Kaspersky Security Center 10

Guía del Administrador

VERSIÓN DE LA APLICACIÓN: 10 SERVICE PACK 1

Estimado usuario:

Gracias por escoger nuestros productos. Esperamos que esta documentación lo ayude en su trabajo y proporcione las respuestas relativas a este software.

Fecha de revisión: 02/02/2015

http://www.kaspersky.com
http://support.kaspersky.com

TABLA DE CONTENIDO

ACERCA DE ESTE DOCUMENTO 9
- En este documento 9
- Convenciones del documento 11

FUENTES DE INFORMACIÓN ACERCA DE LA APLICACIÓN 12
- Fuentes de información para investigación independiente 12
- Debate sobre las aplicaciones de Kaspersky Lab en el foro 13

KASPERSKY SECURITY CENTER 14
- Novedades 15
- Kit de distribución 16
- Requisitos de hardware y software 17

INTERFAZ DE LA APLICACIÓN 20
- Ventana principal de la aplicación 20
- Árbol de consola 22
- Espacio de trabajo 24
  - Conjunto de bloques de administración 26
  - Lista de objetos de administración 26
  - Conjunto de bloques de información 28
- Bloque de filtrado de datos 29
- Menú contextual 31
- Configuración de la interfaz 31

LICENCIA DE LA APLICACIÓN 33
- Acerca del Contrato de licencia de usuario final 33
- Acerca de la licencia 33
- Acerca de la clave 34
- Opciones de licencias de Kaspersky Security Center 34
- Acerca de las restricciones de las funciones principales 35
- Acerca del código de activación 36
- Acerca del archivo de clave 36

ASISTENTE DE INICIO RÁPIDO DE KASPERSKY SECURITY CENTER 38

CONCEPTOS BÁSICOS 39
- Servidor de administración 39
- Jerarquía del Servidor de administración 40
- Servidor de administración virtual 40
- Servidor de dispositivos móviles 41
- Servidor web 41
- Grupo de administración del Agente de red 42
- Estación de trabajo del administrador 42
- Complemento de administración de aplicaciones 42
- Directivas, parámetros de la aplicación y tareas 43
- Modo en que se relacionan las directivas y la configuración local de la aplicación 44

ADMINISTRACIÓN DE LOS SERVIDORES DE ADMINISTRACIÓN 46
- Conexión a un Servidor de administración y alternancia entre Servidores de administración 46
- Permisos de acceso al Servidor de administración y sus objetos 47
- Condiciones de conexión a un Servidor de administración a través de Internet 48
- Conexión segura con Servidor de administración 49
  - Certificado del Servidor de administración 49
  - La autenticación del Servidor de administración durante la conexión del equipo cliente 49
  - Autenticación del Servidor de administración durante la conexión de la Consola 49
- Desconexión de un Servidor de administración 50
- Agregar un Servidor de administración al árbol de consola 50

Eliminar un Servidor de administración del árbol de consola 50
Cambio de una cuenta de servicio del Servidor de administración. Utilidad klsrvswch 50
Visualización y modificación de la configuración de un Servidor de administración 51
Ajuste de la configuración general del Servidor de administración 51
Configuración de parámetros de procesamiento de eventos 51
Control de focos de virus 52
Límite de tráfico 52
Configurar la cooperación con Cisco Network Admission Control (NAC) 52
Configurar el Servidor web 52
Interacción entre el Servidor de administración y el servicio de proxy de KSN 53
Trabajar con usuarios internos 53
ADMINISTRAR GRUPOS DE ADMINISTRACIÓN 54
Creación de grupos de administración 54
Traslado de grupos de administración 55
Eliminación de grupos de administración 56
Creación automática de la estructura de grupos de administración 56
Instalación automática de aplicaciones en equipos de un grupo de administración 57
ADMINISTRACIÓN DE LAS APLICACIONES DE FORMA REMOTA 58
Administrar directivas 58
Creación de directivas 59
Mostrar directiva heredada en un subgrupo 59
Activar una directiva 59
Activar una directiva automáticamente en el evento de foco de virus 60
Implementación de una directiva fuera de la oficina 60
Eliminar una directiva 60
Copiar una directiva 60
Exportación de una directiva 61
Importación de una directiva 61
Convertir directivas 61
Administración de perfiles de directivas 61
Acerca de los perfiles de directivas 62
Crear un perfil de directiva 63
Modificar un perfil de directiva 63
Eliminar un perfil de directiva 64
Administración de tareas 64
Crear una tarea de grupo 65
Crear una tarea del Servidor de administración 65
Creación de una tarea para un conjunto de equipos 66
Crear una tarea local 66
Mostrar una tarea de grupo heredada en el espacio de trabajo de un grupo anidado 67
Iniciar equipos cliente automáticamente antes de iniciar una tarea 67
Apagar el equipo una vez que se haya completado la tarea 67
Limitar el tiempo de ejecución de la tarea 67
Exportar una tarea 68
Importar una tarea 68
Convertir tareas 68
Iniciar y detener una tarea manualmente 69
Pausar y reanudar una tarea manualmente 69
Supervisar la ejecución de tareas 69
Ver resultados de la ejecución de tareas almacenados en el Servidor de administración 69
Configurar el filtrado de información sobre resultados de la ejecución de tareas 70
Ver y modificar la configuración local de la aplicación 70
ADMINISTRACIÓN DE EQUIPOS CLIENTE 71
Conexión de equipos cliente al Servidor de administración 71
Conexión manual de un equipo cliente al Servidor de administración. Utilidad klmover 72

Creación de un túnel de conexión entre un equipo cliente y el Servidor de administración 73
Conexión remota al escritorio de un equipo cliente 73
Configurar el reinicio de un equipo cliente 74
Auditoría de acciones en un equipo cliente remoto 75
Comprobación de la conexión entre un equipo cliente y el Servidor de administración 75
Comprobación automática de la conexión entre un equipo cliente y el Servidor de administración 76
Comprobación manual de la conexión entre un equipo cliente y el Servidor de administración. Utilidad klnagchk 76
Identificación de equipos cliente en el Servidor de Administración 76
Agregar equipos a un grupo de administración 77
Cambio del Servidor de administración para equipos cliente 77
Encendido, apagado y reinicio remoto de equipos cliente 78
Enviar un mensaje a los usuarios de equipos cliente 78
Controlar los cambios en el estado de las máquinas virtuales 79
Diagnóstico remoto de los equipos cliente. Utilidad de diagnóstico remoto de Kaspersky Security Center 79
Conexión de la utilidad de diagnóstico remoto a un equipo cliente 80
Habilitar y deshabilitar el seguimiento, descargar el archivo de seguimiento 81
Descargar configuraciones de aplicaciones 82
Descarga de registros de eventos 82
Inicio de los diagnósticos y descarga de los resultados 82
Inicio, detención y reinicio de las aplicaciones 82

ADMINISTRACIÓN DE CUENTAS DE USUARIO 83
Manejo de cuentas de usuario 83
Agregar una cuenta de usuario 83
Configuración de derechos. Roles de usuarios 84
Agregar un rol de usuario 84
Asignación de un rol a un usuario o grupo de usuarios 85
Enviar mensajes a los usuarios 85
Ver la lista de dispositivos móviles de un usuario 85
Instalar un certificado para un usuario 86
Ver la lista de certificados entregados a un usuario 86

TRABAJO CON INFORMES, ESTADÍSTICAS Y NOTIFICACIONES 87
Trabajo con informes 87
Crear una plantilla de informe 87
Crear y ver un informe 88
Guardar un informe 88
Crear una tarea de envío de informes 88
Manejo de la información estadística 89
Configurar los parámetros de notificación 89
Selecciones de eventos 90
Visualizar una selección de equipos 90
Personalizar una selección de eventos 90
Crear una selección de eventos 91
Exportar una selección de eventos a un archivo de texto 91
Eliminar eventos de la selección 91
Exportación de eventos a un sistema SIEM 91
Selecciones de equipos 92
Visualizar una selección de equipos 92
Configurar una selección de equipos 93
Crear una selección de equipos 93
Exportar una configuración de selección de equipos a un archivo 93
Crear una selección de equipos mediante una configuración importada 93
Eliminación de equipos de los grupos de administración en una selección 94
Selecciones de directivas 94
Selecciones de tarea 94

EQUIPOS NO ASIGNADOS 95
Descubrimiento de red 95
Visualizar y modificar la configuración del sondeo de la red de Windows 96
Ver y modificar las propiedades de grupos de Active Directory 96
Visualizar y modificar los parámetros para el sondeo de la subred IP 96
Trabajar con dominios de Windows. Ver y cambiar la configuración de dominio 97
Trabajar con subredes IP 97
Crear una subred IP 97
Ver y modificar los parámetros de la subred IP 97
Trabajar con los grupos de Active Directory. Ver y cambiar la configuración de grupo 98
Crear reglas para mover equipos a grupos de administración automáticamente 98
Usar el modo dinámico para VDI en los equipos cliente 98
Habilitación del modo dinámico VDI en las propiedades de un paquete de instalación para el Agente de red 99
Buscar equipos que formen parte de la VDI 99
Mover los equipos que forman parte de la VDI a un grupo de administración 99
ADMINISTRAR APLICACIONES EN EQUIPOS CLIENTE 100
Grupos de aplicaciones 100
Creación de categorías de aplicaciones 101
Configuración de administración de inicio de aplicaciones en los equipos cliente 102
Visualización de los resultados de los análisis estadísticos de las reglas de inicio aplicadas a los archivos ejecutables 102
Visualización del registro de aplicaciones 103
Crear grupos de aplicaciones con licencia 103
Administración de claves para los grupos de aplicaciones con licencia 103
Visualización de información sobre archivos ejecutables 104
Vulnerabilidades de la aplicación 104
Visualización de información acerca de vulnerabilidades en las aplicaciones 105
Búsqueda de vulnerabilidades en las aplicaciones 105
Reparación de vulnerabilidades en las aplicaciones 105
Actualizaciones de software 106
Visualización de información sobre actualizaciones disponibles 106
Sincronización de las actualizaciones de Windows Update con el Servidor de administración 107
Instalación automática de actualizaciones en equipos cliente 107
Instalación manual de actualizaciones en equipos cliente 108
Configuración de actualizaciones de aplicaciones en una directiva del Agente de red 109
INSTALACIÓN REMOTA DE SISTEMAS OPERATIVOS Y APLICACIONES 110
Crear imágenes de sistemas operativos 111
Agregar controladores para el Entorno de preinstalación de Windows (WinPE) 111
Agregar controladores a un paquete de instalación con una imagen del sistema operativo 112
Configurar la utilidad sysprep.exe 112
Distribuir sistemas operativos en los nuevos equipos de la red 113
Distribuir sistemas operativos en los equipos cliente 113
Crear paquetes de instalación de aplicaciones 114
Instalar aplicaciones en los equipos cliente 114
ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES 115
Administración de dispositivos móviles mediante una directiva MDM 115
Manejo de comandos para dispositivos móviles 116
Comandos para administración de dispositivos móviles 116
Utilizando Google Cloud Messaging 118
Enviar comandos 118
Ver los estados de los comandos en el registro de comandos 119
Manejo de certificados 119
Instalación de un certificado 119
Configurar reglas de manejo de certificados 120

Integración con la infraestructura de claves públicas 120
Habilitar el soporte de Kerberos Constraint Delegation 121
Administración de dispositivos móviles Exchange ActiveSync 121
Agregar un perfil de administración 122
Eliminación de un perfil de administración 123
Ver la información de un dispositivo EAS 123
Desconectar de la administración un dispositivo EAS 123
Administración de dispositivos móviles con MDM de iOS 124
Agregar un perfil de configuración 124
Instalación de un perfil de configuración en un dispositivo 125
Eliminación de un perfil de configuración de un dispositivo 126
Adición de un perfil de aprovisionamiento 126
Instalación de un perfil de aprovisionamiento en un dispositivo 127
Eliminación de un perfil de aprovisionamiento de un dispositivo 127
Agregar un aplicación administrada 128
Instalar una aplicación en un dispositivo 128
Eliminar una aplicación de un dispositivo 129
Ver la información acerca de un dispositivo con MDM de iOS 130
Desconectar de la administración un dispositivo con MDM de iOS 130
Administración de dispositivos KES 130
Crear un paquete de aplicación móvil para dispositivos KES 130
Ver la información acerca de un dispositivo KES 131
Desconectar de la administración un dispositivo KES 131

SELF SERVICE PORTAL 132
Acerca del Portal de autoservicio 132
Agregar un dispositivo 133
Crear una cuenta para acceder al Portal de autoservicio 133

CARPETA CIFRADO Y PROTECCIÓN DE DATOS 135
Ver la lista de dispositivos cifrados 135
Ver la lista de eventos de cifrado 136
Exportar la lista de eventos de cifrado en un archivo de texto 136
Crear y ver informes de cifrado 137

ADMINISTRACIÓN DEL ACCESO DE LOS DISPOSITIVOS A LA RED DE UNA ORGANIZACIÓN (CONTROL DE ACCESO A LA RED, NAC) 139
Cambio a la configuración de NAC en las propiedades del Agente de red 140
Selección de un modo de operación para el agente NAC 140
Creación de elementos de red 140
Creación de reglas de restricción de acceso a la red 141
Creación de una lista blanca 142
Creación de una lista de direcciones de red permitidas 142
Creación de cuentas para usar en el portal de autorización 142
Configuración de la interfaz de la página de autorización 143
Configuración de NAC en una directiva del Agente de red 143

INVENTARIO DE LOS EQUIPOS DETECTADOS EN LA RED 144
Agregar información sobre los dispositivos nuevos 144
Configurar criterios usados para los dispositivos de empresa 145

ACTUALIZACIÓN DE BASES DE DATOS Y MÓDULOS DE SOFTWARE 146
Creación de la tarea de descarga de actualizaciones en el repositorio 146
Configurar la tarea de descarga de actualizaciones al repositorio 147
Comprobación de actualizaciones descargadas 147
Configurar las directivas de prueba y tareas auxiliares 148
Ver actualizaciones descargadas 149
Distribución automática de las actualizaciones 149
Distribución automática de actualizaciones a equipos cliente 149

Distribución automática de actualizaciones a Servidores de administración secundarios 150
Instalación automática de módulos de programa para Servidores y Agentes de red 150
Creación y configuración de la lista de Agentes de actualización 151
Descarga de actualizaciones a través de Agentes de actualización 151
Revertir las actualizaciones instaladas 152
TRABAJAR CON CLAVES DE APLICACIÓN 153
Visualización de información sobre las claves en uso 153
Agregar una clave al repositorio del Servidor de administración 154
Eliminación de una clave del Servidor de administración 154
Distribución de una clave en equipos cliente 154
Distribución automática de una clave 155
Crear y ver un informe de uso de claves 155
ALMACENAMIENTOS DE DATOS 156
Exportar una lista de objetos de repositorio a un archivo de texto 156
Paquetes de instalación 156
Cuarentena y Copia de seguridad 157
Habilitar la administración remota para archivos en repositorios 157
Visualizar propiedades de un archivo colocado en repositorio 158
Eliminar archivos desde los repositorios 158
Restaurar archivos desde los repositorios 158
Guardar un archivo desde los repositorios al disco 158
Escaneo de archivos en Cuarentena 159
Archivos no procesados 159
Desinfección de archivo aplazada 159
Guardar un archivo no procesado en disco 159
Eliminar archivos desde la carpeta Archivos no procesados 160
KASPERSKY SECURITY NETWORK (KSN) 161
Acerca de KSN 161
Acerca del aprovisionamiento de datos 161
Configuración del acceso a KSN 162
Habilitar y deshabilitar KSN 163
Ver las estadísticas del servidor proxy de KSN 163
CONTACTAR CON EL SERVICIO DE SOPORTE TÉCNICO 164
Acerca del soporte técnico 164
Consultas por teléfono al Servicio de soporte técnico 164
Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico 164
GLOSARIO 166
KASPERSKY LAB ZAO 171
INFORMACIÓN ACERCA DE CÓDIGO DE TERCEROS 172
ACERCA DE LA TECNOLOGÍA NAC/ARP ENFORCEMENT 173
MEJOR PROTECCIÓN CON KASPERSKY SECURITY NETWORK 174
INFORMACIÓN SOBRE LA MARCA REGISTRADA 175
ÍNDICE 176

ACERCA DE ESTE DOCUMENTO

La Guía del administrador de Kaspersky Security Center contiene una introducción; secciones que describen la interfaz, las configuraciones y el mantenimiento de la aplicación; secciones que describen cómo realizar las tareas diarias, y un glosario.

Esta guía proporciona instrucciones sobre cómo configurar y usar Kaspersky Security Center.

Esta Guía también lista las fuentes adicionales de información sobre la aplicación y las distintas formas en que se puede obtener soporte técnico.

EN ESTA SECCIÓN:

En este documento 9

Convenciones del documento 11

EN ESTE DOCUMENTO

La Guía del administrador de Kaspersky Security Center contiene una introducción; secciones que describen la interfaz, las configuraciones y el mantenimiento de la aplicación; secciones que describen cómo realizar las tareas diarias, y un glosario.

Fuentes de información acerca de la aplicación (ver página 12)

Esta sección describe las fuentes de información acerca de la aplicación y enumera los sitios web que puede usar para analizar el funcionamiento de la aplicación.

Kaspersky Security Center (ver página 14)

La sección contiene información sobre el objetivo de Kaspersky Security Center y sobre sus características y componentes principales.

Interfaz de la aplicación (ver página 20)

Esta sección describe las características principales de la interfaz de Kaspersky Security Center.

Licencia de la aplicación

Esta sección proporciona información acerca de los conceptos generales relacionados con la activación de la aplicación. En esta sección se describe el objetivo del Contrato de licencia para usuario final, las formas de activar la aplicación y cómo renovar su licencia.

Asistente de inicio rápido (ver página 38)

Esta sección proporciona información sobre la funcionalidad del Asistente de inicio rápido de Kaspersky Security Center.

Conceptos básicos (ver página 39)

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

Administración de los Servidores de administración (ver página 46)

Esta sección proporciona información sobre cómo manejar los Servidores de administración y cómo configurarlos.

Administración de los grupos de administración (ver página 54)

Esta sección proporciona información sobre cómo manejar grupos de administración.

Administración remota de las aplicaciones (ver página 58)

Esta sección ofrece información sobre cómo realizar la administración remota de las aplicaciones de Kaspersky Lab instaladas en equipos cliente mediante el uso de directivas, perfiles de directivas, tareas y la configuración local de las aplicaciones.

Administración de equipos cliente (ver página 71)

Esta sección proporciona información sobre cómo manejar equipos cliente.

Trabajo con informes, estadísticas y notificaciones (ver página 87)

Esta sección provee información sobre cómo manejar informes, estadísticas y selecciones de eventos y equipos cliente en Kaspersky Security Center y, además, sobre cómo configurar las notificaciones del Servidor de administración.

Equipos no asignados (ver página 95)

Esta sección proporciona información sobre cómo administrar los equipos de una red empresarial si no están incluidos en un grupo de administración.

Administrar aplicaciones en equipos cliente (ver página 100)

Esta sección describe cómo administrar grupos de aplicaciones y cómo actualizar software y reparar vulnerabilidades que Kaspersky Security Center detecta en equipos cliente.

Instalación remota de sistemas operativos y aplicaciones (ver página 110)

Esta sección provee información sobre cómo crear imágenes de sistemas operativos y distribuirlas en los equipos cliente de la red, y también acerca de cómo realizar la instalación remota de las aplicaciones de Kaspersky Lab y de otros proveedores de software.

Administración de dispositivos móviles (ver página 115)

Esta sección describe cómo administrar los dispositivos móviles conectados al Servidor de administración.

Self Service Portal (ver página 132)

Esta sección contiene información acerca del Self Service Portal. La sección proporciona a los usuarios instrucciones para iniciar sesión en el Self Service Portal, así como instrucciones para crear cuentas en el Self Service Portal y agregar dispositivos móviles en el Self Service Portal.

Cifrado y protección de datos (ver página 135)

Esta sección provee información sobre cómo administrar el cifrado de datos almacenados en los discos duros de varios dispositivos y medios extraíbles.

