded Systems Security 2.2 omite las solicitudes de procesamiento de objetos que no son procesadas por el controlador de interceptación de archivos.
Objetivo	Este contador se puede usar para detectar y eliminar una posible menor calidad de la Protección en tiempo real que se produce debido a una baja de recursos del sistema.
Valor umbral/ normal	0 / 1.
Intervalo de lectura recomendado	1 hora.
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador no es cero, los procesos en ejecución de Kaspersky Embedded Systems Security 2.2 necesitan más RAM para procesar solicitudes. Es posible que los procesos activos de otras aplicaciones estén usando toda la memoria RAM disponible.

Cantidad de solicitudes enviadas para su proceso

Table 71. Cantidad de solicitudes enviadas para su proceso

Nombre	Cantidad de solicitudes enviadas para su proceso.
Definición	La cantidad de objetos que esperan ser procesados por los procesos de trabajo.
Objetivo	Este contador se puede usar para hacer un rastreo de la carga de los procesos en ejecución de Kaspersky Embedded Systems Security 2.2 y del nivel general de la actividad de los archivos en el equipo.
Valor umbral/ normal	El valor el contador puede variar según el nivel de la actividad de los archivos en el equipo.
Intervalo de lectura recomendado	1 minuto
Recomendaciones para la configuración si el valor supera el umbral	No

Cantidad promedio de flujos del distribuidor para la interceptación de archivos

Table 72. Cantidad promedio de flujos del distribuidor para la interceptación de archivos

Nombre	Cantidad promedio de flujos del distribuidor para la interceptación de archivos.
Definición	La cantidad de flujos del distribuidor para la interceptación de archivos en un proceso y el promedio de todos los procesos actualmente involucrados en tareas de Protección en tiempo real.
Objetivo	Este contador se puede usar para detectar y eliminar una posible menor calidad de la Protección en tiempo real que se produce porque los procesos de Kaspersky Embedded Systems Security 2.2 se ejecutan con carga completa.
Valor umbral/ normal	Varía / 40
Intervalo de lectura recomendado	1 minuto
Recomendaciones para la configuración si el valor supera el umbral	Se pueden crear hasta 60 flujos del distribuidor para la interceptación de archivos en cada proceso de trabajo. Si el valor del contador se acerca a 60, existe el riesgo de que ninguno de los procesos en ejecución pueda procesar la solicitud siguiente en la cola del controlador de interceptación de archivos y de que Kaspersky Embedded Systems Security 2.2 omita el objeto. Aumente la cantidad de procesos de Kaspersky Embedded Systems Security 2.2 para las tareas de Protección en tiempo real. Puede usar dicha configuración de Kaspersky Embedded Systems Security 2.2 como **Número máximo de procesos activos** y **Número de procesos para la protección en tiempo real**.

Cantidad máxima de flujos del distribuidor para la interceptación de archivos

Table 73. Cantidad máxima de flujos del distribuidor para la interceptación de archivos

Nombre	Cantidad máxima de flujos del distribuidor para la interceptación de archivos.
Definición	La cantidad de flujos del distribuidor para la interceptación de archivos en un proceso y la cantidad máxima de todos los procesos actualmente involucrados en tareas de Protección en tiempo real.
Objetivo	Este contador le permite detectar y eliminar bajas de rendimiento debido a una distribución de cargas dispar en los procesos en ejecución.
Valor umbral/ normal	Varía / 40
Intervalo de lectura recomendado	1 minuto
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador supera de manera considerable y continua el valor siguiente del contador **Cantidad promedio de flujos de distribuidor para la interceptación de archivos**, Kaspersky Embedded Systems Security 2.2 está distribuyendo la carga para los procesos en ejecución de manera dispar. Reinicie Kaspersky Embedded Systems Security 2.2.

Cantidad de elementos en la cola de objetos infectados

Table 74. Cantidad de elementos en la cola de objetos infectados

Nombre	Cantidad de elementos en la cola de objetos infectados.
Definición	Cantidad de objetos infectados que actualmente esperan ser procesados (desinfectados o eliminados).
Objetivo	Este contador puede ayudarlo a detectar: • Interrupciones en la Protección en tiempo real debido a posibles errores de distribuidor para la interceptación de archivos. • Sobrecarga de procesos debido a una distribución dispar del tiempo del procesador entre diferentes procesos en ejecución y Kaspersky Embedded Systems Security 2.2. • Ataques de virus.
Valor umbral/ normal	Este valor puede ser distinto de cero mientras Kaspersky Embedded Systems Security 2.2 procesa objetos infectados o probablemente infectados, pero regresará a cero cuando el procesamiento haya finalizado./El valor se mantiene distinto de cero durante un periodo prolongado.
Intervalo de lectura recomendado	1 minuto
Recomendaciones para la configuración si el valor supera el umbral	Si el valor del contador no regresa a cero durante un periodo prolongado: • Kaspersky Embedded Systems Security 2.2 no está procesando objetos (es posible que se haya interrumpido el distribuidor para la interceptación de archivos). Reinicie Kaspersky Embedded Systems Security 2.2. • El tiempo del procesador es insuficiente para procesar los objetos. Asegúrese de que Kaspersky Embedded Systems Security 2.2 reciba tiempo adicional del procesador (por ejemplo, disminuya la carga de otras aplicaciones en el equipo). • Se produjo un brote de virus. Una gran cantidad de objetos infectados o probablemente infectados en la tarea de Protección de archivos en tiempo real también es un signo de un brote de virus. Puede consultar la información sobre el número de objetos detectados en las estadísticas de la tarea o los registros de tareas.