Administración del acceso de los dispositivos a la red de una organización (Control de acceso a la red, NAC) (ver página 139)

Esta sección provee información sobre cómo controlar el acceso de dispositivos a la red de una organización con reglas de restricción de acceso y con la lista blanca de dispositivos.

Inventario de los equipos detectados en la red (ver página 144)

Esta sección provee información sobre el inventario de hardware conectado a la red de la organización.

Actualización de bases de datos y módulos de programa (ver página 146)

Esta sección describe cómo descargar y distribuir las actualizaciones de las bases de datos y los módulos de software con Kaspersky Security Center.

Trabajar con claves de aplicación (ver página 153)

Esta sección describe las características de Kaspersky Security Center relacionadas con el manejo de claves de las aplicaciones administradas de Kaspersky Lab.

Repositorios de datos (ver página 156)

Esta sección proporciona información sobre los datos almacenados en el Servidor de administración que se usan para hacer un seguimiento del estado de los equipos cliente y para darles mantenimiento.

Contactar con el Servicio de soporte técnico

En esta sección se proporciona información acerca de cómo obtener soporte técnico y las condiciones que deben cumplirse para recibir ayuda del Servicio de soporte técnico.

Glosario

Esta sección enumera los términos usados en la guía.

Kaspersky Lab ZAO (ver página 171)

Esta sección proporciona la información acerca de Kaspersky Lab.

Información sobre el uso de códigos de terceros (ver página 172)

Esta sección proporciona información sobre el uso de códigos de terceros en Kaspersky Security Center.

Notificación de la marca comercial (ver página 175)

Esta sección contiene información sobre la marca registrada.

Índice

Esta sección ayuda a encontrar rápidamente los datos que se necesitan.

CONVENCIONES DEL DOCUMENTO

En el presente documento se usan las convenciones correspondientes (consulte la tabla a continuación).

Tabla 1. Convenciones del documento

TEXTO DE EJEMPLO	DESCRIPCIÓN DE CONVENCIONES DEL DOCUMENTO
Tenga en cuenta que...	Las advertencias se resaltan en rojo y con un recuadro. Las advertencias contienen información sobre las acciones que pueden conducir a resultados no deseados.
Recomendamos la utilización de...	Las notas están en recuadros. Las notas contienen información adicional y de referencia.
Por ejemplo: ...	Los ejemplos se exponen con un fondo amarillo y debajo del encabezado “Por ejemplo”.
Actualizar significa... Se produce el evento *Las bases de datos están desactualizadas*.	Los siguientes elementos se muestran 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 mayúscula. Los nombres de teclas conectados por el signo “+” (más) indican el uso de una combinación de teclas. Esas teclas se deben presionar simultáneamente.
Presione el botón **Habilitar**.	Los nombres de los elementos de la interfaz de la aplicación, por ejemplo, campos de entrada, elementos de menú y botones, están destacados en negrita.
➨ *Para configurar la programación de tarea:*	Las frases introductorias de las instrucciones están en cursiva y tienen una flecha.
Escriba `help` en la línea de comandos. Aparece el siguiente mensaje: `Especifique la fecha en el formato dd:mm:aa.`	Los siguientes tipos de contenido del texto están destacados con una fuente especial: • Texto en la línea de comandos. • Texto de mensajes que se muestra en la pantalla a través de la aplicación. • Datos que el usuario debe ingresar con el teclado.
<Nombre de usuario>	Las variables se ponen entre corchetes angulares. En lugar de una variable, se debe insertar el valor correspondiente, sin los corchetes.

FUENTES DE INFORMACIÓN ACERCA DE LA APLICACIÓN

En esta sección, se enumeran las fuentes de información sobre la aplicación.

Podrá seleccionar la fuente de información más adecuada en relación con el nivel de importancia y la urgencia de su problema.

EN ESTA SECCIÓN:

Fuentes de información para investigación independiente 12

Debate sobre las aplicaciones de Kaspersky Lab en el foro 13

FUENTES DE INFORMACIÓN PARA INVESTIGACIÓN INDEPENDIENTE

Puede usar las siguientes fuentes para buscar información acerca de Kaspersky Security Center:

- La página de Kaspersky Security Center en el sitio web de Kaspersky Lab
- La página de Kaspersky Security Center en el sitio web del Servicio de soporte técnico.
- Ayuda en línea.
- Documentación.

Si no puede encontrar una solución para el problema por sus propios medios, le recomendamos comunicarse con el Servicio de soporte técnico de Kaspersky Lab.

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

La página de Kaspersky Security Center en el sitio web de Kaspersky Lab

En la página de Kaspersky Security Center (http://latam.kaspersky.com/productos/productos-para-empresas/administration-kit), puede ver información general acerca de la aplicación, sus funciones y características.

La página de Kaspersky Security Center contiene un enlace a la tienda electrónica. Allí podrá comprar o renovar la aplicación.

Página de Kaspersky Security Center en la Base de conocimientos

La *Base de conocimientos* es una sección en el sitio web del Soporte técnico

En la página de Kaspersky Security Center (http://support.kaspersky.com/sp/ksc10), puede leer 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 Security Center, sino también con otras aplicaciones de Kaspersky Lab. Los artículos de la Base de conocimientos también pueden incluir novedades del Soporte técnico.

Ayuda en línea

La ayuda en línea de la aplicación incluye archivos de ayuda.

La ayuda contextual ofrece información sobre las ventanas de Kaspersky Security Center: Una descripción de la configuración de Kaspersky Security Center está seguida de enlaces a descripciones de las tareas que usan esta configuración.

La ayuda completa proporciona información sobre cómo configurar y usar Kaspersky Security Center.

Documentación

La documentación de la aplicación consta de los archivos de las guías de la aplicación.

La guía del administrador proporciona instrucciones sobre lo siguiente:

- Preparar Kaspersky Security Center para la instalación, e instalar y activar la aplicación.
- Cómo configurar y usar Kaspersky Security Center.

La guía del administrador proporciona información sobre cómo configurar y usar Kaspersky Security Center.

La guía del usuario describe las tareas comunes que los usuarios pueden realizar usando la aplicación, según los permisos disponibles de Kaspersky Security Center.

La guía de instalación describe cómo realizar las siguientes tareas:

- Preparar Kaspersky Security Center para la instalación, e instalar y activar la aplicación.
- Preparar Kaspersky Security Center para su funcionamiento.
- Restaurar o eliminar Kaspersky Security Center.

La guía de distribución describe cómo puede realizar las siguientes tareas:

- Planificar la instalación de Kaspersky Security Center (teniendo en cuenta los principios operativos de Kaspersky Security Center, los requisitos del sistema, las situaciones comunes de distribución y los detalles específicos sobre la integración de Kaspersky Security Center con otras aplicaciones).
- Cómo configurar Kaspersky Security Center después de la instalación.

La guía de implementación proporciona instrucciones sobre lo siguiente:

- Planificar la instalación de Kaspersky Security Center (teniendo en cuenta los principios operativos de Kaspersky Security Center, los requisitos del sistema, las situaciones comunes de distribución y los detalles específicos sobre la integración de Kaspersky Security Center con otras aplicaciones).
- Preparar Kaspersky Security Center para la instalación, e instalar y activar la aplicación.
- Cómo configurar Kaspersky Security Center después de la instalación.

La guía de Primeros pasos proporciona la información necesaria para comenzar a usar la aplicación rápido (una descripción de la interfaz y las tareas principales que se pueden realizar con Kaspersky Security Center).

La guía de ayuda describe las funciones y la configuración de Kaspersky Security Center. Las secciones de la guía de ayuda están ordenadas alfabéticamente y agrupadas por tema.

DEBATE SOBRE LAS APLICACIONES DE KASPERSKY LAB EN EL FORO

Si su pregunta no requiere una respuesta inmediata, puede tratarla con los expertos de Kaspersky Lab y con los otros usuarios de nuestro foro (http://forum.kaspersky.com/index.php?showforum=80).

En este foro, puede ver los temas existentes, dejar comentarios y crear nuevos temas.

KASPERSKY SECURITY CENTER

La sección contiene información sobre el objetivo de Kaspersky Security Center y sobre sus características y componentes principales.

Kaspersky Security Center está diseñado para ejecutar de forma centralizada tareas de administración y mantenimiento básicas en la red de una organización. La aplicación proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red de la organización; permite configurar todos los componentes de protección desarrollados usando las aplicaciones de Kaspersky Lab.

Kaspersky Security Center está dirigido a administradores de redes corporativas y responsables de la protección antivirus en organizaciones.

Al utilizar Kaspersky Security Center, usted podrá:

- Cree una jerarquía de los Servidores de administración para administrar la red de la organización, como también las redes en las oficinas remotas o en las organizaciones cliente.

  La *organización cliente* es una organización cuya protección antivirus está garantizada por un proveedor de servicios.
- Cree una jerarquía de grupos de administración para administrar una selección de equipos cliente como un todo.
- Administre un sistema de protección antivirus desarrollado sobre la base de las aplicaciones de Kaspersky Lab.
- Cree imágenes de los sistemas operativos y distribúyalas en los equipos cliente de la red, como también realice la instalación remota de las aplicaciones de Kaspersky Lab y de otros proveedores de software.
- Realice la administración remota de aplicaciones mediante Kaspersky Lab y otros proveedores instalados en equipos cliente. Instale actualizaciones, busque y repare vulnerabilidades.
- Realice la distribución centralizada de las claves de las aplicaciones de Kaspersky Lab en equipos cliente, supervise su uso y renueve las licencias.
- Reciba estadísticas e informes sobre el funcionamiento de las aplicaciones y dispositivos.
- Recibir notificaciones sobre eventos críticos en la operación de aplicaciones de Kaspersky Lab.
- Controle el acceso de los dispositivos a la red de una organización mediante reglas de restricción de acceso y una lista blanca de dispositivos. Los agentes NAC se usan para administrar el acceso de los dispositivos a la red de una organización.
- Administre dispositivos móviles que sean compatibles con los protocolos Exchange ActiveSync® o de administración de dispositivos móviles de iOS (MDM de iOS).
- Administre el cifrado de la información almacenada en los discos duros de los dispositivos y medios extraíbles y el acceso de los usuarios a los datos cifrados.
- Realice el inventario del hardware conectado a la red de la organización.
- Administre de forma centralizada los archivos llevados a Cuarentena o Copia de seguridad por las aplicaciones antivirus, y los objetos para los cuales se haya aplazado el procesamiento de parte de las aplicaciones antivirus.

EN ESTA SECCIÓN:

Novedades 15

Kit de distribución 16

Requisitos de hardware y software 17

NOVEDADES

Cambios introducidos en Kaspersky Security Center 10 en comparación con la versión anterior:

- Se ha agregado la nueva función de administración de roles de usuarios. (consulte la sección "Configuración de derechos. Roles de los usuarios" en la página 84)
- Ahora es posible agregar usuarios internos para administrar Servidores de administración virtuales.
- Ahora es posible programar el escaneo de red.
- Ahora puede configurarse la KSN privada. (consulte la sección "Configuración del acceso a KSN" en la página 162)
- Se inició Self Service Portal, que permite a los usuarios tomar el control de algunas de las operaciones de administración de dispositivos móviles. (consulte la sección "Self Service Portal" en la página 132)
- Se ha implementado la característica de exportación de eventos a sistemas SIEM (consulte la sección "Exportando eventos a un sistema SIEM" en la página 91).
- Ahora es posible cambiar la ruta a la carpeta para guardar actualizaciones y revisiones descargadas o actualizaciones y revisiones a la espera de ser descargadas.
- Ahora es posible eliminar actualizaciones descargadas.
- Ahora es posible enviar reparaciones de vulnerabilidades a equipos cliente sin instalar las actualizaciones.
- Las actualizaciones del Servidor de administración pueden administrarse desde la interfaz de la aplicación.
- Ahora es posible seleccionar un agente de actualización para equipos cliente basado en un análisis de red.
- Ahora es posible ver información acerca de la distribución de vulnerabilidades en los equipos administrados.
- Ahora es posible enrutar el tráfico desde dispositivos móviles KES fuera de la red corporativa, a través de una puerta de enlace de conexión en una zona desmilitarizada (DMZ).
- Ahora es posible administrar los dispositivos móviles con comandos remotos.
- Ahora es posible establecer Google Cloud Messaging para intercambiar notificaciones push entre los dispositivos KES y el Servidor de Administración.
- Se ha agregado la función de captura e implementación de imágenes de sistema operativo (ver la página 110).
- Se implementó la opción de instalación remota centralizada de aplicaciones de otros fabricantes (ver la página 114).
- Se implementó la característica de instalación remota centralizada de actualizaciones para sistemas operativos y aplicaciones (ver la página 106).
- Se ha integrado la función Windows Server® Update Services al Servidor de administración (ver la página 106).
- Se ha agregado la función de control de restricciones de licencia; se ha ampliado el alcance operativo del registro de aplicaciones (ver la página 100).
- Se agregó la funcionalidad de administración de registro de hardware (ver la página 144).
- Se ha implementado la opción de Control de acceso a la red para dispositivos que intentan acceder a la red de la organización, mediante la aplicación de reglas y una lista blanca de dispositivos (ver la página 139).
- Se ha agregado la opción de acceso compartido al escritorio de un equipo cliente; se ha ampliado el alcance operativo del escritorio remoto.
- Se implementó el servidor de dispositivos móviles Exchange ActiveSync (ver la página 121).
- Se implementó el servidor de dispositivos móviles con MDM de iOS (ver la página 124).
- Se implementó la característica de envío de mensajes SMS a usuarios de dispositivos móviles (ver la página 83).
- Se implementó la funcionalidad de instalación remota centralizada de aplicaciones en dispositivos móviles administrados.
- Se implementó la funcionalidad de instalación centralizada de certificados en dispositivos móviles administrados.

- Se ha agregado la compatibilidad de la función de administración de cifrado de datos para Kaspersky Endpoint Security 10 para Windows® (ver la página 135).
- Se expandieron las opciones de Control de aplicaciones. Se agregaron las siguientes características: análisis estático de reglas de control de aplicaciones, creación de categorías basadas en un conjunto de archivos ejecutables en equipos de referencia, visualización de varias categorías para un único archivo ejecutable (ver la página 100).
- Se implementó la característica de publicación de paquetes independientes aleatorios en un servidor web integrado en el Servidor de administración (ver la página 114).
- Se incluyó una selección de agentes de actualización en el conjunto de selecciones creadas de forma predeterminada.
- Se agregó un panel de información que muestra el estado de los agentes de actualización.
- Se ha implementado la opción de filtrado de listas de archivos centralizadas en Cuarentena y Copia de seguridad, así como archivos con procesamiento pospuesto.
- Se agregó la funcionalidad de administración de la lista centralizada de usuarios (ver la página 83).
- Se agregó la característica de excluir de la búsqueda las subdivisiones seleccionadas por medio de Active Directory.
- Se agregó la característica de planificación del inicio de una tarea para un día seleccionado del mes.
- Se implementó la configuración automática de demora de inicio de tareas.
- Se implementó el uso de negación en los criterios de búsqueda para equipos específicos.
- Se implementó la característica de especificación de una base de datos vacía y existente como la base de datos del Servidor de administración durante la instalación.
- Se agregó la característica de especificación de grupos como criterios de búsqueda para equipos específicos.
- Se agregó la opción de especificar un tipo de objetos distribuidos en la configuración de un agente de actualización, ya sea que estos sean paquetes de instalación, actualizaciones, o ambos tipos (ver la página 151).
- Se agregó la característica de búsqueda de equipos por nombres de usuario o nombres de sesión. También se agregaron informes sobre usuarios de equipos.
- Se implementó una utilidad gráfica para la administración de Servidores de administración.
- Se agregó visualización individual de la fecha de vencimiento de la licencia y la fecha de finalización del término de validez a las propiedades de la clave y al informe de uso de las claves.
- Se agregó una visualización de información sobre el volumen total de datos almacenados en la base de datos del Servidor de administración y sobre el volumen de eventos almacenados en la base de datos.
- Se agregó la característica de especificación de criterios con el operador “or” en reglas de migración de equipos a grupos de administración.

KIT DE DISTRIBUCIÓN

Puede comprar la aplicación a través de las tiendas en línea de Kaspersky Lab (por ejemplo, http://latam.kaspersky.com, la sección **eStore**) o compañías asociadas.

Si compra Kaspersky Security Center a través de una tienda en línea, copiará la aplicación desde el sitio web de la tienda. La información requerida para la activación de la aplicación se envía por correo electrónico después del pago.

Para obtener más detalles sobre los métodos de compra y el kit de distribución, comuníquese con el Departamento comercial.

REQUISITOS DE HARDWARE Y SOFTWARE

Kaspersky Security Center cuenta con los siguientes requisitos de hardware y software

Tabla 2. Requisitos de software para el Servidor de administración y Kaspersky Security Center Web Console

COMPONENTE	REQUISITOS
Sistema operativo	Microsoft® Windows XP Professional con Service Pack 2 o superior instalado; Microsoft Windows XP Professional x64 o superior; Microsoft Windows Vista® Business/Enterprise/Ultimate Service Pack 1 o superior; Microsoft Windows Vista Business/Enterprise/Ultimate x64 Service Pack 1 o superior; Microsoft Windows 7 Professional/Enterprise/Ultimate; Microsoft Windows 7 Professional/Enterprise/Ultimate x64; Microsoft Windows 8 (todas las ediciones); Microsoft Windows 8 x64 (todas las ediciones); Microsoft Windows Small Business Server 2003; Microsoft Windows Small Business Server 2008; Microsoft Windows Small Business Server 2011; Microsoft Windows Server 2003 o superior; Microsoft Windows Server 2003 x64 o superior; Microsoft Windows Server 2008; Microsoft Windows Server 2008 distribuido en el modo Server Core; Microsoft Windows Server 2008 x64 Service Pack 1 o superior; Microsoft Windows Server 2008 x64 implementado en el modo Server Core; Microsoft Windows Server 2008 R2; Microsoft Windows Server 2008 R2 implementado en el modo Server Core; Microsoft Windows Server 2012 (todas las ediciones); Microsoft Windows Server 2012 distribuido en el modo Server Core.
Componentes de acceso a datos	Componentes de Microsoft Data Access (MDAC) 2.8 o superior Microsoft Windows DAC 6.0.
Sistema de administración de bases de datos	Microsoft SQL Server® Express 2005, Microsoft SQL Server Express 2008, Microsoft SQL Server Express 2008 R2, Microsoft SQL Server Express 2008 R2 Service Pack 2, Microsoft SQL Server Express 2012. Microsoft SQL Server 2005, Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012; MySQL Enterprise versiones 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091; MySQL Enterprise versiones 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90.
Servidor web	Apache HTTP Server versión 2.2.0 o superior (se recomienda la versión 2.2.23).

Tabla 3. Requisitos de hardware para el Servidor de administración y Kaspersky Security Center Web Console

SISTEMA OPERATIVO	FRECUENCIA DE CPU, GHZ	TAMAÑO DE RAM, GB	ESPACIO EN DISCO DISPONIBLE, GB
Microsoft Windows, 32-bit	1 o superior	4	10
Microsoft Windows, 64-bit	1.4 o superior	4	10

Consola de administración

Tabla 4. Requisitos de software para la Consola de administración

COMPONENTE	REQUISITOS
Sistema operativo	Microsoft Windows (la versión compatible del sistema operativo se determina según los requisitos del Servidor de administración).
Consola de administración	Microsoft Management Console versión 2.0 o superior.
Navegador	Microsoft Internet Explorer® 7.0 o superior al trabajar con Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2 o Microsoft Windows Vista Microsoft Internet Explorer 8.0 o superior al trabajar con Microsoft Windows 7 Microsoft Internet Explorer 10.0 o superior al trabajar con Microsoft Windows 8.

Tabla 5. Requisitos de hardware para la Consola de administración

SISTEMA OPERATIVO	FRECUENCIA DE CPU, GHZ	TAMAÑO DE RAM, MB	ESPACIO EN DISCO DISPONIBLE, GB
Microsoft Windows, 32-bit	1 o superior	512	1
Microsoft Windows, 64-bit	1.4 o superior	512	1

Al usar la Administración del sistema, se deberá contar con un espacio libre en disco de 100 GB.