Cantidad de objetos procesados por segundo

Table 75. Cantidad de objetos procesados por segundo

Nombre	Cantidad de objetos procesados por segundo.
Definición	Cantidad de objetos procesados dividida por la cantidad de tiempo empleado para procesar esos objetos (calculada durante intervalos de tiempo idénticos).

Objetivo	Este contador refleja la velocidad de procesamiento de objetos. Se puede usar para detectar y eliminar niveles bajos de rendimiento del equipo que se producen debido a que el procesador asigna tiempo insuficiente a los procesos de Kaspersky Embedded Systems Security 2.2 o debido a errores en la operación de Kaspersky Embedded Systems Security 2.2.
Valor umbral/ normal	Varía / n.º
Intervalo de lectura recomendado	1 minuto.
Recomendaciones para la configuración si el valor supera el umbral	Los valores de este contador dependen de los valores establecidos en la configuración de Kaspersky Embedded Systems Security 2.2 y de la carga de procesos de otras aplicaciones en el equipo. Observe el nivel promedio de las cantidades del contador durante un periodo prolongado. Si disminuye el nivel general de los valores del contador, es posible que se haya producido una de las siguientes situaciones: • Los procesos de Kaspersky Embedded Systems Security 2.2 no disponen del tiempo del procesador necesario para procesar los objetos. Asegúrese de que Kaspersky Embedded Systems Security 2.2 reciba tiempo adicional del procesador (por ejemplo, disminuya la carga de otras aplicaciones en el equipo). • Kaspersky Embedded Systems Security 2.2 experimentó un error (varios flujos están inactivos). Reinicie Kaspersky Embedded Systems Security 2.2.

Contadores y capturas SNMP de Kaspersky Embedded Systems Security 2.2

Esta sección contiene información sobre contadores y capturas de Kaspersky Embedded Systems Security 2.2.

En esta sección

Acerca de contadores y capturas SNMP de Kaspersky Embedded Systems Security 2.2

Si ha incluido **contadores y capturas SNMP** en el conjunto de componentes Antivirus para instalar, puede ver contadores y capturas de Kaspersky Embedded Systems Security 2.2 a través del Protocolo simple de administración de redes (SNMP).

Para ver los contadores y las capturas de Kaspersky Embedded Systems Security 2.2 desde la estación de trabajo del administrador, inicie el servicio SNMP en el equipo protegido e inicie los servicios de capturas SNMP en la estación de trabajo del administrador.

Contadores SNMP de Kaspersky Embedded Systems Security 2.2

Esta sección contiene tablas con una descripción de la configuración para los contadores SNMP de Kaspersky Embedded Systems Security 2.2.

En esta sección

Contadores de rendimiento

Table 76. Contadores de rendimiento

Contador	Definición
currentRequestsAmount	Cantidad de solicitudes enviadas para su proceso (en la página 262)
currentInfectedQueueLength	Número de elementos en la cola de objetos infectados (consulte la sección “Número de elementos en la cola de objetos infectados”, en la página 264)
currentObjectProcessingRate	Cantidad de objetos procesados por segundo (en la página 264)
currentWorkProcessesNumber	Cantidad actual de procesos de trabajo utilizados por Kaspersky Embedded Systems Security 2.2

Contadores de cuarentena

Table 77. Contadores de cuarentena

Contador	Definición
totalObjects	Cantidad de objetos que se encuentran actualmente en cuarentena
totalSuspiciousObjects	Cantidad de objetos probablemente infectados que se encuentran actualmente en cuarentena
currentStorageSize	Tamaño total de datos en cuarentena (MB)

Contadores de Copia de seguridad

Table 78. Contadores de Copia de seguridad

Contador	Definición
currentBackupStorageSize	Tamaño total de datos en copia de seguridad (MB)

Contadores generales

Table 79. Contadores generales

Contador	Definición
lastCriticalAreasScanAge	El periodo desde el último análisis completo de las áreas críticas del equipo (tiempo transcurrido en segundos desde que se completó la última tarea de *Análisis de áreas críticas*).
licenseExpirationDate	Fecha de caducidad de la licencia. Si se ha agregado una clave activa y claves adicionales, se muestra la fecha de caducidad de la licencia asociada con la clave adicional.
currentApplicationUptime	Cantidad de tiempo que Kaspersky Embedded Systems Security 2.2 ha estado en ejecución desde su último inicio, en centésimos de segundos.
currentFileMonitorTaskStatus	Estado de la tarea de Protección de archivos en tiempo real: **Encendido**: en ejecución; **Apagado**: detenida o en pausa.

Contador de actualización

Table 80. Contador de actualizaciones

Contador	Definición
avBasesAge	"Antigüedad" de las bases de datos (tiempo transcurrido en centésimos de segundos desde la fecha de creación de las bases de datos con las últimas actualizaciones instaladas).