Servidor de dispositivos móviles para la administración de dispositivos móviles de iOS

Tabla 6. Requisitos de software para el Servidor de dispositivos móviles con MDM de iOS

COMPONENTE	REQUISITOS
Sistema operativo	Microsoft Windows (la versión compatible del sistema operativo se determina según los requisitos del Servidor de administración).

Tabla 7. Requisitos de hardware para el Servidor de dispositivos móviles con MDM de iOS

SISTEMA OPERATIVO	FRECUENCIA DE CPU, GHZ	TAMAÑO DE RAM, GB	ESPACIO EN DISCO DISPONIBLE, GB
Microsoft Windows, 32-bit	1 o superior	2	2
Microsoft Windows, 64-bit	1.4 o superior	2	2

Servidor de dispositivos móviles Exchange ActiveSync

Todos los requisitos de software y hardware para el servidor de dispositivos móviles Exchange ActiveSync están incluidos en los requisitos para Microsoft Exchange Server.

Colaboración con Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 y Microsoft Exchange Server 2013 admitido.

Agente de red o Agente de actualización instalado

Tabla 8. Requisitos de software para el Agente de red y el Agente de actualizaciones

COMPONENTE	REQUISITOS
Sistema operativo	Microsoft Windows Linux® Mac OS

La versión del sistema operativo admitido se define por medio de los requisitos de las aplicaciones que se pueden administrar con Kaspersky Security Center.

Tabla 9. Requisitos de hardware para el Agente de red y el Agente de actualización

SISTEMA OPERATIVO	FRECUENCIA DE CPU, GHZ	TAMAÑO DE RAM, GB	ESPACIO LIBRE EN DISCO DISPONIBLE PARA EL AGENTE DE ADMINISTRACIÓN, GB	ESPACIO LIBRE EN DISCO DISPONIBLE PARA EL AGENTE DE ACTUALIZACIÓN, GB
Microsoft Windows, 32-bit	1 o superior	0.5	1	4
Microsoft Windows, 64-bit	1.4 o superior	0.5	1	4
Linux, 32 bits	1 o superior	1	1	4
Linux, 64 bits	1.4 o superior	1	1	4
Mac OS	1	1	1	4

Para la instalación simultánea del Agente de red y Kaspersky Endpoint Security, el espacio libre en disco debe ser de 2 GB como mínimo.

Puede recuperar los detalles de la versión más reciente de los requisitos de hardware y software del sitio web del Servicio de soporte técnico, en la página del Kaspersky Security Center 10, en la sección Requisitos del sistema.

INTERFAZ DE LA APLICACIÓN

Esta sección describe las características principales de la interfaz de Kaspersky Security Center.

La visualización, creación, modificación y configuración de los grupos de administración, y la administración centralizada de las aplicaciones de Kaspersky Lab instaladas en los dispositivos cliente se realizan desde la estación de trabajo del administrador. La interfaz de administración es proporcionada por el componente Consola de administración. Es un complemento especializado independiente integrado con Microsoft Management Console (MMC), de modo que la interfaz Kaspersky Security Center es estándar para MMC.

La Consola de administración permite la conexión remota al Servidor de administración a través de Internet.

Para el trabajo local con equipos cliente, la aplicación admite la conexión remota a un equipo a través de la Consola de administración, utilizando la aplicación estándar de Conexión a Escritorio remoto de Microsoft Windows Remote.

Para utilizar esta funcionalidad, debe autorizar la conexión remota al escritorio en el equipo cliente.

EN ESTA SECCIÓN:

Ventana principal de la aplicación 20

Árbol de consola 22

Espacio de trabajo 24

Bloque de filtrado de datos 29

Menú contextual 31

Configuración de la interfaz 31

VENTANA PRINCIPAL DE LA APLICACIÓN

La ventana principal de la aplicación (ver la figura siguiente) contiene un menú, una barra de herramientas, un panel de descripción y un espacio de trabajo.

La barra del menú permite utilizar las ventanas y proporciona el acceso al sistema de Ayuda. El menú **Acción** duplica los comandos del menú contextual para el objeto del árbol de consola actual.

El árbol de consola muestra el espacio de nombres de **Kaspersky Security Center** en una vista de árbol (consulte la sección “Árbol de consola” en la página 22).

El conjunto de los botones de la barra de herramientas permite acceder directamente a algunos elementos del menú. El conjunto de botones de la barra de herramientas cambia en función del nodo actual o de la carpeta seleccionada en el árbol de consola.

La apariencia del espacio de trabajo de la ventana principal de la aplicación depende de con cuál nodo (carpeta) del árbol de consola se relaciona el área y cuál es su función.

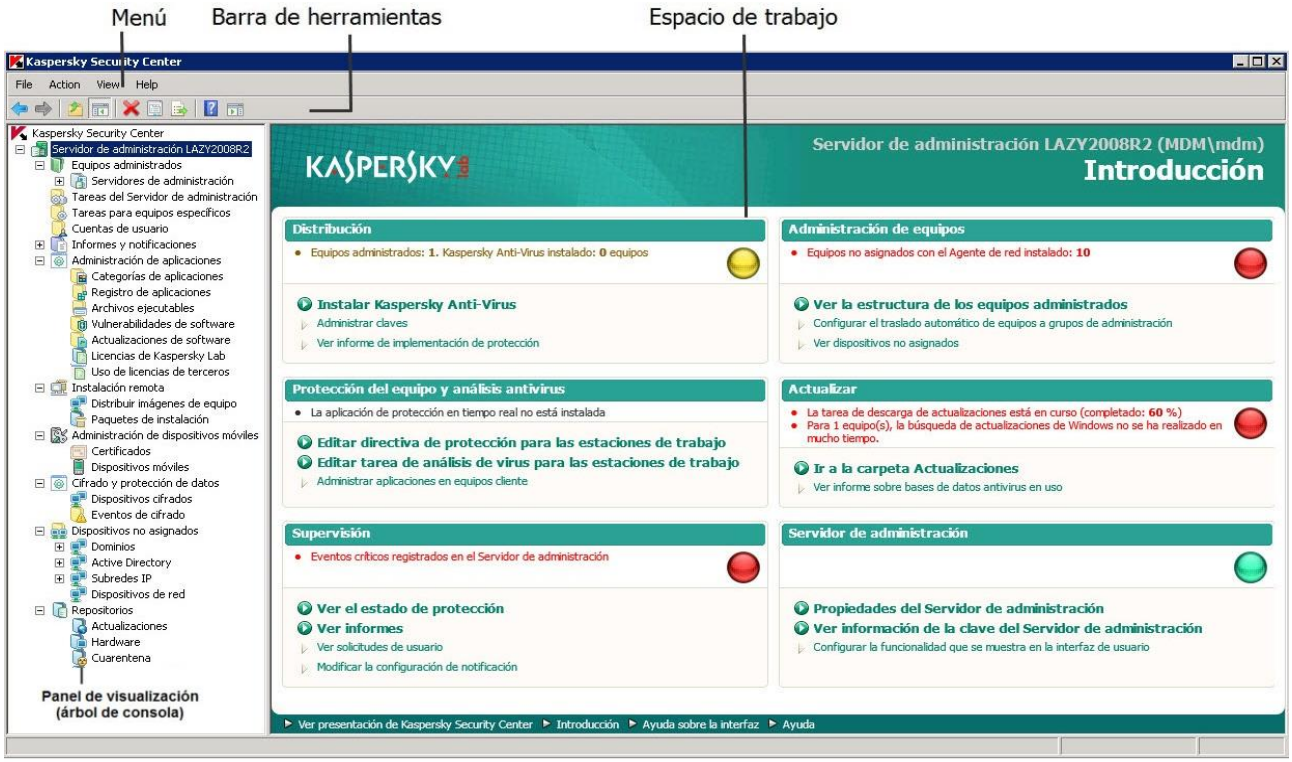


Figura 1. Ventana principal de la aplicación Kaspersky Security Center

ÁRBOL DE CONSOLA

El árbol de consola (ver la figura siguiente) está diseñado para mostrar la jerarquía de los Servidores de administración de la red corporativa, la estructura de sus grupos de administración y otros objetos de la aplicación, como las carpetas **Repositorios** o **Informes y notificaciones**. El espacio de nombres de Kaspersky Security Center puede contener varios nodos incluyendo los nombres de los servidores correspondientes a los Servidores de administración incluidos en la jerarquía.

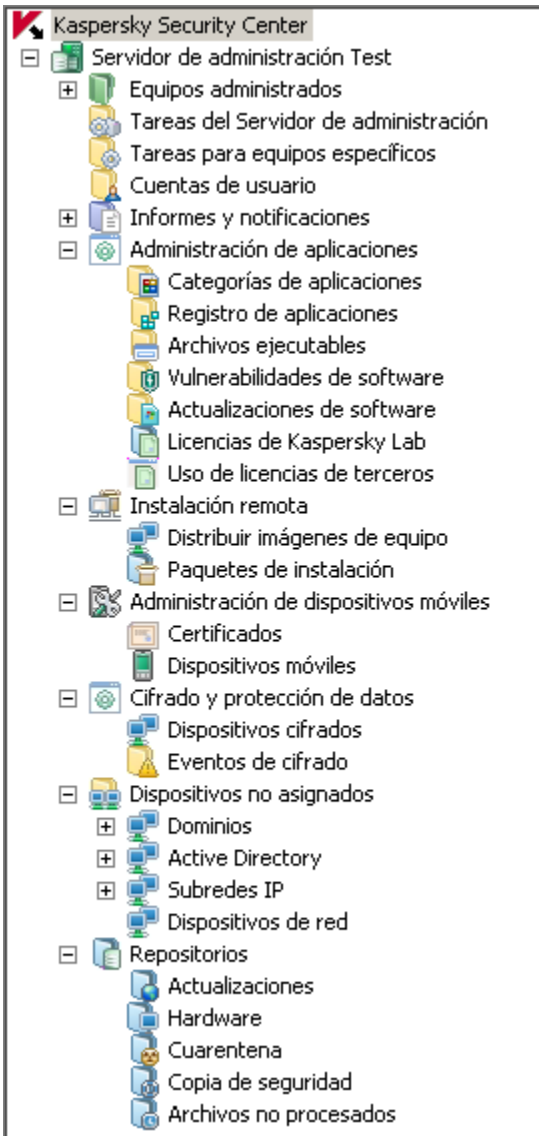


Figura 2. Árbol de consola

El nodo **Servidor de administración - <Nombre del equipo>** es un contenedor que muestra la organización estructural del Servidor de administración seleccionado. El contenedor **Servidor de administración – <Nombre del equipo>** incluye las siguientes carpetas:

- **Equipos administrados**
- **Cuentas de usuario**
- **Informes y notificaciones**
- **Tareas del Servidor de administración**.
- **Tareas para equipos específicos**.
- **Administración de las aplicaciones**.
- **Instalación remota**

- **Administración de dispositivos móviles**.
- **Cifrado y protección de datos**
- **Equipos no asignados**
- **Repositorios**

La carpeta **Equipos administrados** está diseñada para almacenar, mostrar, configurar y modificar la estructura de los grupos de administración, directivas de grupo y tareas de grupo.

La carpeta **Cuentas de usuario** contiene información de las cuentas de usuario de la red.

La carpeta **Informes y notificaciones** contiene un conjunto de plantillas para la generación de informes acerca del estado del sistema de protección en los equipos cliente de los grupos de administración. La carpeta **Informes y notificaciones** contiene las siguientes subcarpetas:

- **Selecciones de equipos**. Diseñada para buscar equipos cliente de acuerdo con criterios especificados.
- **Eventos**. Contiene selecciones de eventos que presentan información sobre eventos de la aplicación y resultados de las tareas ejecutadas.

La carpeta **Tareas del Servidor de administración** contiene un conjunto de tareas definidas para el Servidor de administración.

La carpeta **Tareas para equipos específicos** contiene tareas definidas para un conjunto de equipos de grupos de administración o en la carpeta **Equipos no asignados**. Estas tareas son convenientes para grupos pequeños de equipos cliente que no pueden combinarse en un grupo de administración separado.

La carpeta **Administración de aplicaciones** está diseñada para administrar las aplicaciones instaladas en los equipos de la red. Contiene las siguientes subcarpetas:

- **Categorías de aplicaciones**. Diseñada para manejar categorías de usuario de las aplicaciones.
- **Registro de aplicaciones**. Contiene la lista de aplicaciones instaladas en equipos cliente en los que se encuentra instalado el Agente de red.
- **Archivos ejecutables**. Contiene la lista de archivos ejecutables almacenados en equipos cliente en los que se encuentra instalado el Agente de red.
- **Vulnerabilidades de software**. Contiene la lista de vulnerabilidades de aplicaciones de equipos cliente en los que se encuentra instalado el Agente de red.
- **Actualizaciones de software**. Contiene la lista de actualizaciones descargadas por el Servidor de administración que se pueden distribuir a los equipos cliente.
- **Licencias de Kaspersky Lab**. Contiene una lista de las claves de los equipos cliente.
- **Uso de licencias de terceros**. Contiene una lista de grupos de aplicaciones con licencia.

La carpeta **Instalación remota** está diseñada para administrar la instalación remota de sistemas operativos y aplicaciones. Incluye las siguientes subcarpetas:

- **Distribución de imágenes de equipo** Está diseñada para distribuir imágenes de sistemas operativos en equipos cliente.
- **Paquetes de instalación**. Contiene una lista de los paquetes de instalación que se pueden utilizar para la instalación remota de aplicaciones en equipos cliente.

La carpeta **Dispositivos móviles** está diseñada para administrar los dispositivos móviles de Exchange ActiveSync y con MDM de iOS.

La carpeta **Cifrado y protección de datos** está diseñada para administrar el proceso de cifrado de datos del usuario en discos y medios extraíbles.

La carpeta **Equipos no asignados** muestra la red donde está instalado el Servidor de administración. La información sobre la estructura de la red y los equipos en la misma es recibida por el Servidor de administración mediante sondeos regulares de la red de Windows, subredes IP y Active Directory dentro de la red corporativa de equipos. Los resultados del sondeo se muestran en las áreas de información de las correspondientes carpetas: **Dominios**, **Subredes IP** y **Active Directory**.

La carpeta **Repositorios** está diseñada para las operaciones con objetos utilizados para controlar el estado de los equipos cliente y llevar a cabo su mantenimiento. Incluye las siguientes carpetas:

- **Actualizaciones**. Contiene una lista de actualizaciones recibidas por el Servidor de administración que se pueden distribuir a los equipos cliente.
- **Hardware**. Contiene una lista del hardware conectado a la red de la organización.
- **Cuarentena**. Contiene una lista de objetos colocados en Cuarentena por el software antivirus en equipos cliente.
- **Copia de seguridad**. Contiene la lista de copias de seguridad de los objetos que están en almacenamiento.
- **Archivos no procesados**. Contiene una lista de los archivos asignados para escaneo posterior por las aplicaciones antivirus.

ESPACIO DE TRABAJO

El *espacio de trabajo* es un área de la ventana principal de la aplicación de Kaspersky Security Center ubicada a la derecha del árbol de consola (ver la siguiente figura). Contiene descripciones de los objetos del árbol de consola y sus funciones respectivas. El contenido del espacio de trabajo corresponde al objeto seleccionado del árbol de consola.

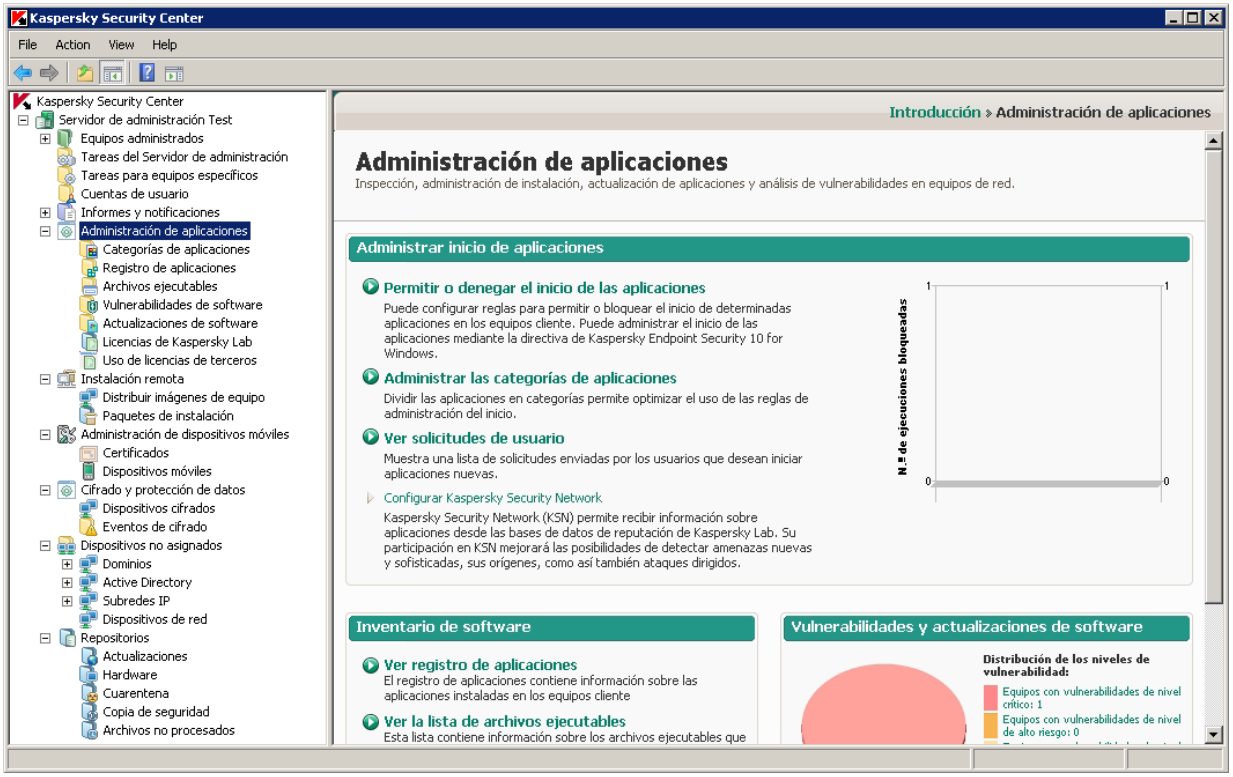


Figura 3. Espacio de trabajo

La apariencia del espacio de trabajo para varios objetos del árbol de consola depende del tipo de datos visualizados. Existen tres apariencias del espacio de trabajo:

- conjunto de casillas de administración;
- lista de objetos de administración;
- conjunto de paneles de información.

Si el árbol de consola no muestra algunos de los elementos dentro del un objeto del árbol de consola, el espacio de trabajo se divide en pestañas. Cada pestaña corresponde a un elemento del árbol de consola (ver la siguiente figura).