Contadores de protección en tiempo real

Table 81. Contadores de protección en tiempo real

Contador	Definición
totalObjectsProcessed	Cantidad total de objetos analizados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalInfectedObjectsFound	Cantidad total de Objetos infectados y otros objetos detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalSuspiciousObjectsFound	Cantidad total de Objetos probablemente infectados detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalVirusesFound	Cantidad total de objetos detectados desde la hora en que se ejecutó la última tarea de Protección de archivos en tiempo real
totalObjectsQuarantined	Cantidad total de objetos infectados, objetos infectados y otros objetos que Kaspersky Embedded Systems Security 2.2 colocó en cuarentena; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotQuarantined	Cantidad total de objetos infectados o probablemente infectados que Kaspersky Embedded Systems Security 2.2 intentó poner en cuarentena pero no pudo hacerlo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez

Contador	Definición
totalObjectsDisinfected	Cantidad total de objetos infectados que Kaspersky Embedded Systems Security 2.2 desinfectó; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotDisinfected	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security 2.2 intentó desinfectar pero no pudo hacerlo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsDeleted	Cantidad total de objetos infectados, objetos infectados y otros objetos que Kaspersky Embedded Systems Security 2.2 desinfectó; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotDeleted	Cantidad total de objetos probablemente infectados, objetos infectados y otros objetos que Kaspersky Embedded Systems Security 2.2 intentó desinfectar pero no pudo hacerlo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsBackedUp	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security 2.2 colocó en Copia de seguridad; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez
totalObjectsNotBackedUp	Cantidad total de objetos infectados y otros objetos que Kaspersky Embedded Systems Security 2.2 intentó colocar en Copia de seguridad pero no pudo hacerlo; se calcula desde la hora en que se inició la tarea de Protección de archivos en tiempo real por última vez

Capturas SNMP

La configuración de capturas SNMP en Kaspersky Embedded Systems Security 2.2 se resume en la tabla a continuación.

Table 82. Capturas SNMP de Kaspersky Embedded Systems Security 2.2

Captura	Descripción	Opciones
eventThreatDetected	Se ha detectado un objeto.	eventDateAndTime eventSeverity computerName userName objectName threatName detectType detectCertainty

Captura	Descripción	Opciones
eventBackupStorageSizeExceeds	Se superó el tamaño máximo de la copia de seguridad. El tamaño total de los datos en la copia de seguridad ha excedido el valor especificado por el **Tamaño máx. de Copia de seguridad (MB)**. Kaspersky Embedded Systems Security 2.2 continúa realizando copias de seguridad de objetos infectados.	eventDateAndTime eventSeverity eventSource
eventThresholdBackupStorageSizeExceeds	Umbral de espacio disponible para la copia de seguridad alcanzado. La cantidad de espacio libre en Copia de seguridad asignado por el **Valor umbral de espacio disponible (MB)** es igual o menor que el valor especificado. Kaspersky Embedded Systems Security 2.2 continúa realizando copias de seguridad de objetos infectados.	eventDateAndTime eventSeverity eventSource
eventQuarantineStorageSizeExceeds	Se superó el tamaño máximo de la cuarentena El tamaño total de los datos en Cuarentena ha superado el valor especificado por el **Tamaño máximo de cuarentena (MB)**. Kaspersky Embedded Systems Security 2.2 continúa poniendo en cuarentena objetos probablemente infectados.	eventDateAndTime eventSeverity eventSource
eventThresholdQuarantineStorageSizeExceeds	Umbral de espacio disponible para la cuarentena alcanzado. La cantidad de espacio libre en la Cuarentena asignado por el **Valor umbral de espacio disponible (MB)** es inferior al valor especificado. Kaspersky Embedded Systems Security 2.2 continúa poniendo en cuarentena objetos probablemente infectados.	eventDateAndTime eventSeverity eventSource

Captura	Descripción	Opciones
eventObjectNotQuarantined	Error de cuarentena.	eventSeverity eventDateAndTime eventSource userName computerName objectName storageObjectNotAddedEventReason
eventObjectNotBackuped	Error al guardar una copia de objeto en Copia de seguridad.	eventSeverity eventDateAndTime eventSource objectName userName computerName storageObjectNotAddedEventReason
eventQuarantineInternalError	Error de cuarentena.	eventSeverity eventDateAndTime eventSource eventReason
eventBackupInternalError	Error de Copia de seguridad.	eventSeverity eventDateAndTime eventSource eventReason
eventAVBasesOutdated	La base de datos antivirus está desactualizada. Se está calculando la cantidad de días desde la última ejecución de la tarea de actualización de bases de datos (tarea local o tarea de grupo, o tarea para conjuntos de equipos).	eventSeverity eventDateAndTime eventSource días
eventAVBasesTotallyOutdated	La base de datos antivirus es obsoleta. Se está calculando la cantidad de días desde la última ejecución de la tarea de actualización de bases de datos (tarea local o tarea de grupo, o tarea para conjuntos de equipos).	eventSeverity eventDateAndTime eventSource días

Captura	Descripción	Opciones
eventApplicationStarted	Kaspersky Embedded Systems Security 2.2 se está ejecutando.	eventSeverity eventDateAndTime eventSource
eventApplicationShutdown	Kaspersky Embedded Systems Security 2.2 está detenido.	eventSeverity eventDateAndTime eventSource
eventCriticalAreasScanWasntPerformForALongTime	Las áreas críticas no se han analizado durante un periodo prolongado. Calculado como la cantidad de días desde la última finalización de la tarea de *Análisis de áreas críticas* .	eventSeverity eventDateAndTime eventSource días
eventLicenseHasExpired	La licencia ha caducado.	eventSeverity eventDateAndTime eventSource
eventLicenseExpiresSoon	La licencia expira pronto. Calculado como la cantidad de días hasta la fecha de caducidad de la licencia.	eventSeverity eventDateAndTime eventSource días
eventTaskInternalError	La tarea finalizó con un error.	eventSeverity eventDateAndTime eventSource errorCode knowledgeBaseId taskName
eventUpdateError	Error al realizar una tarea de actualización.	eventSeverity eventDateAndTime taskName updaterErrorEventReason

La siguiente tabla describe la configuración de capturas y los valores de parámetros posibles.

Table 83. Capturas SNMP: valores de la configuración

Configuración	Descripción y valores posibles
eventDateAndTime	Hora del evento.
eventSeverity	Nivel de importancia. La configuración puede tener los siguientes valores: • critical (1): crítico • warning (2): advertencia • info (3): informativo

Configuración	Descripción y valores posibles
userName	Nombre de usuario (por ejemplo, nombre de usuario que intentó acceder a un archivo infectado).
computerName	Nombre del equipo (por ejemplo, nombre del equipo desde el que se intentó acceder a un archivo infectado).
eventSource	Origen de evento: componente funcional donde se generó el evento. La configuración puede tener los siguientes valores: • unknown (0): componente funcional no conocido • quarantine (1): cuarentena • backup (2): Copia de seguridad • reporting (3): registros de tareas • updates (4): actualización • realTimeProtection (5): protección de archivos en tiempo real • onDemandScanning (6): análisis a pedido • product (7): evento relacionado con la operación de Kaspersky Embedded Systems Security 2.2 en su totalidad en lugar de estar relacionado con operaciones de componentes individuales • systemAudit (8): registro de auditoría del sistema
eventReason	Activador del evento: qué provocó el evento. La configuración puede tener los siguientes valores: • reasonUnknown(0): se desconoce el motivo • reasonInvalidSettings (1): solo para los eventos de copia de seguridad y cuarentena, se muestra si la cuarentena o la copia de seguridad no están disponibles (permisos de acceso insuficientes o la carpeta está especificada de manera incorrecta en la Configuración de cuarentena, por ejemplo, se especificó una ruta de red). En este caso, Kaspersky Embedded Systems Security 2.2 utilizará la carpeta de Copia de seguridad o de Cuarentena predeterminada.
objectName	Nombre de objeto (por ejemplo, nombre del archivo donde se detectó el virus).
threatName	El nombre del objeto según la clasificación de la Enciclopedia de Virus. Este nombre se incluye en el nombre completo del objeto detectado en los resultados de detección de objetos de Kaspersky Embedded Systems Security 2.2. Puede ver el nombre completo de un objeto detectado en el registro de tareas (consulte la sección “Configuración del registro”, en la página 143).
detectType	Tipo de objeto detectado. La configuración puede tener los siguientes valores: • undefined (0): sin definir • virware: virus habituales y gusanos de red • trojware: troyanos • malware: otros programas maliciosos • adware: software de publicidad • pornware: software pornográfico • riskware: aplicaciones legítimas que utilizan los intrusos para dañar el equipo o los datos del usuario

Configuración	Descripción y valores posibles
detectCertainty	Nivel de certeza de detección de amenaza. La configuración puede tener los siguientes valores: • Sospecha (probablemente infectado): Kaspersky Embedded Systems Security 2.2 ha detectado una coincidencia parcial entre una sección del código del objeto y la sección del código malicioso conocido. • Seguro (infectado): Kaspersky Embedded Systems Security 2.2 ha detectado una coincidencia completa entre una sección del código del objeto y la sección del código malicioso conocido.
días	Cantidad de días (por ejemplo, la cantidad de días hasta la fecha de caducidad de la licencia).
errorCode	Código de error.
knowledgeBaseId	Dirección de un artículo de la base de conocimientos (por ejemplo, dirección del artículo que explica un error en particular).
taskName	Nombre de la tarea.
updaterErrorEventReason	Motivo del error de actualización. La configuración puede tener los siguientes valores: • reasonUnknown(0): se desconoce el motivo • reasonAccessDenied: acceso denegado • reasonUrlsExhausted: se agotó la lista de orígenes de actualizaciones • reasonInvalidConfig: archivo de configuración no válido • reasonInvalidSignature: firma no válida • reasonCantCreateFolder: no se puede crear la carpeta • reasonFileOperError: error de archivo • reasonDataCorrupted: el objeto está dañado • reasonConnectionReset: conexión restablecida • reasonTimeOut: se excedió el tiempo de espera de conexión • reasonProxyAuthError: error de autenticación de proxy • reasonServerAuthError: error de autenticación del servidor • reasonHostNotFound: no se encuentra el equipo • reasonServerBusy: servidor no disponible • reasonConnectionError: error de conexión • reasonModuleNotFound: no se encontró el objeto • reasonBlstCheckFailed(16): error al consultar la lista negra de claves. Es posible que se estuvieran publicando actualizaciones de las bases de datos durante la actualización; repita la actualización dentro de unos minutos.

Configuración	Descripción y valores posibles
storageObjectNotAdded EventReason	Motivo por el que no se realizó una copia de seguridad del objeto o no se colocó en cuarentena. La configuración puede tener los siguientes valores: • reasonUnknown(0): se desconoce el motivo • reasonStorageInternalError: error de base de datos, restaure Kaspersky Embedded Systems Security 2.2. • reasonStorageReadOnly: la base de datos es de solo lectura; restaure Kaspersky Embedded Systems Security 2.2. • reasonStorageIOError: error de entrada-salida: a) Kaspersky Embedded Systems Security 2.2 está dañado, reinicie Kaspersky Embedded Systems Security 2.2; b) el disco con archivos de Kaspersky Embedded Systems Security 2.2 está dañado. • reasonStorageCorrupted: el almacenamiento está dañado, restaure Kaspersky Embedded Systems Security 2.2. • reasonStorageFull: la base de datos está completa; libere espacio en disco • reasonStorageOpenError: no se pudo abrir el archivo de base de datos; restaure Kaspersky Embedded Systems Security 2.2. • reasonStorageOSFeatureError: algunas funciones del sistema operativo no se corresponden con los requisitos de Kaspersky Embedded Systems Security 2.2. • reasonObjectNotFound: el objeto que se coloca en cuarentena no existe en el disco. • reasonObjectAccessError: permisos insuficientes para usar la API de Copia de seguridad: la cuenta que se utiliza para realizar la operación no tiene permisos del operador de Copia de seguridad • reasonDiskOutOfSpace: espacio en disco insuficiente