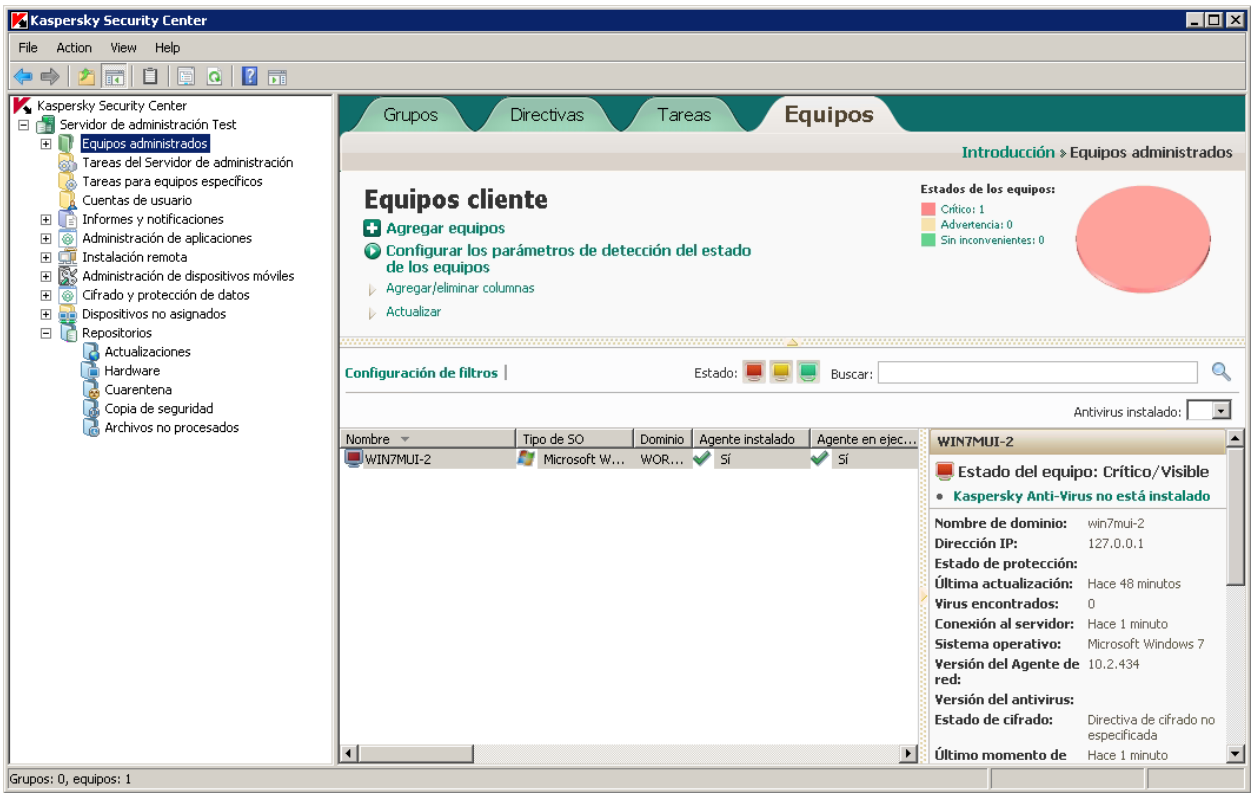


Figura 4. Espacio de trabajo dividido en pestañas

EN ESTA SECCIÓN:

Conjunto de bloques de administración 26
Lista de objetos de administración 26
Conjunto de bloques de información 28

CONJUNTO DE BLOQUES DE ADMINISTRACIÓN

En el espacio de trabajo representado como un conjunto de *bloques de administración*, las tareas de administración están divididas en bloques. Cada bloque de administración contiene un conjunto de vínculos, cada uno de los cuales corresponde a una tarea de administración (ver la siguiente figura).

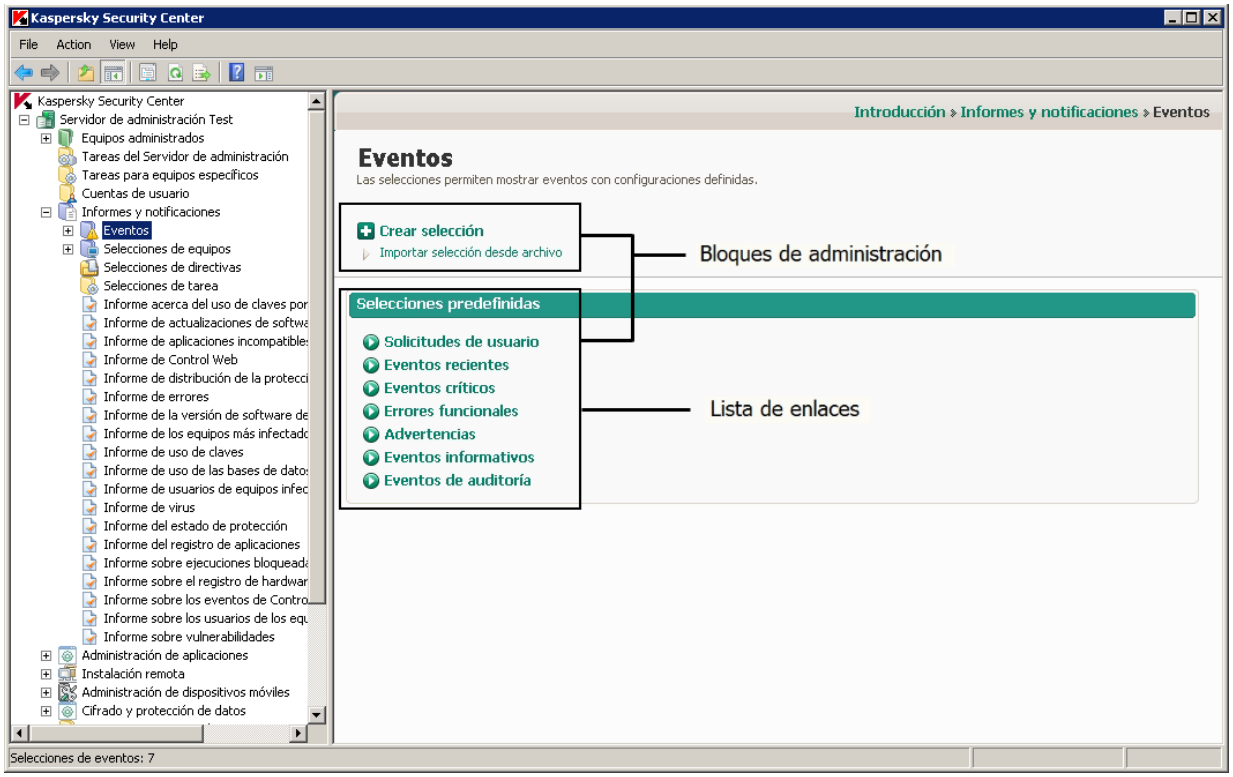


Figura 5. Espacio de trabajo representado como un conjunto de bloques de administración

LISTA DE OBJETOS DE ADMINISTRACIÓN

El espacio de trabajo representado como una lista de objetos de administración incluye cuatro áreas (ver la siguiente figura):

- Bloque de administración de la lista de objetos.
- Lista de objetos.

- Bloque de objeto seleccionado (opcional).
- Bloque de filtrado de datos (opcional).

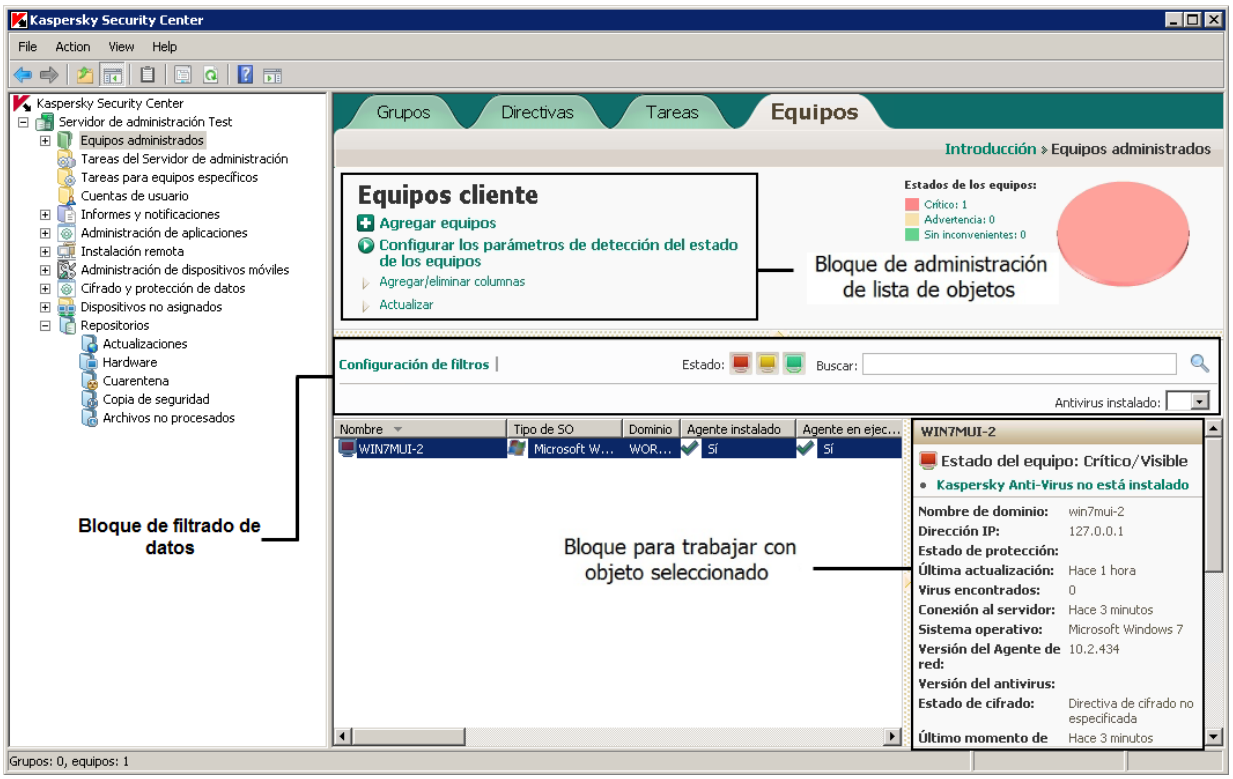


Figura 6. Área de información representada como una lista de objetos de administración

El bloque de administración de la lista de objetos contiene el encabezado de la lista y un conjunto de vínculos, cada uno de los cuales corresponde a una lista de tareas de administración.

La lista de objetos se muestra en una tabla. El conjunto de columnas de la tabla puede cambiarse mediante un menú contextual.

El bloque de objetos seleccionados contiene información detallada acerca de un objeto y un conjunto de enlaces diseñado para ejecutar tareas principales de la administración de objetos.

El bloque de filtrado de datos le permite crear ejemplos de objetos de la lista (consulte la sección “Bloque de filtrado de datos” en la página 29).

CONJUNTO DE BLOQUES DE INFORMACIÓN

Los datos de información se muestran en el espacio de trabajo como *paneles de información* sin controles (ver la siguiente figura).

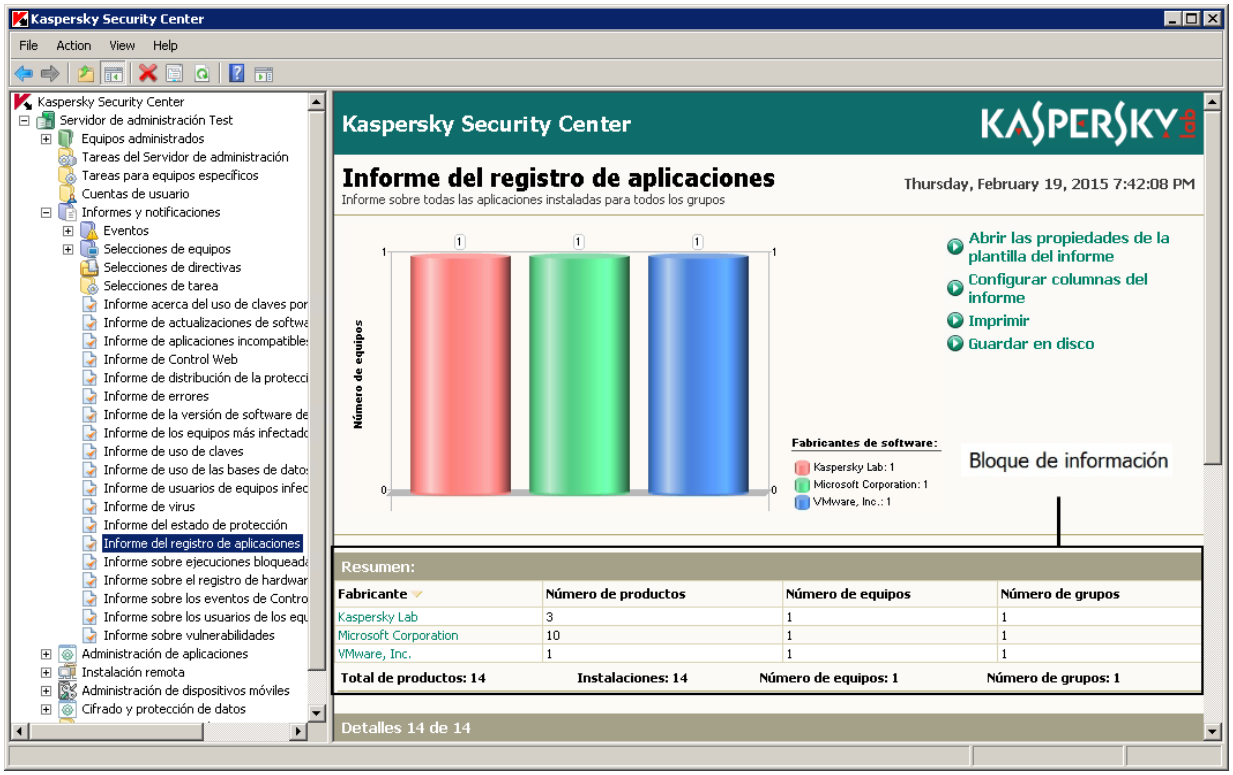


Figura 7. Espacio de trabajo representado como un conjunto de paneles de información

Los paneles informativos pueden representarse en varias páginas (ver la siguiente figura).

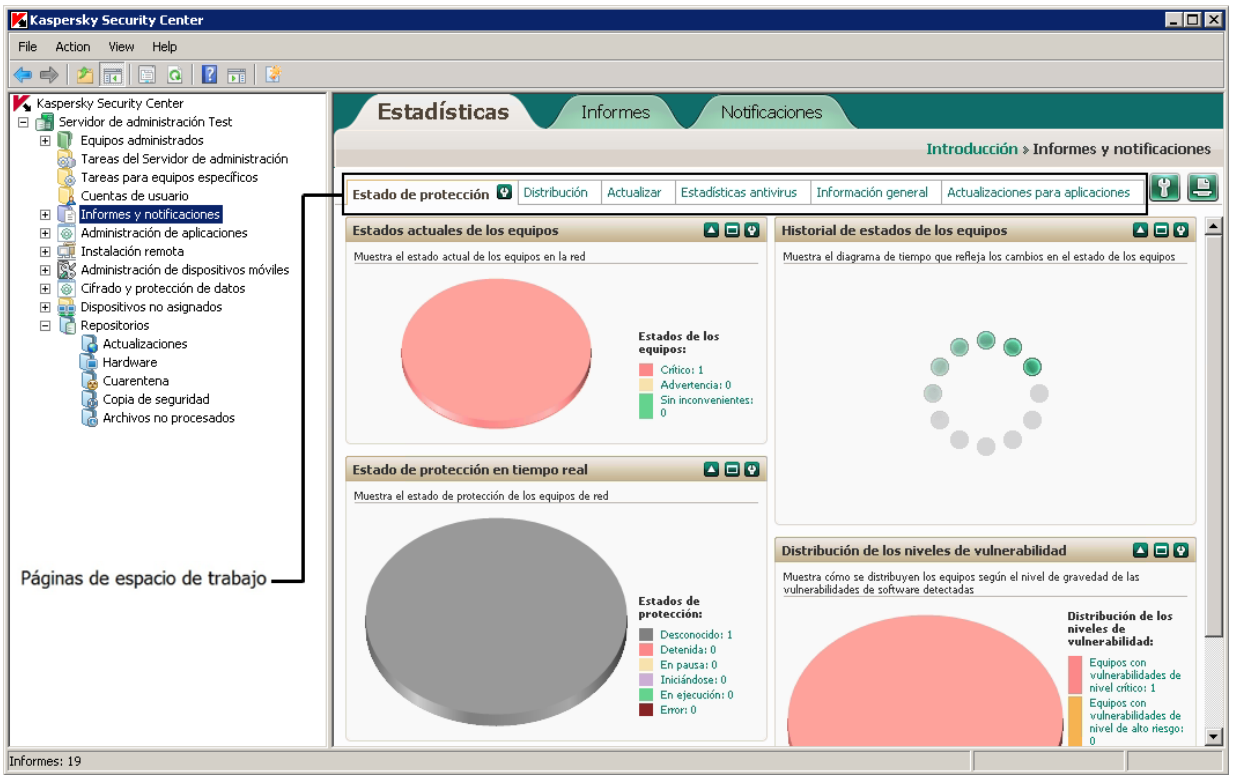
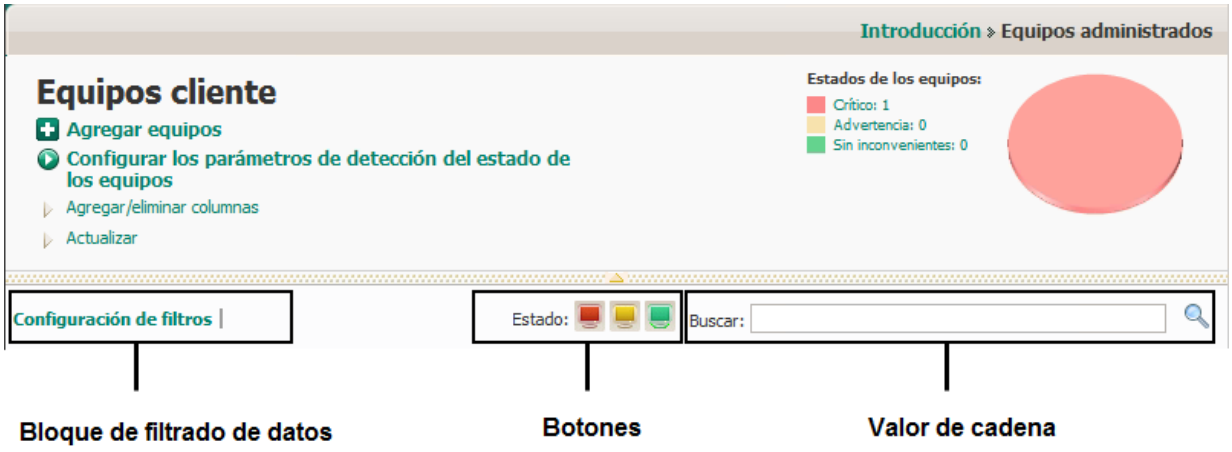


Figura 8. Espacio de trabajo dividido en páginas

BLOQUE DE FILTRADO DE DATOS

El *Bloque de filtrado de datos* (en adelante también denominado *bloque de filtrado*) se encuentra en espacios de trabajo y secciones de cuadros de diálogo que contienen listas de objetos (como equipos, aplicaciones, vulnerabilidades o usuarios).

El bloque de filtrado puede contener un campo de búsqueda, un filtro y botones (vea la siguiente figura).



Campo Búsqueda

El campo de búsqueda se usa para buscar en la lista el texto que se ingresa en él.

Use las siguientes expresiones comunes en el campo de búsqueda para buscar texto:

- *. Reemplaza cualquier secuencia de carácteres.

Por ejemplo:

Para buscar las palabras **Servidor**, **Servidores** o **Sala de servidores**, ingrese la expresión **Servidor*** en el campo de búsqueda.

- ?. Reemplaza cualquier carácter individual.

Por ejemplo:

Para buscar las palabras **Casa** o **Capa**, ingrese la expresión **Ca?a** en el campo de búsqueda.

- [<rango>]. Reemplaza cualquier carácter individual dentro del rango o conjunto especificado.

Por ejemplo:

Para buscar cualquier dígito, ingrese la expresión **[0-9]** en el campo de búsqueda.

Para buscar uno de los caracteres (**a**, **b**, **c**, **d**, **e** o **f**), ingrese la expresión **[abcdef]** en el campo de búsqueda.

La búsqueda de texto completo está disponible en los siguientes bloques de filtrado:

- En el bloque de filtrado de la lista de eventos, en las columnas **Evento** y **Descripción**.
- En el bloque de filtrado de cuentas de usuarios, en la columna **Nombre**.
- En el bloque de filtrado de registro de aplicaciones, en la columna **Nombre** si la casilla **Agrupar aplicaciones por nombre** está desactivada.

Use las siguientes expresiones comunes en el campo de búsqueda para realizar una búsqueda de texto completo:

- Espacio. Verá todos los equipos cuyas descripciones contengan alguna de las palabras enumeradas.

Por ejemplo:

Para buscar una frase que contenga la palabra **Esclavo** o **Virtual** (o ambas), ingrese la expresión **Esclavo virtual** en el campo de búsqueda.

- **+,** AND o &&. Cuando un signo más precede una palabra, todos los resultados de la búsqueda contendrán esta palabra.