Integración con WMI

Kaspersky Embedded Systems Security 2.2 admite la integración con Windows Management Instrumentation (WMI): puede usar sistemas cliente que utilicen WMI para recibir datos a través del estándar Web-Based Enterprise Management (WBEM) para recopilar información sobre el estado de Kaspersky Embedded Systems Security 2.2 y sus componentes.

Cuando se instala Kaspersky Embedded Systems Security 2.2, registra el módulo propietario en el sistema, lo que facilita la creación de un espacio de nombre de Kaspersky Embedded Systems Security 2.2 y de un espacio de nombre WMI en el equipo local. Un espacio de nombre de Kaspersky Embedded Systems Security 2.2 le permite trabajar con clases e instancias de Kaspersky Embedded Systems Security 2.2 y sus propiedades.

Los valores de algunas propiedades de instancias dependen de los tipos de tareas.

Tarea no periódica es una tarea de aplicación que no posee límite de tiempo, y puede estar en constante ejecución o detenida. No existe progreso de ejecución existe para estas tareas. Los resultados de la ejecución de la tarea se registran sin parar mientras la tarea se está ejecutando como evento individual (por ejemplo, la detección de un objeto infectado por cualquiera de las tareas de Protección del equipo en tiempo real). Este tipo de tareas se administra mediante las directivas de Kaspersky Security Center.

Tarea periódica es una tarea de aplicación que posee límite de tiempo y posee un progreso de ejecución que se muestra como porcentaje. Los resultados de la tarea se generan después de su finalización, y se representan como un solo elemento o estado de aplicación modificado (por ejemplo, actualización de bases de datos de la aplicación completada, archivos de configuración generados para las tareas de generación de reglas). Se pueden ejecutar varias tareas periódicas del mismo tipo en un solo equipo simultáneamente (tres tareas de Análisis a pedido con diferentes áreas del

análisis). Las tareas periódicas se pueden administrar mediante Kaspersky Security Center como tareas de grupo.

Si usa herramientas para generar consultas de espacios de nombre WMI y recibir datos dinámicos de espacios de nombre WMI en una red corporativa, podrá recibir información sobre el estado de la aplicación actual (consulte la tabla a continuación).

Table 84. Información sobre el estado de la aplicación

Propiedad de la instancia	Descripción	Valores
ProductName	El nombre de la aplicación instalada.	Nombre completo de aplicación sin número de versión.
ProductVersion	La versión completa de la aplicación instalada	Número completo de la versión de la aplicación, incluido el número de compilación.
InstalledPatches	El grupo de nombres de parches que se implementaron para la aplicación.	La lista de parches críticos instalados para la aplicación.
IsLicenseInstalled	El estado de activación de la aplicación.	El estado de la clave utilizada para activar la aplicación. Valores posibles: • False: no se han configurado una clave o el código de activación en la aplicación. • True: se han agregado una clave o el código de activación en la aplicación.
LicenseDaysLeft	Muestra cuántos días restan antes de que caduque la licencia actual.	Número de días restantes antes del vencimiento de la licencia actual. Valores no positivos posibles: • 0 - La licencia ha caducado • -1 - No se pudo obtener información sobre la clave actual, o la clave especificada no puede usarse para activar la aplicación (por ejemplo, se bloquea según una lista negra de claves).
AVBasesDatetime	La marca de fecha y hora para una versión de la base de datos antivirus actual.	Fecha y hora de la creación de las bases de datos antivirus actualmente en uso. Si la aplicación instalada no usa bases de datos antivirus, el campo tiene el valor “No instalada”.

Propiedad de la instancia	Descripción	Valores
IsExploitPreventionEnabled	El estado del componente Prevención de exploits.	Estado del componente Prevención de exploits. Valores posibles: • True - El componente Prevención de exploits está habilitado y ofrece protección. • False - El componente Prevención de exploits no ofrece protección. Por ejemplo: desactivado, no instalado, se ha infringido el contrato de licencia.
ProtectionTasksRunning	El grupo de tareas de protección que se están ejecutando actualmente.	Enumera las tareas de protección, control y supervisión que se están ejecutando actualmente. Este campo debería explicar todas las tareas no periódicas en ejecución. Si no se está ejecutando ninguna tarea no periódica, el campo tiene el valor "No".
IsAppControlRunning	El estado de la tarea Control de inicio de aplicaciones.	Estado de la tarea Control de inicio de aplicaciones. • True - La tarea Control de inicio de aplicaciones se está ejecutando actualmente. • False - La tarea Control de inicio de aplicaciones no se está ejecutando actualmente o el componente Control de inicio de aplicaciones no está instalado.
AppControlMode	El modo de la tarea Control de inicio de aplicaciones.	Descripción del estado actual del componente Control de inicio de aplicaciones que explicita el modo seleccionado para la tarea correspondiente. Valores posibles: • Activo - El modo **Activo** está seleccionado en la configuración de la tarea. • Solo estadísticas - El modo **Solo estadísticas** está seleccionado en la configuración de la tarea. • No instalado - El componente Control de inicio de aplicaciones no está instalado
AppControlRulesNumber	Número total de reglas de control de inicio de aplicaciones.	El número de reglas especificadas actualmente en la configuración de la tarea Control de inicio de aplicaciones.

Propiedad de la instancia	Descripción	Valores
AppControlLastBlocking	La marca de fecha y hora del último inicio de aplicaciones bloqueado por la tarea Control de inicio de aplicaciones en cualquier modo.	La fecha y la hora en que el componente Control de inicio de aplicaciones bloqueó por última vez el inicio de una aplicación. Este campo incluye todas las aplicaciones bloqueadas, sin tener en cuenta el modo de la tarea. Si no hay ninguna instancia de inicio de aplicaciones bloqueada registrada al momento de procesar la consulta WMI, se asigna el valor “No” al campo.
PeriodicTasksRunning	El grupo de tareas periódicas que se están ejecutando actualmente.	Lista de tareas Análisis a pedido, Actualización y de inventario que se están ejecutando actualmente. Este campo debe incluir todas las tareas periódicas en ejecución. Si ninguna tarea periódica se están ejecutando actualmente, el campo tiene el valor "No".
ConnectionState	El estado de la conexión entre el componente Proveedor de WMI y el servicio de Kaspersky Security (KAVFS).	Información sobre el estado de la conexión entre el módulo Proveedor de WMI y el servicio de Kaspersky Security. Valores posibles: • Éxito - Se estableció correctamente la conexión: el cliente de WMI puede recibir la información sobre el estado de la aplicación. • Error. Código de error: <código> - La conexión no se pudo establecer debido a un error con el código especificado.

Estos datos representan propiedades de instancias KasperskySecurity_ProductInfo.ProductName=Kaspersky Embedded Systems Security, donde:

- KasperskySecurity_ProductInfo es el nombre de la clase Kaspersky Embedded Systems Security 2.2
- .ProductName=Kaspersky Embedded Systems Security es el parámetro de la clave s the Kaspersky Embedded Systems Security 2.2

La instancia se crea en el espacio de nombre ROOT\Kaspersky\Security.

Comunicarse con el soporte técnico

Esta sección describe cómo se puede recibir soporte técnico y las condiciones en las cuales se encuentra disponible.

En este capítulo

Cómo acceder al Servicio de soporte técnico

Si no encuentra una solución a su problema en la documentación de la aplicación ni en ninguna de las fuentes de información sobre la aplicación, le recomendamos que se comunique con el Servicio de soporte técnico. Los especialistas del soporte técnico responderán sus preguntas acerca de la instalación y el uso de la aplicación.

El soporte técnico se encuentra disponible solo para los usuarios que adquirieron una licencia comercial de la aplicación. El soporte técnico no está disponible para los usuarios que tienen una licencia de prueba.

Antes de ponerse en contacto con el servicio de soporte técnico, lea rápidamente las reglas del Servicio de soporte técnico.

Puede comunicarse con el soporte técnico en una de las siguientes maneras:

- Llamando al servicio de soporte técnico.
- Enviando una solicitud al servicio de soporte técnico de Kaspersky Lab por medio del portal de Kaspersky CompanyAccount (https://companyaccount.kaspersky.com).

Soporte técnico mediante Kaspersky CompanyAccount

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) es un portal para empresas que usan aplicaciones de Kaspersky Lab. Kaspersky CompanyAccount está diseñado para facilitar la interacción entre usuarios y especialistas de Kaspersky Lab mediante solicitudes en línea. El portal de Kaspersky CompanyAccount le permite supervisar el progreso del procesamiento de solicitud electrónico por parte de especialistas de Kaspersky Lab y almacenar un historial de solicitudes electrónicas.

Puede registrar a todos los empleados de su organización en una única cuenta de usuario en Kaspersky CompanyAccount. Una única cuenta le permite administrar de manera centralizada las solicitudes electrónicas de empleados registrados en Kaspersky Lab y también gestionar los privilegios de dichos empleados mediante Kaspersky CompanyAccount.

Kaspersky CompanyAccount se encuentra disponible en los siguientes idiomas:

- 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 http://support.kaspersky.com/faq/companyaccount_help.

Uso de archivos de rastreo y scripts AVZ

Después de informar un problema a los especialistas del servicio de soporte técnico de Kaspersky Lab, es posible que le soliciten que genere un informe con datos sobre el funcionamiento de Kaspersky Embedded Systems Security 2.2 y que lo envíe al servicio de soporte técnico de Kaspersky Lab. También es posible que los especialistas del servicio de soporte técnico de Kaspersky Lab le pidan que cree un archivo de rastreo. El archivo de rastreo le permite seguir el proceso de cómo se llevan a cabo los comandos de la aplicación, paso a paso, a fin de determinar la etapa de funcionamiento de la aplicación en la que se produce el error.

Luego de analizar los datos que envíe, los especialistas de soporte técnico de Kaspersky Lab pueden crear un script AVZ y enviárselo. Mediante los scripts AVZ resulta posible analizar procesos activos en busca de amenazas, analizar el equipo en busca de amenazas, desinfectar o eliminar archivos infectados y crear informes de análisis del sistema.

Para una mayor eficacia en la asistencia y la solución de problemas de la aplicación, es posible que los especialistas del Servicio de soporte técnico le soliciten que cambie la configuración de la aplicación temporalmente con fines de depuración durante el diagnóstico. Esto puede requerir que realice lo siguiente:

- Activar la funcionalidad que procesa y almacena información diagnóstica ampliada.
- Afinar la configuración de los componentes individuales de la aplicación, que no están disponibles mediante los elementos de la interfaz de usuario estándar.
- Cambiar la configuración del almacenamiento y la transmisión de la información de diagnóstico que se procesa.
- Configurar la interceptación y el registro del tráfico de red.