Por ejemplo:

Para buscar una frase que contenga la palabra **Esclavo** y la palabra **Virtual**, ingrese una de las siguientes expresiones en el campo de búsqueda: **+Esclavo+Virtual**, **Esclavo AND Virtual**, **Esclavo && Virtual**.

- OR o ||. Cuando se colocan entre dos palabras, indican que se puede encontrar una palabra o la otra en el texto.

Por ejemplo:

Para buscar una frase que contenga la palabra **Esclavo** o la palabra **Virtual**, ingrese una de las siguientes expresiones en el campo de búsqueda: **Esclavo OR Virtual**, **Esclavo || Virtual**.

- **-**. Cuando un signo menos precede una palabra, ningún resultado de la búsqueda contendrá esta palabra.

Por ejemplo:

Para buscar una frase que deba contener la palabra **Esclavo** y no deba contener la palabra **Virtual**, ingrese la expresión **+Esclavo-Virtual** en el campo de búsqueda.

- **"<un texto>"**. El texto que se introduce entre comillas debe estar presente en el texto.

Por ejemplo:

Para buscar una frase que contenga la combinación de palabras **Servidor esclavo**, ingrese la expresión "**Servidor esclavo**" en el campo de búsqueda.

- ?. Reemplaza cualquier carácter individual.

Por ejemplo:

Para buscar las palabras **Casa** o **Capa**, ingrese la expresión **Ca?a** en el campo de búsqueda.

> El texto en el campo de búsqueda no puede empezar con el símbolo ?.

- *. Reemplaza cualquier secuencia de carácteres.

Por ejemplo:

Para buscar las palabras **Servidor**, **Servidores** o **Sala de servidores**, ingrese la expresión **Servidor*** en el campo de búsqueda.

> El texto en el campo de búsqueda no puede empezar con el símbolo *.

Botones del bloque de filtrado

Los botones del bloque de filtrado tienen forma de iconos multicolores sobre un fondo más oscuro.

Al hacer clic en un botón, el fondo se pone más brillante. Luego, al hacer clic en el botón una vez más, el fondo vuelve a quedar oscuro.

Se aplican las siguientes reglas de filtrado:

- Un elemento de la lista con el valor de un atributo especificado se considera seleccionado si el icono con el valor del atributo se muestra en un fondo oscuro del bloque de filtrado (por ejemplo:  – La selección incluirá los equipos con el estado *Crítico*.
- Un elemento de la lista con el valor de un atributo especificado se considera no seleccionado si el icono con el valor del atributo se muestra en un fondo claro del bloque de filtrado (por ejemplo:  – La selección no incluirá los equipos con el estado *Crítico*.
- La selección incluye todos los elementos de la lista si los iconos de todos los valores del atributo están colocados en el fondo más claro (como ) o en el fondo más oscuro (como ).

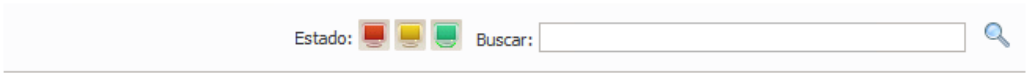
Los valores de los atributos dependen de los estados de los equipos (o dispositivos de red) y de los niveles de gravedad de los eventos. Una lista de estados de equipos, dispositivos de red y niveles de gravedad de eventos (con sus iconos correspondientes) se proporciona en el apéndice.

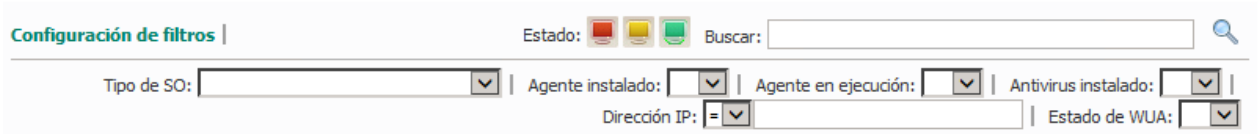
Bloque de filtrado extendido

Al usar un bloque de filtrado, puede crear selecciones de datos y restablecer el filtrado; también puede habilitar el formato extendido del bloque mediante la inclusión de la configuración de filtrado adicional (vea la siguiente figura).

- Crear una selección:
  - Si usa solamente botones para crear una selección, esta se crea automáticamente después de que hace clic en un botón.
  - Si usa una configuración de búsqueda de texto y selección (por ejemplo, en el bloque de filtrado extendido) además de los botones, la selección se crea cuando hace clic en el botón  , en la esquina superior derecha del bloque de filtrado.
- Restablecimiento del filtro:

  Puede restablecer el filtro haciendo clic en el botón  que aparece a la izquierda del botón  después de haber usado el bloque de filtrado por primera vez.





- Uso del bloque de filtrado extendido: Puede expandir el bloque de filtrado extendido haciendo clic en el enlace **Configuración de filtros**.

  Al hacer clic en el enlace **Configuración de filtros**, se muestran campos en los que puede especificar la configuración del filtro (vea la siguiente figura) y se abre la ventana **Configuración de filtrado**. En la ventana **Configuración de filtrado**, use casillas para especificar las columnas de lista en las que se debe realizar el filtrado. La selección de casillas en la ventana **Configuración de filtrado** depende de las columnas de lista disponibles y puede variar.

MENÚ CONTEXTUAL

En el árbol de consola de Kaspersky Security Center, cada objeto tiene su propio menú contextual. En el árbol de consola, los comandos estándar del menú contextual de Microsoft Management Console se complementan con comandos utilizados para operaciones con el objeto. Una lista de objetos y un conjunto adicional de comandos del menú contextual se incluyen en el apéndice.

En el espacio de trabajo, cada elemento de un objeto seleccionado en el árbol también tiene un menú contextual que contiene los comandos utilizados para manipular ese elemento. Los tipos básicos de elementos y un conjunto adicional de comandos se incluyen en el apéndice.

CONFIGURACIÓN DE LA INTERFAZ

Kaspersky Security Center permite configurar la interfaz de la Consola de administración.

➧ *Para cambiar los parámetros de la interfaz especificados:*

1. En el árbol de consola, haga clic el nodo del Servidor de administración.
2. En el menú **Ver**, seleccione **Configuración de interfaz**.

3. En la ventana **Configuración de interfaz** que se abre, configure la visualización de los elementos de la interfaz mediante las siguientes casillas de verificación:

   - **Mostrar administración de sistema.**

     Si esta casilla está seleccionada, en la carpeta **Instalación remota**, se muestra la carpeta anidada **Distribución de imágenes de equipo**, mientras que en la carpeta **Repositorios** se muestra la carpeta anidada **Hardware**.

     Esta casilla se desactiva de forma predeterminada.

   - **Mostrar cifrado y protección de datos.**

     Si esta casilla está seleccionada, la administración de cifrado de datos estará disponible en los dispositivos que estén conectados a la red. Después de que reinicie la aplicación, el árbol de consola mostrará la carpeta **Cifrado y Protección de datos**.

     Esta casilla se desactiva de forma predeterminada.

   - **Mostrar Anti-malware avanzado.**

     Si esta casilla está seleccionada, se mostrarán las siguientes subsecciones en la sección **Control de Endpoint** de la ventana de propiedades de la directiva de Kaspersky Endpoint Security 10 para Windows:

     - **Control de inicio de aplicaciones**.
     - **Monitor de vulnerabilidades**.
     - **Control de dispositivos**.
     - **Control Web**.

     Si esta casilla está desactivada, las subsecciones especificadas anteriormente no se mostrarán en la sección **control de Endpoint**.

     Esta casilla se desactiva de forma predeterminada.

   - **Mostrar administración de dispositivos móviles.**

     Si esta casilla está seleccionada, la función **Administración de dispositivos móviles** está disponible. Después de que reinicie la aplicación, el árbol de consola mostrará la carpeta **Dispositivos móviles**.

     Esta casilla se desactiva de forma predeterminada.

   - **Mostrar Servidores de administración secundarios.**

     Si la casilla de verificación está seleccionada, el árbol de consola muestra los nodos de los Servidores de administración secundarios y virtuales incluidos en los grupos de administración. Está disponible la funcionalidad conectada con los Servidores de administración secundarios y virtuales, en particular, la creación de tareas de instalación remota de aplicaciones en Servidores de administración secundarios.

     Esta casilla se activa de forma predeterminada.

   - **Mostrar secciones de configuración de seguridad.**

     Si esta casilla está seleccionada, se muestra la sección **Seguridad** en las propiedades del Servidor de administración, grupos de administración y otros objetos. Esta casilla permite otorgar permisos personalizados para trabajar con objetos a usuarios y grupos de usuarios.

     Esta casilla se activa de forma predeterminada.

LICENCIA DE LA APLICACIÓN

Esta sección proporciona información acerca de los conceptos generales relacionados con la licencia de la aplicación.

EN ESTA SECCIÓN:

Acerca del Contrato de licencia de usuario final 33
Acerca de la licencia 33
Acerca de la clave 34
Opciones de licencias de Kaspersky Security Center 34
Acerca de las restricciones de las funciones principales 35
Acerca del código de activación 36
Acerca del archivo de clave 36

ACERCA DEL CONTRATO DE LICENCIA DE USUARIO FINAL

El Contrato de licencia de usuario final es un contrato vinculante entre usted y Kaspersky Lab ZAO, en el cual se establecen los términos de uso de la aplicación.

Le recomendamos que lea los términos del Contrato de Licencia de Usuario Final cuidadosamente antes de empezar a usar la aplicación.

Puede ver los términos del Contrato de Licencia de Usuario Final usando los siguientes métodos:

- Al instalar Kaspersky Security Center.
- Al leer el documento license.txt. Este documento está incluido en el kit de distribución de la aplicación.

Acepta los términos del Contrato de Licencia de Usuario Final al confirmar que está de acuerdo con el Contrato de Licencia de Usuario Final al instalar la aplicación. Si no acepta los términos del Contrato de Licencia de Usuario Final, deberá cancelar la instalación de la aplicación y renunciar a su uso.

ACERCA DE LA LICENCIA

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

Una licencia válida le permite usar los servicios siguientes:

- El uso de la aplicación de conformidad con los términos del Contrato de Licencia de Usuario Final.
- Soporte técnico.

El alcance del período de uso de los servicios y las aplicaciones proporcionados depende del tipo de licencia que se usó para activar la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *De prueba*: licencia gratuita diseñada para la prueba de la aplicación.

  Usualmente, una licencia de prueba tiene un plazo corto. Apenas vence la licencia de prueba, todas las características de Kaspersky Security Center se deshabilitan. Para continuar usando la aplicación, debe adquirir la licencia comercial.

  Puede activar la aplicación con la licencia de prueba sólo una vez.

- *Comercial*: una licencia paga otorgada por la compra de la aplicación.

  Cuando vence la licencia comercial, la aplicación se continúa ejecutando, pero con funcionalidades limitadas (por ejemplo, no están disponibles las actualizaciones ni el uso de las bases de datos de Kaspersky Security Center). Para continuar usando Kaspersky Security Center en un modo completamente funcional, debe renovar su licencia comercial.

Se recomienda renovar la licencia antes de que caduque de modo de garantizar la protección máxima contra todas las amenazas a la seguridad.

ACERCA DE LA CLAVE

Una *llave* es una secuencia de bits que puede aplicar para activar y, luego, usar la aplicación de acuerdo con los términos del Contrato de licencia de usuario final. Las llaves son generadas por los especialistas de Kaspersky Lab.

Para agregar una llave a la aplicación, debe ingresar un *código de activación*. La llave se muestra en la interfaz de la aplicación como una secuencia alfanumérica única después de que la agrega a la aplicación.

Kaspersky Lab puede bloquear la llave en caso de que se hayan infringido los términos del Contrato de licencia. Si la llave se ha bloqueado, debe agregar otra si desea usar la aplicación.

Una llave puede ser activa o adicional.

Llave activa: una llave que se usa en el momento de trabajar con la aplicación. La aplicación no puede usar más de una llave activa.

Llave adicional: una llave que verifica el uso de la aplicación, pero que no se usa en el momento. La llave adicional se activa de forma automática cuando caduca la licencia asociada con la llave activa actual. Se puede agregar una llave adicional únicamente si ya se ha agregado una llave activa.

Se puede agregar una clave para la licencia de prueba solo como la clave activa. No se puede agregar una clave para la licencia de prueba como una clave adicional.

OPCIONES DE LICENCIAS DE KASPERSKY SECURITY CENTER

En Kaspersky Security Center, la licencia puede aplicarse a diferentes grupos de funcionalidades.

Funcionalidad básica de la Consola de administración

Están disponibles las siguientes funciones:

- Creación de Servidores de administración virtuales para administrar una red de oficinas remotas u organizaciones cliente.
- Creación de una jerarquía de grupos de administración para administrar una selección de dispositivos como un todo.
- Control del estado de la seguridad antivirus de una organización.
- Instalación remota de aplicaciones.
- Visualización de la lista de imágenes de sistemas operativos disponibles para la instalación remota.
- Configuración centralizada para aplicaciones instaladas en equipos cliente.
- Visualización y edición de los grupos existentes de aplicaciones con licencia.
- Estadísticas e informes sobre la operación de la aplicación, así como notificaciones sobre eventos críticos.
- Administración del cifrado y de la protección de los datos.
- Visualización y edición manual de la lista de componentes de hardware detectados mediante el sondeo de la red.
- Operaciones centralizadas con archivos que se movieron a Cuarentena o Copia de seguridad y archivos cuyo procesamiento se pospuso.

Kaspersky Security Center con compatibilidad para la funcionalidad básica de la Consola de administración se entrega como parte de los productos de Kaspersky Lab para la protección de redes corporativas. También se puede descargar desde el sitio web de Kaspersky Lab (http://latam.kaspersky.com).

Hasta activar la aplicación, o después de que vence la licencia comercial, Kaspersky Security Center se ejecuta en el modo de funcionalidad básica de la Consola de administración (ver la sección “Acerca de las restricciones de la funcionalidad básica“ en la página 35).

Administración del sistema.

Están disponibles las siguientes funciones:

- Instalación remota de sistemas operativos.
- Instalación remota de actualizaciones de software; escaneo y reparación de vulnerabilidades.
- Administración del acceso de los dispositivos a la red de una organización (Control de acceso a la red, NAC).
- Inventario de componentes de hardware.
- Administración del grupo de aplicaciones con licencia
- Permiso remoto para la conexión con equipos cliente mediante un componente de Microsoft Windows® denominado Conexión de escritorio remoto.
- Conexión remota con equipos cliente mediante Windows Desktop Sharing.
- Administración de roles de usuarios.

La unidad de administración para la Administración del sistema es un equipo cliente del grupo “Equipos administrados”.

Para que la Administración de sistema funcione sin inconvenientes, se deberá contar con al menos 100 GB de espacio libre en disco.

Administración de dispositivos móviles

La Administración de dispositivos móviles se usa para Administrar dispositivos móviles de Exchange ActiveSync y iOS MDM.

Las siguientes funciones están disponibles para los dispositivos móviles Exchange ActiveSync:

- Creación y edición de perfiles de administración de dispositivos móviles, asignación de perfiles a buzones de usuarios
- Configuración de un dispositivo móvil (sincronización de correo, uso de aplicaciones, contraseña de usuario, cifrado de datos, conexión de medios extraíbles)
- Instalación de certificados en los dispositivos móviles.

Las siguientes funciones están disponibles para los dispositivos móviles con MDM de iOS:

- Creación y edición de perfiles de configuración, e instalación de perfiles de configuración en los dispositivos móviles
- Instalación de aplicaciones en un dispositivo móvil a través de App Store o mediante archivos de manifiesto (.plist)
- Bloqueo de dispositivos móviles, restablecimiento de la contraseña de dispositivos móviles y eliminación de todos los datos del dispositivo móvil

Además, la Administración de dispositivos móviles permite ejecutar comandos proporcionados por protocolos relevantes.

La unidad de administración para la Administración de dispositivos móviles es un dispositivo móvil. Un dispositivo móvil se considera administrado desde que se conecta a un servidor de dispositivos móviles.

ACERCA DE LAS RESTRICCIONES DE LAS FUNCIONES PRINCIPALES

Hasta activar la aplicación o después de vencida la licencia comercial, Kaspersky Security Center proporciona la funcionalidad básica de la Consola de administración. Las limitaciones impuestas sobre el funcionamiento de la aplicación se describen a continuación.

Administración de dispositivos móviles

No se puede crear un perfil nuevo y asignarlo a un dispositivo móvil (MDM de iOS) ni a una casilla de correo (Exchange ActiveSync). La opciones de edición de los perfiles existentes y de asignación de perfiles a las casillas de correo están siempre disponibles.

Administración de las aplicaciones

No se puede ejecutar la tarea de instalación de actualizaciones ni la tarea de eliminación de actualizaciones. Todas las tareas que se han iniciado antes de vencida la licencia se completarán, pero no se instalarán las últimas actualizaciones. Por ejemplo, si la tarea de instalación de actualizaciones críticas se ejecutó antes de que caduque la licencia, solo las actualizaciones críticas que se encontraron antes de la caducidad de la licencia se instalarán.

Las tareas de inicio y edición de la sincronización, análisis de vulnerabilidades y actualización de la base de datos de vulnerabilidades siempre están disponibles. Tampoco se establecen limitaciones para ver, buscar y ordenar las entradas en la lista de vulnerabilidades y actualizaciones.

Instalación remota de sistemas operativos y aplicaciones

No se pueden ejecutar tareas de captura e instalación de imágenes del sistema operativo. Las tareas que se han iniciado antes de vencida la licencia se completarán.

Control de acceso a la red

El agente NAC y NAC cambian al modo “Desactivado” sin opción para habilitarlos.

Inventario de hardware

No se puede usar la función de recopilación de información sobre nuevos dispositivos con NAC y con el servidor de dispositivos móviles La información sobre los equipos y los dispositivos conectados se actualiza.

No recibe ninguna notificación sobre los cambios en las configuraciones de los dispositivos.

La lista de equipos está disponible para verla y editarla manualmente.

Administrar grupos de aplicaciones con licencia

No se puede agregar una clave nueva.

No recibirá notificación de las limitaciones violadas impuestas sobre el uso de claves.

Conexión remota a equipos cliente.

La conexión remota con los equipos cliente no está disponible.

Seguridad antivirus

Anti-Virus usa bases de datos que se han instalado antes de vencida la licencia.

ACERCA DEL CÓDIGO DE ACTIVACIÓN

Un *código de activación* es un código que se recibe al comprar una licencia comercial de Kaspersky Security Center. El código de activación es una secuencia única de veinte dígitos y letras latinas con el formato xxxxx-xxxxx-xxxxx-xxxxx.

Para activar la aplicación con un código de activación, debe conectarse con los servidores de activación de Kaspersky Lab por Internet. Si no se ha establecido una conexión con los servidores de activación e Internet, la aplicación se activa mediante un archivo de clave (ver la sección “Acerca del archivo de clave“ en la página 36).

El plazo de la licencia empieza el día en que se activa la aplicación. Si ha comprado una licencia que le permite usar Kaspersky Security Center en distintos dispositivos, el término de la licencia comienza desde el momento en que ha implementado por primera vez el código de activación.

Si ha perdido o eliminado accidentalmente su código de activación después de la activación de la aplicación, póngase en contacto con el Servicio de soporte técnico de Kaspersky Lab para recuperar el código de activación.

ACERCA DEL ARCHIVO DE CLAVE

El archivo de clave es un archivo con el nombre siguiente: xxxxxxx.key.

Los archivos de clave se usan para activar la aplicación. Un archivo de clave incluye la información necesaria para la activación. Para activar la aplicación mediante el archivo de clave, no es necesario conectarse a los servidores de activación ni a Internet.

Para obtener un archivo de clave o recuperar la clave en el caso de perderla, envíe una solicitud al Servicio de soporte técnico.

El archivo de clave contiene la siguiente información:

- La clave es una secuencia alfanumérica única. La clave se puede usar, por ejemplo, para obtener soporte técnico de Kaspersky Lab.
- El archivo de clave de Kaspersky Security Center puede especificar las restricciones para la cantidad de equipos y dispositivos móviles administrados. El tipo de límite se determina mediante la licencia actual (ver la sección “Opciones de licencia de Kaspersky Security Center“ en la página 34).
- Fecha de creación del archivo de clave: la fecha en que se creó el archivo de clave en el servidor de activación.
- El período de validez de la licencia es el término de uso de la aplicación estipulado por el Contrato de licencia y que comienza a partir del día de la primera activación de la aplicación que hace uso del archivo de clave proporcionado (por ejemplo, un año).