AO Kaspersky Lab

Kaspersky Lab es un proveedor de fama internacional de sistemas para proteger equipos contra diferentes tipos de amenazas digitales, incluidos virus y otro malware, correo electrónico no solicitado (spam), ataques de hackers y de redes.

En 2008, Kaspersky Lab fue clasificado entre los cuatro mayores proveedores del mundo en cuanto a soluciones de software de seguridad de información para usuarios finales (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab es el proveedor preferido de sistemas de protección de equipos domésticos en Rusia (IDC Endpoint Tracker 2014).

Kaspersky Lab se creó en Rusia en 1997. Desde entonces, se ha convertido en un grupo internacional de compañías con 38 oficinas en 33 países. La compañía emplea a más de 3000 profesionales especializados.

Productos. Los productos de Kaspersky Lab proporcionan protección para todos los sistemas, desde equipos domésticos hasta grandes redes corporativas.

La gama de productos personales incluye aplicaciones de seguridad para equipos de escritorio, equipos portátiles, equipos tablet, teléfonos inteligentes y otros dispositivos móviles.

La empresa ofrece soluciones de protección y control, y tecnologías para estaciones de trabajo y dispositivos móviles, máquinas virtuales, servidores de archivos y web, puertas de enlace de correo y firewalls. La cartera de productos de la compañía incluye además productos especializados que ofrecen protección contra ataques de DDoS, protección para sistemas de control industriales y prevención de fraude financiero. Utilizado en conjunto con herramientas de administración centralizadas, estas soluciones garantizan una protección automatizada efectiva para compañías y organizaciones contra amenazas de equipos de cualquier tamaño. Los productos de Kaspersky Lab están certificados por importantes laboratorios de pruebas, son compatibles con software de diferentes proveedores y están optimizados para funcionar en varias plataformas de hardware.

Los analistas de virus de Kaspersky Lab trabajan las 24 horas. Todos los días, descubren cientos de miles de amenazas informáticas nuevas, crean herramientas para detectarlas y desinfectarlas, e incluyen sus firmas en las bases de datos que utilizan las aplicaciones de Kaspersky Lab.

Tecnologías. Muchas tecnologías que ahora son parte integral de las herramientas antivirus modernas fueron desarrolladas por Kaspersky Lab. No es ninguna coincidencia que muchos otros desarrolladores usen el motor de Kaspersky Anti-Virus en sus productos, entre ellos: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu y ZyXEL. Muchas de las tecnologías innovadoras de la compañía están patentadas.

Logros. Con el paso de los años, Kaspersky Lab ha obtenido cientos de premios por sus servicios para combatir las amenazas informáticas. Después de las pruebas y la investigación realizadas por el prestigioso laboratorio de pruebas austríaco AV-Comparatives en 2014, Kaspersky Lab se clasificó entre los dos primeros proveedores por el número de certificados Advanced+ que obtuvo y, finalmente, se le otorgó el certificado de clasificación más alta. Sin embargo, el logro principal de Kaspersky Lab es la lealtad de sus usuarios en todo el mundo. Los productos y las tecnologías de la compañía protegen a más de 400 millones de usuarios, y sus clientes corporativos suman más de 270 000.

Sitio web de Kaspersky Lab:	https://latam.kaspersky.com/
Enciclopedia de Virus:	https://securelist.lat/
Virus Lab:	https://virusdesk.kaspersky.com/ (para analizar archivos y sitios web sospechosos)
Foro web de Kaspersky Lab:	https://forum.kaspersky.com

Información sobre código de terceros

La información sobre código de terceros se encuentra en el archivo denominado legal_notices.txt, en la carpeta de instalación de la aplicación.

Avisos de marcas registradas

Las marcas comerciales registradas y las marcas de servicio son propiedad de sus respectivos titulares.

Intel y Pentium son marcas comerciales de Intel Corporation en los Estados Unidos y/u otros países.

Microsoft, Active Directory, Excel, Internet Explorer, Outlook, Windows, Windows Server y Windows Vista son marcas comerciales registradas de Microsoft Corporation en los Estados Unidos y otros países.

Linux es la marca comercial registrada de Linus Torvalds en los Estados Unidos y otros países.

Glosario

A

Actualización

El procedimiento de sustituir o agregar archivos nuevos (bases de datos o módulos de la aplicación) que se recuperaron de los servidores de actualización de Kaspersky Lab.

Analizador heurístico

Una tecnología para detectar amenazas sobre la información que aún no se ha agregado a las bases de datos de Kaspersky Lab. El analizador heurístico detecta objetos que, por su comportamiento, pueden ser una amenaza para la seguridad del sistema operativo. Los objetos detectados por el analizador heurístico se consideran probablemente infectados. Por ejemplo, un objeto se puede considerar probablemente infectado si contiene secuencias de comandos que son habituales de objetos maliciosos (abrir archivo, escribir en el archivo).

Archivo comprimido

Uno o varios archivos empaquetados en un solo archivo a través de la compresión. Se requiere una aplicación dedicada, denominada archivador, para comprimir y descomprimir los datos.

Archivo infectable

Un archivo que, debido a su estructura o formato, puede ser utilizado por criminales como contenedor para almacenar y extender código malicioso. Como regla general, se trata de archivos ejecutables con extensiones de archivo como .com, .exe, y .dll. El riesgo de penetración del código malicioso en estos archivos es bastante alto.

B

Bases de datos antivirus

Bases de datos que contienen información sobre amenazas a la seguridad de los equipos que son conocidas por Kaspersky Lab a la fecha de publicación de las bases de datos antivirus. Las entradas en las bases de datos antivirus permiten que se detecte código malicioso en objetos analizados. Las bases de datos antivirus son creadas por especialistas de Kaspersky Lab y se actualizan cada hora.

C

Clave activa

Una clave que es utilizada actualmente por la aplicación.

Configuración de tareas

Configuración de la aplicación que es específica de cada tipo de tarea.

Copia de seguridad

Un almacenamiento especial para copias de seguridad de archivos, que se crean antes de intentar operaciones de desinfección o eliminación.

Cuarentena

Carpeta a la que la aplicación Kaspersky Lab pasa los objetos probablemente infectados que se han detectado. Los objetos se almacenan en Cuarentena de forma cifrada con el fin de evitar cualquier efecto en el equipo.

D

Desinfección

Método de procesamiento de objetos infectados que produce una recuperación total o parcial de datos. No todos los objetos infectados se pueden desinfectar.

Directiva

Una directiva determina la configuración de una aplicación y administra el acceso a la configuración de una aplicación instalada en equipos dentro de un grupo de administración. Debe crearse una directiva particular para cada aplicación. Puede crear un número ilimitado de distintas directivas para aplicaciones instaladas en equipos en cada grupo de administración, pero se puede aplicar solo una directiva a cada aplicación de forma simultánea dentro de un grupo de administración.

E

Estado de protección

El estado de protección actual, que refleja el nivel de seguridad del equipo.

F

Falso positivo

Una situación en la cual una aplicación de Kaspersky Lab considera que un objeto no infectado está infectado porque su código es similar al de un virus.

G

Gravedad del evento

Propiedad de un evento encontrada durante la operación de una aplicación de Kaspersky Lab. Hay cuatro niveles de gravedad:

- Evento crítico.
- Error.
- Advertencia.
- Información.

Los eventos del mismo tipo pueden tener niveles de gravedad diferentes según la situación en la cual se produjeron.

K

Kaspersky Security Network (KSN)

Una infraestructura de servicios en la nube que permite acceder a la base de datos de Kaspersky Lab con información constantemente actualizada sobre la reputación de archivos, recursos web y software. Kaspersky Security Network asegura respuestas más rápidas por parte de aplicaciones de Kaspersky Lab a amenazas, mejora el rendimiento de algunos componentes de protección y reduce la posibilidad de falsos positivos.

M

Máscara de archivo

Representación de un nombre de archivo con comodines. Los comodines estándar utilizados en máscaras del archivo son * y ?, dónde * representa cualquier número de cualquier cantidad de caracteres, y ? representa cualquier carácter.

N

Nivel de seguridad

El nivel de seguridad se define como un conjunto preconfigurado de opciones del componente de la aplicación.

O

Objetos de inicio

Un conjunto de aplicaciones necesario para que el sistema operativo y el software que está instalado en el equipo se inicie y funcione correctamente. Estos objetos se ejecutan cada vez que se inicia el sistema operativo. Hay virus capaces de infectar específicamente estos objetos y que pueden conducir, por ejemplo, al bloqueo del inicio del sistema operativo.

Objeto infectado

Un objeto que posee una porción de código coincide completamente con parte de código de malware conocido.

Kaspersky Lab no recomienda acceder a esos objetos.

Objeto OLE

Un objeto vinculado a otro archivo o integrado en otro archivo a través del uso de la tecnología Object Linking and Embedding (OLE). Un ejemplo de un objeto OLE es una hoja de cálculo de Microsoft Office Excel® integrada en un documento de Microsoft Office Word.

P

Protección en tiempo real

Modo de funcionamiento de la aplicación en el cual se analizan los objetos para detectar la presencia de código malicioso en tiempo real.

La aplicación intercepta todos los intentos de abrir un objeto (leer, escribir o ejecutar) y analiza el objeto para detectar amenazas. Los objetos no infectados se pasan al usuario, mientras que los objetos que contienen amenazas u objetos probablemente infectados se procesan según la configuración de la tarea (desinfectado, eliminado o en cuarentena).

S

Servidor de administración

Un componente de Kaspersky Security Center que almacena centralmente la información sobre todas las aplicaciones de Kaspersky Lab que se instalan dentro de la red corporativa. También puede usarse para administrar estas aplicaciones.

SIEM

Una tecnología que analiza eventos de seguridad que provienen de varias aplicaciones y dispositivos de red.

T

Tarea

Las funciones realizadas por la aplicación Kaspersky Lab se implementan como tareas, por ejemplo: Protección de archivos en tiempo real, Análisis completo del equipo y Actualización de bases de datos.

Tarea local

Una tarea definida y en ejecución en un solo equipo cliente.

Término de la licencia

Un periodo de tiempo durante el cual se tiene acceso a las funciones de la aplicación y a derechos de usar servicios adicionales. Los servicios que se pueden usar dependen del tipo de licencia.

V

Vulnerabilidad

Una falla en un sistema operativo o una aplicación que puede ser utilizada por programadores de malware para penetrar en el sistema operativo o la aplicación y corromper su integridad. Presencia de una gran cantidad de vulnerabilidades en el sistema operativo que no lo hacen de confianza, debido a que los virus que penetraron en el sistema operativo pueden ocasionar alteraciones en él y en las aplicaciones instaladas.

Índice

D