  La licencia vence, a más tardar, el día de vencimiento del archivo de clave que se utilizó para activar la aplicación con esta licencia.

- La fecha de vencimiento del archivo de clave es un período específico que comienza a partir del día en que se crea el archivo de clave. La aplicación se activará utilizando la clave proporcionada antes de que finalice este período.

  El período de vencimiento del archivo de clave se considera automáticamente vencido cuando vence la licencia para la aplicación activada que usa este archivo de clave.

ASISTENTE DE INICIO RÁPIDO DE KASPERSKY SECURITY CENTER

Esta sección proporciona información sobre la funcionalidad del Asistente de inicio rápido de Kaspersky Security Center.

La aplicación Kaspersky Security Center permite ajustar los parámetros mínimos necesarios para desarrollar un sistema de administración centralizado para la protección antivirus. Esta configuración se realiza mediante el Asistente de inicio rápido. Mientras que el Asistente de inicio rápido está en ejecución, se realizan los siguientes cambios en la aplicación:

- El Asistente agrega claves que se pueden distribuir automáticamente a los equipos dentro de los grupos de administración.
- Se configura la interacción con Kaspersky Security Network (KSN). KSN permite recuperar información sobre las aplicaciones instaladas en equipos administrados si esta información se pueda encontrar en las bases de datos de reputación de Kaspersky Lab. Si se permitió el uso de KSN, el asistente inicia el servicio del servidor proxy de KSN, que garantiza la conexión entre KSN y los equipos cliente.
- Genera la configuración para la entrega mediante correo electrónico de notificaciones de eventos registrados en el Servidor de administración y de aplicaciones administradas (para garantizar una notificación exitosa, el servicio Messenger debe mantenerse en ejecución en el Servidor de administración y en todos los equipos de destino).
- Luego, el Asistente ajusta la configuración de actualización y de reparación de vulnerabilidades de las aplicaciones instaladas en equipos cliente.
- Las directivas de protección para estaciones de trabajo se crean en el nivel superior de la jerarquía de equipos administrados; también se crean tareas de escaneo de virus, tareas de actualización y tareas de copias de seguridad.

> El Asistente de inicio rápido crea directivas de protección solo para aplicaciones para las cuales la carpeta **Equipos administrados** no contiene ninguna. El Asistente de inicio rápido no crea tareas si alguna tarea con el mismo nombre ya se creó para el nivel superior de la jerarquía de equipos administrados.

Se ofrece ejecutar el Asistente de inicio rápido luego de la instalación del Servidor de administración, cuando se realiza la primera conexión con este. También puede ejecutar el Asistente de inicio rápido de forma manual mediante el menú contextual del nodo **Servidor de administración <nombre del equipo>**.

CONSULTE TAMBIÉN:

Interacción entre el Servidor de administración y el servicio de proxy de KSN 53

CONCEPTOS BÁSICOS

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

EN ESTA SECCIÓN:

Servidor de administración 39
Jerarquía del Servidor de administración 40
Servidor de administración virtual 40
Servidor de dispositivos móviles 41
Servidor web 41
Agente de red. Grupo de administración 42
Estación de trabajo del administrador 42
Complemento de administración de aplicaciones 42
Directivas, parámetros de la aplicación y tareas 43
Modo en que se relacionan las directivas y la configuración local de la aplicación 44

SERVIDOR DE ADMINISTRACIÓN

Los componentes de Kaspersky Security Center permiten la administración remota de las aplicaciones Kaspersky Lab instaladas en equipos cliente.

Los equipos con el componente Servidor de administración instalado serán mencionados como *Servidores de administración* (en adelante denominados *Servidores*).

El Servidor de administración se instala en un equipo como un servicio con el siguiente conjunto de atributos:

- Con el nombre "Servidor de administración de Kaspersky Security Center".
- Utilizando el inicio automático cuando inicia el sistema operativo.
- Con la cuenta del **sistema local** o la cuenta de usuario seleccionada durante la instalación del Servidor de administración.

El Servidor de administración realiza las siguientes funciones:

- almacenar la estructura de los grupos de administración;
- almacenar la información sobre la configuración de equipos cliente;
- organizar los almacenamientos para paquetes de distribución de aplicaciones;
- instalar de manera remota aplicaciones en dispositivos cliente y eliminarlas;
- actualización de bases de datos de aplicaciones y módulos de software de aplicaciones Kaspersky Lab;
- administración de directivas y tareas en los equipos cliente;
- almacenar información sobre eventos producidos en equipos cliente;
- generación de informes sobre el funcionamiento de aplicaciones Kaspersky Lab;
- distribuir claves en los equipos cliente y almacenar información sobre claves;
- enviar notificaciones sobre el progreso de las tareas (por ejemplo, de virus detectados en un equipo cliente).

JERARQUÍA DEL SERVIDOR DE ADMINISTRACIÓN

Los Servidores de administración se pueden organizar en una jerarquía tipo maestro/secundario. Cada Servidor de administración puede tener varios Servidores de administración secundarios (denominados *Servidores secundarios*) en diferentes niveles de anidamiento de la jerarquía. El nivel de anidamiento para los Servidores secundarios no está restringido. Por tanto, los grupos de administración del Servidor de administración maestro incluirán los equipos cliente de todos los Servidores de administración secundarios. De esta manera, secciones independientes y aisladas de redes de equipos pueden ser controladas por diferentes Servidores de administración que, a su vez, están administrados por el Servidor primario.

Los *Servidores de administración virtuales* (ver la sección “Servidor de administración virtual” en la página 40) son un caso particular de Servidores de administración secundarios.

La jerarquía de Servidores de administración se puede usar para realizar lo siguiente:

- Disminuir la carga en el Servidor de administración (en comparación con un único Servidor de administración instalado en toda la red).
- Disminuir el tráfico de intranet y simplificar el trabajo con las oficinas remotas. No es necesario establecer conexiones entre el Servidor de administración maestro y todos los equipos de la red, que pueden estar ubicados, por ejemplo, en otras regiones. Es suficiente instalar, en cada segmento de red, un Servidor de administración secundario, distribuir los equipos entre grupos de administración de Servidores secundarios y establecer conexiones entre los Servidores secundarios y el Servidor primario sobre canales de comunicación rápida.
- Distribuir las responsabilidades entre los administradores de seguridad antivirus. Todas las capacidades para la administración centralizada y el control de la seguridad antivirus en las redes corporativas permanecen disponibles.
- Cómo usan los proveedores de servicio Kaspersky Security Center. Un proveedor de servicios necesita instalar únicamente Kaspersky Security Center y Kaspersky Security Center Web Console. Para administrar más equipos cliente de varias organizaciones, un proveedor de servicios puede agregar Servidores de administración virtuales a una jerarquía de Servidores de administración.

Cada equipo incluido en la jerarquía de los grupos de administración puede ser conectado solamente a un Servidor de administración. Debe controlar el estado de la conexión de equipos a los Servidores de administración. Use las funciones para la búsqueda de equipos en los grupos de administración de diferentes Servidores en función de los atributos de red.

SERVIDOR DE ADMINISTRACIÓN VIRTUAL

El Servidor de administración virtual (también llamado *Servidor virtual*.) es un componente de Kaspersky Security Center cuyo propósito es administrar la protección antivirus de la red de la organización cliente.

El Servidor de administración virtual es un caso particular de Servidor de administración secundario y posee las siguientes restricciones en comparación con el Servidor de administración físico:

- El Servidor de administración virtual puede crearse solamente en el Servidor de administración maestro.
- El Servidor de administración virtual usa bases de datos del Servidor de administración maestro en su funcionamiento: las tareas de copia de seguridad de los datos, las tareas de recuperación de datos, las tareas de actualización de verificación, y las tareas de descarga de actualizaciones no son compatibles con el Servidor virtual. Estas tareas existen únicamente en el Servidor de administración maestro.
- El Servidor virtual no admite la creación de Servidores de administración secundarios (incluidos Servidores virtuales).

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

- En la ventana de propiedades del Servidor de administración virtual el número de secciones está limitada.
- Para llevar a cabo la instalación remota de las aplicaciones de Kaspersky Lab en equipos cliente administrados por el Servidor de administración virtual, debe asegurarse de que el Agente de red esté instalado en uno de los equipos clientes para garantizar la comunicación con el Servidor de administración virtual. En la primera conexión con el Servidor de administración virtual, ese equipo se designa automáticamente como Agente de actualización y por lo tanto funciona como puerta de enlace para la conexión entre los equipos cliente y el Servidor de administración virtual.
- Un Servidor virtual solo puede sondear la red utilizando Agentes de actualización.
- Para reiniciar un Servidor virtual que funciona incorrectamente, Kaspersky Security Center reinicia el Servidor de administración maestro y todos los Servidores de administración virtuales.

El administrador de un Servidor de administración virtual tiene todos los privilegios en este Servidor virtual particular.

SERVIDOR DE DISPOSITIVOS MÓVILES

Un servidor de dispositivos móviles es un componente de Kaspersky Security Center que proporciona acceso a los dispositivos móviles y permite administrarlos por medio de la Consola de administración. El servidor de dispositivos móviles recupera información acerca de los dispositivos móviles y almacena sus perfiles.

Hay dos tipos de servidores de dispositivos móviles:

- Servidor de dispositivos móviles que admiten Exchange ActiveSync. Se instala en un equipo cliente donde se haya instalado un servidor de Microsoft Exchange, lo que permite recuperar datos del servidor de Microsoft Exchange y pasarlos al Servidor de administración. Este servidor de dispositivos móviles se usa para administrar los dispositivos móviles que admiten el protocolo Exchange ActiveSync.
- Servidor de dispositivos móviles con MDM de iOS. Este servidor de dispositivos móviles se usa para administrar los dispositivos móviles que admiten el servicio Apple Push Notifications (APNs).

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

- Un dispositivo móvil individual
- Varios dispositivos móviles
- Varios dispositivos móviles conectados simultáneamente a un clúster de servidores. Después de conectarse a un clúster de servidores, los dispositivos móviles instalados en este clúster aparecen en la Consola de administración como un único servidor.

SERVIDOR WEB

El *Servidor web* de Kaspersky Security Center (en adelante también denominado *Servidor web*) es un componente de Kaspersky Security Center que se instala junto con el Servidor de administración. El Servidor web está diseñado para la transferencia de paquetes de instalación independiente, perfiles MDM de iOS MDM, y archivos de la carpeta compartida a la red.

Al crear un paquete de instalación independiente, éste se publica automáticamente en el Servidor web. En la lista de paquetes de instalación independiente creados se muestra un enlace de descarga del paquete independiente. De ser necesario, puede cancelar la publicación del paquete independiente o publicarlo nuevamente en el Servidor web.

Cuando crea un perfil de MDM de iOS para el dispositivo móvil del usuario, también se publica automáticamente en el Servidor web. Cuando se publica el perfil, se elimina automáticamente del Servidor web después de ser instalado correctamente en el dispositivo móvil del usuario (para obtener más detalles sobre cómo crear e instalar un perfil de MDM de iOS, consulte la *Guía de implementación de Kaspersky Security Center*).

La carpeta compartida está diseñada como una zona de almacenamiento de información disponible para todos los usuarios cuyos equipos sean administrados a través del Servidor de administración. Si el usuario no posee un acceso directo a la carpeta compartida, puede obtener información sobre esa carpeta en el servidor web.

Para brindar información a los usuarios de la carpeta compartida con el Servidor web, el administrador debe crear una subcarpeta llamada “Pública” en la carpeta compartida y pegar la información en ella.

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

`http://<Web Server name>:<HTTP port>/public/<object>`

donde:

`<Web Server name>` es el nombre del Servidor web de Kaspersky Security Center.

`<HTTP port>` es un puerto HTTP del Servidor web definido por el administrador. Un puerto HTTP se puede configurar en la sección **Servidor web** de la ventada de propiedades del Servidor de administración. El número de puerto predeterminado es el 8060.

`<object>` es una subcarpeta o archivo al cual el usuario debe tener acceso.

El administrador puede enviar el nuevo enlace al usuario de cualquier manera que le resulte conveniente: por ejemplo, por correo electrónico.

Al hacer clic en el enlace, el usuario puede descargar la información solicitada a un equipo local.

GRUPO DE ADMINISTRACIÓN DEL AGENTE DE RED

La interacción entre el Servidor de administración y los equipos cliente se realiza mediante un componente de la aplicación Kaspersky Security Center denominado *Agente de red*. El Agente de red debe instalarse en todos los equipos cliente en los que se utiliza Kaspersky Security Center para administrar las aplicaciones de Kaspersky Lab.

El Agente de red se instala en un equipo como un servicio con el siguiente conjunto de atributos:

- Con el nombre "Agente de red de Kaspersky Security Center".
- Establecer al inicio automático cuando el sistema operativo se inicie
- Utilizando la cuenta del **sistema local**.

El Agente de red se instala en el equipo junto con un complemento para trabajar con Cisco® NAC. Este complemento se utiliza si el equipo tiene Cisco® Trust Agent instalado. La configuración para la operación conjunta con Cisco® NAC se especifica en la ventana de propiedades del Servidor de administración.

Cuando se integra con Cisco® NAC, el Servidor de administración actúa como un servidor de directivas estándar del Servidor de Validación de Postura (PVS), que un administrador puede usar para autorizar o bloquear el acceso de un equipo a la red, en función del estado de la protección antivirus.

Un equipo, servidor o estación de trabajo donde está instalado el Agente de red y las aplicaciones Kaspersky Lab administradas se denominará *cliente del Servidor de administración* (también, *equipo cliente* o solo *equipo*).

El conjunto de equipos en una red corporativa puede ser subdividido en grupos organizados en una determinada estructura jerárquica. Tales grupos se denominan *grupos de administración*. La jerarquía de los grupos de administración se muestra en el árbol de consola dentro del nodo del Servidor de administración.

Grupo de administración (en adelante, también referido como *grupo*) es un conjunto de equipos cliente unidos en base a un determinado criterio para administrar los equipos agrupados como un todo. Todos los equipos cliente en un grupo se configuran para:

- Utilizar los mismos parámetros de aplicación (que están definidos en las *directivas de grupo).*
- Usar un modo común de funcionamiento de aplicaciones debido a la creación de *tareas de grupo* con un conjunto especificado de configuraciones. Por ejemplo, crear e instalar un *paquete de instalación* común, actualizar las bases de datos y módulos de la aplicación, escanear el equipo a pedido y garantizar la protección en tiempo real.

Un equipo cliente puede ser incluido sólo en un único grupo de administración.

Puede crear jerarquías de Servidores y grupos con cualquier grado de anidamiento. Un único nivel de jerarquía puede incluir Servidores de administración secundarios y virtuales, grupos y equipos cliente.

ESTACIÓN DE TRABAJO DEL ADMINISTRADOR

Los equipos en los que se instaló el componente *Consola de administración* se denominan *equipos administradores*. Los administradores pueden usar esos equipos para la administración remota centralizada de aplicaciones Kaspersky Lab instaladas en equipos cliente.

Una vez instalada la Consola de administración, su icono aparecerá en el menú **Inicio** → **Programas** → **Kaspersky Security Center**, y puede ser usado para iniciar la consola.

No hay restricciones sobre el número de equipos administrador. Desde cualquier estación de trabajo de un administrador, puede administrar grupos de administración de varios Servidores de administración en la red, al mismo tiempo. Puede conectar el equipo administrador a un Servidor de administración (ya sea físico o virtual) de cualquier nivel de jerarquía.

Puede incluir el equipo administrador en un grupo de administración como equipo cliente.

Dentro de los grupos de administración de cualquier Servidor de administración, el mismo equipo puede actuar como un cliente del Servidor de administración, un Servidor de administración o una estación de trabajo de un administrador.

COMPLEMENTO DE ADMINISTRACIÓN DE APLICACIONES

La administración de las aplicaciones de Kaspersky Lab mediante la Consola de administración se realiza usando un componente especial llamado *complemento de administración*, que se incluye en todas las aplicaciones de Kaspersky Lab que se pueden administrar usando Kaspersky Security Center.

El complemento de administración está instalado en el equipo administrador. Mediante el complemento de administración, es posible realizar las siguientes acciones en la Consola de administración:

- crear y editar las directivas y configuración de la aplicación, además de la configuración de las tareas de la aplicación;
- obtener información sobre las tareas de la aplicación, eventos que se producen en su funcionamiento, y también estadísticas de funcionamiento de la aplicación recibidas desde equipos cliente.

DIRECTIVAS, PARÁMETROS DE LA APLICACIÓN Y TAREAS

Una acción realizada por una aplicación Kaspersky Lab se denomina *tarea*. Las tareas se organizan por *tipos* de acuerdo con las funciones.

Cada tarea se asocia a un conjunto de configuraciones utilizadas durante la ejecución de la tarea. El conjunto de configuraciones de la aplicación comunes a todos los tipos de tareas constituye la configuración de la aplicación. Las configuraciones de aplicación específicas para cada tipo de tarea constituyen la configuración de la tarea correspondiente.

Una descripción detallada de los tipos de tarea para cada aplicación Kaspersky Lab está disponible en las respectivas guías de la aplicación.

La configuración de la aplicación, definida para un equipo cliente individual a través de la interfaz local o de forma remota a través de la Consola de administración se denomina *configuración de la aplicación local*.

Las aplicaciones instaladas en los equipos cliente se configuran de modo centralizado a través de la definición de directivas.

Una *directiva* es un conjunto de configuraciones de la aplicación definido para un grupo de administración. La directiva no define todos los parámetros de la aplicación.

Se pueden definir varios valores con diferentes parámetros para una única aplicación. Sin embargo, solo puede existir una directiva activa a la vez para una aplicación.

El programa puede ejecutarse de maneras diferentes para grupos de parámetros diferentes. Cada grupo puede tener su propia directiva para una aplicación.

Los parámetros de aplicación se definen como los parámetros de la directiva y los parámetros de tarea.

Los grupos secundarios y Servidores de administración secundarios heredan las tareas desde los grupos pertenecientes a los niveles de jerarquía superiores. Una tarea definida para un grupo se realiza no solo en los equipos cliente incluidos en ese grupo sino también en equipos cliente incluidos en sus grupos secundarios y que pertenecen a los Servidores secundarios en todos los niveles jerárquicos inferiores.

Cada configuración representada en una directiva posee un atributo de "bloqueo":  . El “bloqueo” que muestra si se permite modificar la configuración en las directivas de los niveles jerárquicos inferiores (para grupos anidados y Servidores de administración secundarios), en la configuración de la tarea y la configuración local de la aplicación. Si un parámetro está “bloqueado” en la directiva, su valor no puede volver a definirse (ver la sección “Cómo se relaciona la configuración de la aplicación local con las directivas” en la página 44).

Si se desactiva la casilla **Heredar configuración desde la directiva primaria** en la sección **Herencia de configuración** de la sección **General** en la ventana de propiedades de una directiva heredada, se levanta el “bloqueo” para esa directiva.

Usted puede activar una directiva deshabilitada en función del suceso de un evento determinado. Esto significa que puede, por ejemplo, forzar los parámetros de protección antivirus estricta durante un foco de virus.

También puede crear directivas para usuarios móviles.

Las tareas para los objetos administrados, por un único Servidor de administración, son creadas y configuradas de forma centralizada. Pueden definirse tareas de los siguientes tipos:

- *Tarea de grupo* es una tarea que define los parámetros para una aplicación instalada en los equipos de un grupo de administración.
- *Tarea local* es una tarea para un equipo individual.
- *Tarea para una selección de equipos* es una tarea para un conjunto de equipos arbitrarios incluidos o no en grupos de administración.
- *Tarea del Servidor de administración* es una tarea definida directamente para un Servidor de administración.

Una tarea de grupo puede ser definida para un grupo, incluso si una aplicación de Kaspersky Lab está instalada sólo en algunos equipos cliente de ese grupo. En ese caso, la tarea de grupo se realizará únicamente en aquellos equipos donde la aplicación esté instalada.

Las tareas creadas para un equipo cliente localmente solo se realizarán en ese equipo. Cuando se sincroniza un equipo cliente con el Servidor de administración, las tareas locales se agregan a la lista de tareas creadas para ese equipo cliente.

Dado que la configuración de la aplicación se define según directivas, la configuración de la tarea puede redefinir aquellos parámetros que no estén bloqueados en la directiva. La configuración de la tarea también puede redefinir parámetros que puedan ser configurados únicamente por una instancia específica de una tarea. Por ejemplo, el nombre de la unidad y las máscaras de archivos que se deben escanear son configuraciones de ese tipo para la tarea de escaneo de la unidad.

Una tarea puede ser iniciada automáticamente (de acuerdo con la planificación) o manualmente. Los resultados de la tarea se guardan localmente y en el Servidor de administración. El administrador puede recibir notificaciones acerca de las tareas específicas realizadas y ver informes detallados.

La información sobre directivas, configuración de la aplicación, configuración de tareas para equipos específicos e información sobre tareas de grupo se guardan en el Servidor de administración y se distribuyen a los equipos cliente durante la sincronización. En ese momento, el Servidor de administración almacena información sobre cambios locales permitidos por la directiva y realizados en equipos cliente. Además, se actualiza la lista de aplicaciones en ejecución en un cliente, su estado y las tareas existentes.

MODO EN QUE SE RELACIONAN LAS DIRECTIVAS Y LA CONFIGURACIÓN LOCAL DE LA APLICACIÓN

Puede usar las directivas para establecer valores idénticos de configuración de la aplicación para todos los equipos del grupo.

Los valores de configuración especificados por una directiva pueden ser redefinidos por equipos individuales de un grupo, utilizando la configuración local de la aplicación. Solo se pueden establecer los valores de configuración que la directiva permite modificar, es decir, parámetros “desbloqueados”.

El valor que una aplicación utiliza en un equipo cliente (ver la figura siguiente), se determina por la posición del “bloqueo” para esa configuración en la directiva:

- Si la modificación del parámetro está “bloqueada”, el mismo valor definido en la directiva se utiliza en todos los equipos cliente;
- Si la modificación del parámetro está “desbloqueada”, la aplicación utiliza en cada equipo cliente el valor local en lugar del valor especificado en la directiva. Entonces, el valor del parámetro puede ser cambiado en los parámetros locales de la aplicación.

Figura 9. Directiva y parámetros de locales aplicación

De esta manera, cuando la tarea se ejecuta en un equipo cliente, la aplicación utiliza configuraciones definidas de dos maneras diferentes:

- mediante la configuración de la tarea y la configuración de la aplicación si el parámetro correspondiente no está bloqueado para la modificación;
- mediante la directiva de grupo si el parámetro está bloqueado para la modificación.

Los parámetros locales de la aplicación se cambian una vez que se aplica por primera vez la directiva, de acuerdo con los parámetros de la directiva.

ADMINISTRACIÓN DE LOS SERVIDORES DE ADMINISTRACIÓN

Esta sección proporciona información sobre cómo manejar los Servidores de administración y cómo configurarlos.

EN ESTA SECCIÓN:

Conexión a un Servidor de administración y alternancia entre Servidores de administración 46

Permisos de acceso al Servidor de administración y sus objetos 47

Condiciones de conexión a un Servidor de administración a través de Internet 48

Conexión segura con Servidor de administración 49

Desconexión de un Servidor de administración 50

Agregar un Servidor de administración al árbol de consola 50

Eliminar un Servidor de administración del árbol de consola 50

Cambio de una cuenta de servicio del Servidor de administración. Utilidad klsrvswch 50

Visualización y modificación de la configuración de un Servidor de administración 51

CONEXIÓN A UN SERVIDOR DE ADMINISTRACIÓN Y ALTERNANCIA ENTRE SERVIDORES DE ADMINISTRACIÓN

Una vez que se inicia Kaspersky Security Center, intenta conectarse a un Servidor de administración. Si existen varios Servidores de administración disponibles en la red, la aplicación solicita el Servidor al que se conectó durante la sesión anterior de Kaspersky Security Center.

Si la aplicación se inicia por primera vez después de la instalación, intenta conectarse al Servidor de administración especificado durante la instalación de Kaspersky Security Center.

Una vez que se estableció la conexión con un Servidor de administración, el árbol de carpetas de ese Servidor se muestra en el árbol de consola.

Si se agregaron varios Servidores de administración al árbol de consola, puede cambiar entre esos servidores.

Para conectarse a otro Servidor de administración:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el menú contextual del nodo, seleccione **Conectarse al Servidor de administración**.
3. En la ventana **Configuración de la conexión** que se abre, especifique en el campo **Dirección del servidor** el nombre del Servidor de administración al que desea conectarse. Puede especificar una dirección IP o el nombre de un equipo de una red de Windows como nombre del Servidor de administración. Puede hacer clic en el botón **Avanzado** en la parte inferior de la ventana para configurar la conexión al Servidor de administración (vea la siguiente figura).

   Para conectarse al Servidor de administración mediante un puerto diferente del predeterminado, ingrese un valor en el campo **Dirección del servidor** con el formato <Nombre del Servidor de administración>:<Puerto>.cv

Los usuarios que no tienen permiso de **Lectura** no tendrán acceso al Servidor de administración.

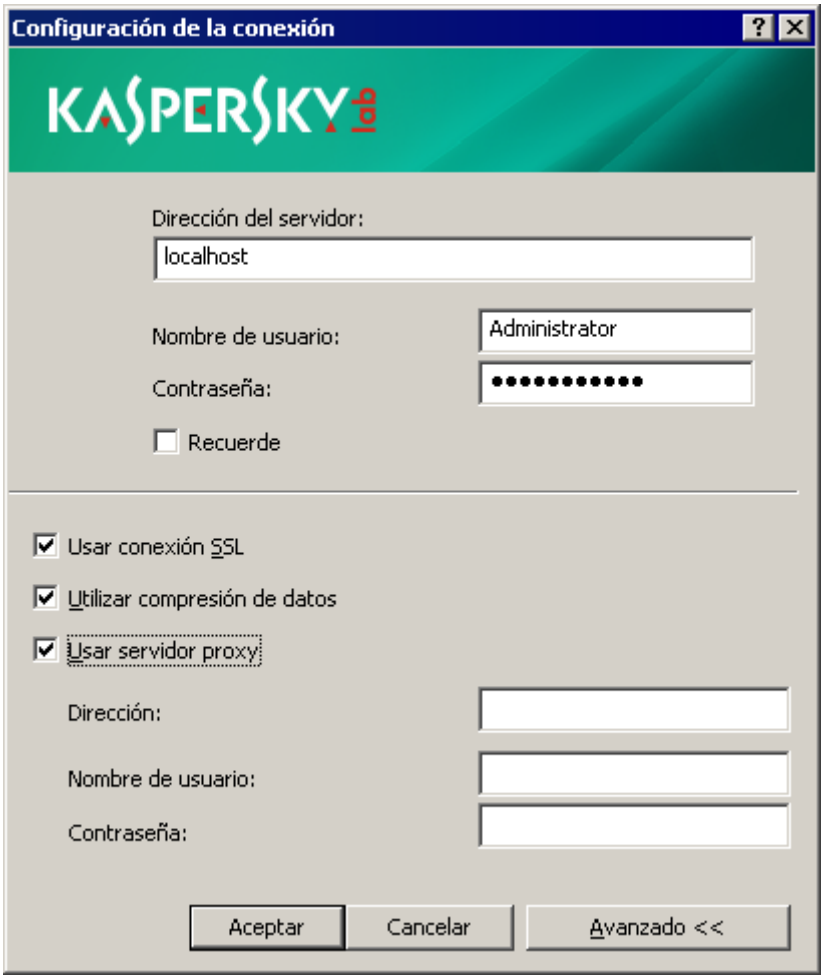


Figura 10. Conectarse al Servidor de administración

4. Haga clic en el botón **Aceptar** para completar el cambio entre servidores.

Una vez que el Servidor de administración está conectado, se actualiza el árbol de carpeta del nodo correspondiente en el árbol de consola.

PERMISOS DE ACCESO AL SERVIDOR DE ADMINISTRACIÓN Y SUS OBJETOS

Los grupos **KLAdmins** y **KLOperators** se crean automáticamente durante la instalación de Kaspersky Security Center. A estos grupos se les otorgan permisos para conectarse al Servidor de administración y trabajar con los objetos de este.

Según la cuenta que se use para instalar Kaspersky Security Center, los grupos **KLAdmins** y **KLOperators** se crean de la siguiente manera:

- Si la aplicación se instala con una cuenta de usuario incluida en un dominio, los grupos se crean en el dominio que incluye el Servidor de administración y en el propio Servidor de administración.
- Si la aplicación se instala con una cuenta de sistema, los grupos se crean solo en el Servidor de administración.

Puede ver los grupos **KLAdmins** y **KLOperators** y modificar los privilegios de acceso de los usuarios que pertenecen a los grupos **KLAdmins** y **KLOperators** utilizando las herramientas administrativas estándar del sistema operativo.

El grupo **KLAdmins** tiene todos los permisos de acceso; el grupo **KLOperators** únicamente tiene permisos de Lectura y Ejecución. Los permisos otorgados al grupo **KLAdmins** están bloqueados.

Los usuarios que pertenecen al grupo **KLAdmins** se denominan *administradores de Kaspersky Security Center*; los usuarios del grupo **KLOperators** se denominan *operadores de Kaspersky Security Center*.

Los derechos de administrador de Kaspersky Security Center no solo se otorgan a los usuarios incluidos en el grupo **KLAdmins**, sino que también se otorgan a los administradores locales de los equipos en los que está instalado el Servidor de administración.

Puede excluir a los administradores locales de la lista de usuarios que poseen permisos de administrador de Kaspersky Security Center.

Todas las operaciones iniciadas por los administradores de Kaspersky Administration Kit serán realizadas usando los permisos de la cuenta del Servidor de administración.

Se puede crear un grupo individual **KLAdmins** para cada Servidor de administración desde la red; el grupo tendrá los permisos necesarios para ese Servidor de administración únicamente.

Si equipos que pertenecen al mismo dominio están incluidos dentro de grupos de administración de diferentes Servidores de administración, el administrador del dominio es un administrador de Kaspersky Security Center para todos los grupos. El grupo **KLAdmins** es el mismo para estos grupos de administración; éste se crea durante la instalación del primer Servidor de administración. Todas las operaciones iniciadas por el administrador de Kaspersky Security Center se realizan utilizando los permisos de la cuenta del Servidor de administración para el cual se iniciaron dichas operaciones.

Una vez instalada la aplicación, un administrador de Kaspersky Security Center puede:

- modificar los permisos concedidos a los grupos **KLOperators**;
- conceder los permisos para acceder a la funcionalidad de Kaspersky Security Center a otros grupos de usuarios y usuarios individuales registrados en el equipo administrador;
- asignar permisos de acceso en cada grupo de administración.

El administrador de Kaspersky Security Center puede asignar permisos de acceso a cada grupo de administración o a otros objetos del Servidor de administración, en la sección **Seguridad** de la ventana de propiedades del objeto seleccionado.

Puede realizar un seguimiento de la actividad de usuario mediante los registros de eventos en el funcionamiento del Servidor de administración. Estos registros de eventos se muestran en el árbol de consola de la carpeta **Eventos**, en la subcarpeta **Eventos de auditoría**. Estos eventos tienen el nivel de seguridad **Información** y comienzan con la palabra **Auditoría**.

CONDICIONES DE CONEXIÓN A UN SERVIDOR DE ADMINISTRACIÓN A TRAVÉS DE INTERNET

Si un Servidor de administración es remoto, ubicado fuera de una red corporativa, los equipos cliente se conectan a este a través de la Internet. Para que los equipos cliente se conecten a un Servidor de administración a través de Internet, se deben cumplir los siguientes requisitos:

- Un Servidor de administración remoto debe poseer una dirección IP interna, mientras que los puertos entrantes 13000 y 14000 deben permanecer abiertos.
- Primero debe instalarse el Agente de red en los equipos cliente.
- Al instalar el Agente de red en equipos cliente, debe especificar la dirección IP externa del Servidor de administración remoto. Si se utiliza un paquete de instalación para la instalación, la dirección IP externa se debe especificar manualmente en las propiedades de este paquete, en la sección **Configuración**.
- Para usar el Servidor de administración remoto con el fin de administrar las aplicaciones y tareas de un equipo cliente, en la ventana de propiedades de ese equipo, en la sección **General**, seleccione la casilla **No desconectar del Servidor de administración**. Una vez que la casilla está seleccionada, espere a que el Servidor de administración esté sincronizado con el equipo cliente remoto. El número de equipos cliente que mantienen una conexión continua con un Servidor de administración remoto no puede superar los 100.

Para aumentar el rendimiento de las tareas generadas por un Servidor de administración remoto, puede abrir el puerto 15000 en un equipo cliente. En este caso, para ejecutar una tarea, el Servidor de administración envía un paquete especial al Agente de red a través del puerto 15000 sin esperar a que se complete la sincronización con el equipo cliente.

CONEXIÓN SEGURA CON SERVIDOR DE ADMINISTRACIÓN

El intercambio de datos entre los equipos cliente y el Servidor de administración, así como la conexión de la Consola al Servidor de administración, puede realizarse mediante el protocolo SSL (Secure Sockets Layer). El protocolo SSL puede identificar las partes que interactúan, cifrar los datos que se transfieren y protegerlos de las modificaciones durante la transferencia. El protocolo SSL usa claves públicas para autenticar las partes que interactúan y cifrar datos.

EN ESTA SECCIÓN:

Certificado del Servidor de administración 49

La autenticación del Servidor de administración durante la conexión del equipo cliente 49

Autenticación del Servidor de administración durante la conexión de la Consola 49

CERTIFICADO DEL SERVIDOR DE ADMINISTRACIÓN

La autenticación del Servidor de administración durante la conexión de la Consola de administración a este y el intercambio de datos con los equipos cliente está basado en el *Certificado del Servidor de administración*. El certificado también se usa para la autenticación cuando se establece una conexión entre los Servidores de administración patrón y esclavo.

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

El certificado del Servidor de administración solo se crea una vez: durante la instalación del Servidor. Si el certificado del Servidor de administración se pierde, para recuperarlo debe reinstalar el componente Servidor de administración y restaurar datos.

LA AUTENTICACIÓN DEL SERVIDOR DE ADMINISTRACIÓN DURANTE LA CONEXIÓN DEL EQUIPO CLIENTE

Cuando un equipo cliente se conecta al Servidor de administración por primera vez, el Agente de red del equipo cliente descarga una copia del certificado del Servidor de administración y lo almacena localmente.

Si instala el Agente de red en un equipo cliente localmente, puede seleccionar el certificado del Servidor de administración manualmente.

La copia descargada del certificado se utiliza para verificar los permisos del Servidor de administración durante las siguientes conexiones.

Durante futuras sesiones, el Agente de red solicita el certificado del Servidor de administración en cada conexión del equipo cliente al Servidor y lo compara con la copia local. Si las copias no coinciden, el equipo cliente no podrá acceder al Servidor de administración.

AUTENTICACIÓN DEL SERVIDOR DE ADMINISTRACIÓN DURANTE LA CONEXIÓN DE LA CONSOLA

Durante la primera conexión al Servidor de administración, la Consola de administración solicita el certificado del Servidor de administración y lo guarda localmente, en el equipo administrador. Después de ello, cada vez que la Consola de administración intenta conectarse con este Servidor de administración, este es identificado a partir de la copia del certificado.

Si el certificado del Servidor de administración no coincide con la copia almacenada en el equipo administrador, la Consola ofrece confirmar la conexión al Servidor con el nombre especificado y descargará un nuevo certificado. Una vez establecida la conexión, la Consola de administración guarda una copia del nuevo certificado del Servidor de administración, que será utilizada para identificar al Servidor en el futuro.

DESCONEXIÓN DE UN SERVIDOR DE ADMINISTRACIÓN

Para desconectarse de un Servidor de administración:

1. En el árbol de consola, seleccione el nodo correspondiente al Servidor de administración que se debe desconectar.
2. En el menú contextual del nodo, seleccione **Desconectarse del Servidor de administración**.

AGREGAR UN SERVIDOR DE ADMINISTRACIÓN AL ÁRBOL DE CONSOLA

Para agregar un nuevo Servidor de administración al árbol de consola:

1. En la ventana principal de Kaspersky Security Center, seleccione el nodo **Kaspersky Security Center** del árbol de consola.
2. En el menú contextual del nodo seleccione **Crear** → **Servidor de administración**.

Luego de ello, se creará un nodo denominado **Servidor de administración - <Nombre del equipo> (no conectado)** en el árbol de consola, desde el cual se podrá conectar a cualquier Servidor de administración de la red.

ELIMINAR UN SERVIDOR DE ADMINISTRACIÓN DEL ÁRBOL DE CONSOLA

Eliminar un Servidor de administración del árbol de consola:

1. En el árbol de consola, seleccione el nodo correspondiente al Servidor de administración que desea eliminar.
2. En el menú contextual del nodo seleccione **Eliminar**.

CAMBIO DE UNA CUENTA DE SERVICIO DEL SERVIDOR DE ADMINISTRACIÓN. UTILIDAD KLSRVSWCH

Si necesita cambiar la cuenta de servicio del Servidor de administración establecida al instalar Kaspersky Security Center, puede usar una utilidad denominada klsrvswch, diseñada para cambiar la cuenta del Servidor de administración.

Al instalar Kaspersky Security Center, la utilidad se copia automáticamente en la carpeta de instalación de la aplicación.

La cantidad de inicios de la utilidad es prácticamente ilimitada.

Para cambiar una cuenta de servicio del Servidor de administración:

1. Inicie la utilidad klsrvswch desde la carpeta de instalación de Kaspersky Security Center.

   Esta acción inicia también el asistente para la modificación de la cuenta de servicio del Servidor de administración. Siga las instrucciones del asistente.

2. En la ventana **Cuenta de servicio del Servidor de administración** seleccione cualquiera de las dos opciones para configurar una cuenta:

   - **Cuenta del sistema local**. El servicio del Servidor de administración se iniciará mediante la *Cuenta del sistema local*, utilizando sus credenciales.

     El funcionamiento correcto de Kaspersky Security Center requiere que la cuenta utilizada para iniciar el servicio del Servidor de administración posea los permisos de administrador del recurso donde se aloja la base de datos del Servidor de administración.

- **Cuenta de usuario**. El servicio del Servidor de administración se iniciará mediante la cuenta de un usuario dentro del dominio. En este caso, el Servidor de administración deberá iniciar todas las operaciones utilizando los permisos de esa cuenta.

  Para seleccionar el usuario cuya cuenta será utilizada para iniciar el servicio del Servidor de administración:

  1. Haga clic en el botón **Buscar ahora** y seleccione un usuario en la ventana **Seleccionar: "Usuario"** que se abrirá.

     Cierre la ventana **Seleccionar: "Usuario"** y haga clic en **Siguiente**.

  2. En la ventana **Contraseña de la cuenta** establezca una contraseña para la cuenta de usuario seleccionada, si es necesario.

Una vez que finalicen las operaciones del asistente, se modificará la cuenta del Servidor de administración.

Al usar un servidor SQL en un modo que presupone la autenticación de cuentas de usuario con herramientas de Microsoft Windows, debería otorgarse el acceso a la base de datos. El usuario debe contar con el estado del propietario de la base de datos de Kaspersky Anti-Virus. El esquema propietario de base de datos (dbo) se utiliza de forma predeterminada.

VISUALIZACIÓN Y MODIFICACIÓN DE LA CONFIGURACIÓN DE UN SERVIDOR DE ADMINISTRACIÓN

Puede ajustar la configuración de un Servidor de administración en la ventana de propiedades de este Servidor.

Para abrir la ventana Propiedades: Servidor de administración

seleccione **Propiedades** en el menú contextual del nodo del Servidor de administración en el árbol de consola.

EN ESTA SECCIÓN:

Ajuste de la configuración general del Servidor de administración 51
Configuración de parámetros de procesamiento de eventos 51
Control de focos de virus 52
Límite de tráfico 52
Configurar la cooperación con Cisco Network Admission Control (NAC) 52
Configurar el Servidor web 52
Interacción entre el Servidor de administración y el servicio de proxy de KSN 53
Trabajar con usuarios internos 53

AJUSTE DE LA CONFIGURACIÓN GENERAL DEL SERVIDOR DE ADMINISTRACIÓN

Puede ajustar la configuración general del Servidor de administración en **General**, **Configuración**, **Almacenamiento de eventos** y **Seguridad** de la ventana de propiedades del Servidor de administración.

El usuario puede determinar si la sección **Seguridad** se muestra o se oculta, mediante la configuración de la interfaz del usuario. Para mostrar esta sección, vaya a **Ver** → **Configurar interfaz** y en la ventana **Configurar interfaz** que se abre seleccione la casilla **Mostrar secciones de configuración de seguridad**.

CONFIGURACIÓN DE PARÁMETROS DE PROCESAMIENTO DE EVENTOS

Puede ver una lista de eventos que se producen durante el funcionamiento de las aplicaciones y configurar el procesamiento de eventos en la sección **Eventos** de la ventana de propiedades del Servidor de administración.

Cada evento tiene un atributo que indica el nivel de importancia. Los eventos del mismo tipo pueden tener diferentes niveles de gravedad según las condiciones en que ocurrió el evento.

CONTROL DE FOCOS DE VIRUS

Kaspersky Security Center le permite responder rápidamente a las amenazas emergentes de focos de virus. Los riesgos de los focos de virus se evalúan mediante el control de la actividad de virus en equipos cliente.

Puede configurar reglas de evaluación para amenazas de focos de virus y las medidas que se deben tomar en caso de que surja alguno. Para hacer esto, use la sección **Foco de virus** de la ventana de propiedades del Servidor de administración.

Puede especificar el procedimiento de notificación para el evento *Foco de virus* en la sección **Eventos** de la ventana de propiedades del Servidor de administración (ver la sección "Configuración del procesamiento de eventos" en la página 51), en la ventana de propiedades del evento *Foco de virus*.

El evento *Foco de virus* se genera en caso de que se detecten los eventos *Objeto malintencionado detectado* en el funcionamiento de las aplicaciones antivirus. Por lo tanto, debe guardar la información de todos los eventos *Objeto malintencionado detectado* en el Servidor de administración para reconocer los focos de virus.

Puede especificar la configuración para guardar la información acerca de los eventos *Objeto malintencionado detectado* en las directivas de las aplicaciones antivirus.

Al contar los eventos *Objeto infectado detectado*, solamente se tomará en cuenta la información de los equipos cliente del Servidor de administración maestro. La información de los Servidores de administración secundarios no se toma en cuenta. Para cada Servidor secundario, la configuración del evento *Foco de virus* se ajusta individualmente.

LÍMITE DE TRÁFICO

Para reducir los volúmenes de tráfico dentro de una red, la aplicación proporciona la opción de limitar la velocidad de transferencia de datos a un Servidor de administración desde los intervalos IP y subredes IP especificados.

Se pueden crear y configurar reglas de límite de tráfico en la sección **Tráfico** de la ventana de propiedades del Servidor de administración.

CONFIGURAR LA COOPERACIÓN CON CISCO NETWORK ADMISSION CONTROL (NAC)

Puede definir los vínculos de correspondencia entre condiciones de protección antivirus de los equipos cliente y los estados de seguridad de Cisco® Network Admission Control (NAC).

Para ello, debe crear las condiciones según las cuales se asignarán a los equipos cliente determinados estados de seguridad de Cisco® Network Admission Control (NAC): *Sin inconvenientes*, *Revisar*, *Cuarentena* o *Infectado*.

Puede configurar la correspondencia entre los estados de seguridad de Cisco® NAC y las condiciones de protección antivirus de equipos cliente en la sección **Cisco NAC** de la ventana de propiedades del Servidor de administración.

La sección **Cisco NAC** se muestra en la ventana de propiedades del Servidor de administración si el componente de validación de postura de Cisco® NAC de Kaspersky Lab se instaló junto con el Servidor de administración durante la instalación de la aplicación (para obtener más información, consulte la *Guía de implementación de Kaspersky Security Center*). Caso contrario, la sección **Cisco NAC** no se muestra en la ventana de propiedades del Servidor de administración.

CONFIGURAR EL SERVIDOR WEB

El Servidor Web está diseñado para publicar paquetes de instalación independientes, perfiles de MDM de iOS y archivos de la carpeta compartida.

Puede definir la configuración de la conexión del Servidor web al Servidor de administración y configurar un certificado de Servidor web en la sección **Servidor web** de la ventana de propiedades del Servidor de administración.

INTERACCIÓN ENTRE EL SERVIDOR DE ADMINISTRACIÓN Y EL SERVICIO DE PROXY DE KSN

El *proxy de KSN* es un servicio que asegura la interacción entre la infraestructura de Kaspersky Security Network y los equipos cliente administrados por un Servidor de administración.

El uso del proxy de KSN le proporciona las siguientes opciones:

- Los equipos cliente pueden enviar solicitudes a KSN y transferir información a KSN, incluso si no se tiene acceso directo a Internet.
- El proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga de trabajo en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un equipo cliente.

Puede configurar el proxy de KSN en la sección **Servidor proxy de KSN** de la ventana de propiedades del Servidor de administración.

TRABAJAR CON USUARIOS INTERNOS

Las cuentas de *usuarios internos* se utilizan para trabajar con Servidores de administración virtuales. Con la cuenta de un usuario interno, el administrador de un Servidor de administración interno puede iniciar Kaspersky Security Center Web Console para comprobar el estado de seguridad antivirus de una red. Kaspersky Security Center otorga los permisos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo para trabajar dentro de Kaspersky Security Center. No se transfiere ningún dato sobre usuarios internos al sistema operativo. Kaspersky Security Center autentica a los usuarios internos.

Puede configurar los parámetros de cuentas de usuarios internos en la sección **Usuarios internos** de la ventana de propiedades del Servidor de administración.

La sección **Usuarios internos** solo se muestra en la ventana de propiedades del Servidor de administración si el Servidor es virtual o contiene Servidores de administración virtuales.

ADMINISTRAR GRUPOS DE ADMINISTRACIÓN

Esta sección proporciona información sobre cómo manejar grupos de administración.

Se pueden realizar las siguientes acciones en los grupos de administración:

- agregar cualquier número de grupos anidados de cualquier nivel de jerarquía a los grupos de administración;
- agregar equipos cliente a los grupos de administración;
- cambiar la jerarquía de los grupos de administración moviendo los equipos cliente individuales y los grupos enteros a otros grupos;
- eliminar los grupos anidados y los equipos cliente de los grupos de administración;
- agregar Servidores de administración secundarios y virtuales a los grupos de administración;
- mover los equipos cliente de los grupos de administración de un Servidor de administración a los de otro Servidor;
- definir qué aplicaciones de Kaspersky Lab serán automáticamente instaladas en los equipos cliente incluidos en un grupo.

EN ESTA SECCIÓN:

Creación de grupos de administración 54

Traslado de grupos de administración 55

Eliminación de grupos de administración 56

Creación automática de la estructura de grupos de administración 56

Instalación automática de aplicaciones en equipos de un grupo de administración 57

CREACIÓN DE GRUPOS DE ADMINISTRACIÓN

La jerarquía de grupos de administración se crea en la ventana principal de la aplicación de Kaspersky Security Center, en la carpeta **Equipos administrados**. Los grupos de administración se muestran como carpetas en el árbol de consola (ver figura a continuación).

Inmediatamente después de la instalación de Kaspersky Security Center, la carpeta **Equipos administrados** contiene únicamente la carpeta **Servidores de administración**, que está vacía.

La configuración de la interfaz de usuario determina si la carpeta **Servidores de administración** aparece o no en el árbol de consola. Para mostrar esta sección, vaya a **Ver** → **Configuración de interfaz** y en la ventana **Configuración de interfaz** que se abre seleccione la casilla **Mostrar Servidores de administración esclavos**.

Al crear una jerarquía de grupos de administración, puede agregar equipos cliente y máquinas virtuales a la carpeta **Equipos administrados**, y también puede agregar grupos anidados. Puede agregar Servidores de administración secundarios a la carpeta **Servidores de administración**.

Al igual que con el **Equipos administrados**, cada grupo recién creado contiene solamente la carpeta **Servidores de administración**, que está vacía y que sirve para manejar los Servidores de administración secundarios de este grupo. La información sobre directivas, las tareas del grupo y los equipos incluidos se muestra en las pestañas correspondientes del espacio de trabajo de este grupo.

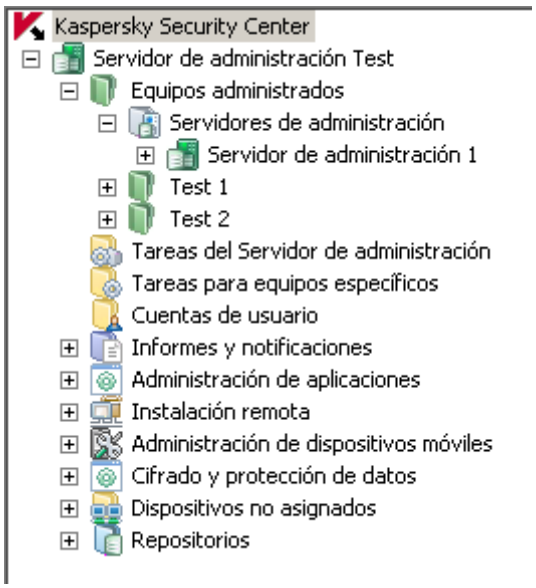


Figura 11. Ver jerarquía de grupos de administración

Para crear un grupo de administración:

1. Abra la carpeta **Equipos administrados** en el árbol de consola.
2. Si desea crear un subgrupo para un grupo de administración existente, en la carpeta **Equipos administrados** seleccione la carpeta anidada que corresponde al grupo, que debería incluir el nuevo grupo de administración.

   Puede omitir este paso si crea un nuevo grupo de administración de nivel superior.
3. Inicie el proceso de creación del grupo de administración de una de las siguientes formas:
   - Utilizando el comando **Crear** → **Grupo** del menú contextual.
   - Mediante un clic en el enlace **Crear un subgrupo** ubicado en el espacio de trabajo de la ventana principal de la aplicación, en la pestaña **Grupos**.
4. En la ventana **Nombre de grupo** que se abre, escriba un nombre para el grupo y haga clic en el botón **Aceptar**.

Como resultado, aparece una nueva carpeta de grupo de administración con el nombre especificado en el árbol de consola.

TRASLADO DE GRUPOS DE ADMINISTRACIÓN

Puede mover grupos de administración anidados dentro de la jerarquía de grupos.

Un grupo de administración se mueve junto con todos sus grupos secundarios, Servidores de administración secundarios, equipos cliente, directivas de grupo y tareas. El sistema aplicará al grupo toda la configuración correspondiente a su nueva posición en la jerarquía de los grupos de administración.

El nombre del grupo debe ser único dentro de un nivel de la jerarquía. Si ya existe un grupo con el mismo nombre en la carpeta a la que se mueve el grupo de administración, debe cambiar el nombre de este último. Si no cambió el nombre del grupo, una vez que se movió se agrega un formato de índice **_<número de serie>** al nombre, por ejemplo: **(1)**, **(2)**.

No se puede cambiar el nombre a la carpeta **Equipos administrados** porque es un elemento integrado de la Consola de administración.

Para mover un grupo a otra carpeta del árbol de consola:

1. Seleccione un grupo para mover desde el árbol de consola.
2. Realice una de las siguientes acciones:
   - Mueva el grupo mediante el menú contextual:
     1. Seleccione **Cortar** en el menú contextual del grupo.
     2. Seleccione **Pegar** en el menú contextual del grupo de administración al que necesita mover el grupo seleccionado.
   - Mueva el grupo mediante el menú principal de la aplicación:
     a. Seleccione **Acción** → **Cortar** en el menú principal;
     b. En el árbol de consola, seleccione el grupo de administración al que necesita mover el grupo seleccionado.
     c. Seleccione **Acción** → **Pegar** en el menú principal.
   - Con el mouse, mueva el grupo a otro en el árbol de consola.

ELIMINACIÓN DE GRUPOS DE ADMINISTRACIÓN

Se puede eliminar un grupo de administración si no contiene Servidores de administración secundarios, grupos anidados o equipos cliente y si no se han creado tareas o directivas de grupo.

Antes de eliminar el grupo de administración, debe eliminar todos los Servidores de administración secundarios, grupos anidados y equipos cliente de ese grupo.

Para eliminar un grupo:

1. Seleccione un grupo de administración del árbol de consola.
2. Realice una de las siguientes acciones:
   - Seleccione **Eliminar** en el menú contextual del grupo.
   - Seleccione **Acción** → **Eliminar** del menú principal de la aplicación.
   - Presione la tecla **Supr**.

CREACIÓN AUTOMÁTICA DE LA ESTRUCTURA DE GRUPOS DE ADMINISTRACIÓN

Kaspersky Security Center permite crear una estructura de grupos de administración mediante el Asistente de nueva estructura para un grupo de administración.

El Asistente crea una estructura de grupos de administración basada en los siguientes datos:

- estructuras de dominios y grupos de trabajo Windows;
- estructuras de grupos del Active Directory;
- contenido de un archivo de texto creado manualmente por el administrador.

Al generar el archivo de texto, se deben cumplir los siguientes requisitos:

- El nombre de cada grupo nuevo debe comenzar con una nueva línea; y el separador debe comenzar con un fin de línea. Se ignoran las líneas en blanco.

Por ejemplo:

Oficina 1

Oficina 2

Oficina 3

Se deben crear tres grupos del primer nivel de jerarquía en el grupo de destino.

- El nombre del grupo anidado se debe ingresar con una barra diagonal (/).

Por ejemplo:

Oficina 1/División 1/Departamento 1/Grupo 1

Se crearán cuatro subgrupos anidados en cada uno, en el grupo de destino.

- Para crear varios grupos anidados del mismo nivel de jerarquía, debe especificar la "ruta completa al grupo".

Por ejemplo:

Oficina 1/División 1/Departamento 1

Oficina 1/División 2/Departamento 1

Oficina 1/División 3/Departamento 1

Oficina 1/División 4/Departamento 1

Un grupo de la Oficina 1 del primer nivel de jerarquía deberá ser creado en el grupo de destino. Este grupo incluirá cuatro grupos anidados del mismo nivel de jerarquía: "División 1", "División 2", "División 3" y "División 4". Cada uno de estos grupos incluirá el grupo "Departamento 1".

Si utiliza el Asistente para crear la estructura de los grupos de administración, se preservará la integridad de la red: los nuevos grupos no reemplazan a los grupos existentes. Un equipo cliente no puede volver a incluirse en un grupo de administración, ya que se eliminó del grupo **Equipos no asignados** luego de que el equipo cliente se movió al grupo de administración.

Si, al crear una estructura de grupos de administración, un equipo cliente no se incluyó en el grupo **Equipos no asignados** por cualquier motivo (se cerró o se perdió la conexión de red), no se moverá automáticamente al grupo de administración. Puede agregar manualmente equipos cliente a los grupos de administración luego de que el Asistente concluya su operación.

Para iniciar la creación automática de una estructura de grupos de administración:

1. Seleccione la carpeta **Equipos administrados** en el árbol de consola.
2. Abra el menú contextual del nodo **Equipos administrados** y seleccione **Todas las tareas** → **Crear estructura de grupos**.

Como resultado, se iniciará el Asistente de nueva estructura de grupos de administración. Siga las instrucciones del asistente.

INSTALACIÓN AUTOMÁTICA DE APLICACIONES EN EQUIPOS DE UN GRUPO DE ADMINISTRACIÓN

Puede especificar qué paquetes de instalación deben ser utilizados para la instalación remota automática de aplicaciones Kaspersky Lab a los equipos cliente que hayan sido agregados al grupo recientemente.

Para configurar la instalación automática de las aplicaciones en dispositivos nuevos de un grupo de administración:

1. En el árbol de consola, seleccione el grupo de administración requerido.
2. Abra la ventana de propiedades de este grupo de administración.
3. En la sección **Instalación automática**, seleccione los paquetes de instalación que se instalarán en los nuevos equipos, al seleccionar las casillas de verificación que se encuentran junto a los nombres de los paquetes de instalación de las aplicaciones requeridas. Haga clic en **Aceptar**.

Como resultado, se crearán las tareas de grupo que se ejecutarán en los equipos cliente inmediatamente después de que se hayan agregado al grupo de administración.

Si se seleccionaran varios paquetes de instalación de una aplicación para la instalación automática, la tarea de instalación se creará solamente para la versión más reciente de la aplicación.

ADMINISTRACIÓN DE LAS APLICACIONES DE FORMA REMOTA

Esta sección ofrece información sobre cómo realizar la administración remota de las aplicaciones de Kaspersky Lab instaladas en equipos cliente mediante el uso de directivas, perfiles de directivas, tareas y la configuración local de las aplicaciones.

EN ESTA SECCIÓN:

Administrar directivas 58

Administración de perfiles de directivas 61

Administración de tareas 64

Ver y modificar la configuración local de la aplicación 70

ADMINISTRAR DIRECTIVAS

Las aplicaciones instaladas en los equipos cliente se configuran de modo centralizado a través de la definición de directivas.

Las directivas creadas para las aplicaciones de un grupo de administración se muestran en el espacio de trabajo de la pestaña **Directivas**. Delante del nombre de cada directiva, se muestra un icono con su estado.

Después de eliminar o revocar una directiva, la aplicación continúa trabajando con la configuración especificada en la directiva. Posteriormente, esa configuración se puede modificar manualmente.

La aplicación de las directivas se realiza de la siguiente forma: si un equipo cliente está ejecutando tareas residentes (tareas de protección en tiempo real), estas continúan ejecutándose con los nuevos valores de la configuración. Cualquier tarea periódica (análisis a petición, actualización de bases de datos de la aplicación) que haya comenzado se seguirá ejecutando con los valores sin modificar. La siguiente vez que se ejecuten usarán los valores nuevos de la configuración.

Si los Servidores de administración tienen una estructura jerárquica, los Servidores secundarios reciben directivas del Servidor de administración maestro y las distribuyen a los equipos cliente. Cuando está habilitada la herencia, la configuración de la directiva se puede modificar en el Servidor de administración maestro. Luego de ello, cualquier cambio realizado a la configuración de la directiva se propaga a las directivas heredadas de los Servidores de administración secundarios.

Si finaliza la conexión entre los Servidores de administración maestro y secundario, la directiva en el Servidor secundario seguirá usando la configuración aplicada. La configuración de la directiva modificada en el Servidor de administración maestro se distribuye a un Servidor secundario una vez restablecida la conexión.

Si se deshabilita la herencia, la configuración de la directiva se puede modificar en un Servidor de administración secundario, independientemente del Servidor maestro.

Si se interrumpe la conexión entre el Servidor de administración y el equipo cliente, dicho equipo cliente comienza a funcionar con la directiva para usuarios móviles (si está definida) o la directiva se sigue ejecutando según la configuración aplicada hasta que se restablece la conexión.

Los resultados de la distribución de directivas en el Servidor de administración secundario se muestran en la ventana de propiedades de la directiva en la consola del Servidor de administración maestro.

Los resultados de la propagación de directivas en equipos cliente se muestran en la ventana de propiedades de la directiva del Servidor de administración al que están conectados.

EN ESTA SECCIÓN:

Crear una directiva 59

Mostrar directiva heredada en un subgrupo 59

Activar una directiva 59

Activar una directiva automáticamente en el evento de foco de virus 60

Implementación de una directiva fuera de la oficina 60
Eliminar una directiva 60
Copiar una directiva 60
Exportación de una directiva 61
Importación de una directiva 61
Convertir directivas 61

CREACIÓN DE DIRECTIVAS

Para crear una directiva para un grupo de administración:

1. En el árbol de consola, seleccione el grupo de administración para el que desea crear una directiva.
2. En el espacio de trabajo para el grupo, seleccione la pestaña **Directivas** y haga clic en el enlace **Crear una directiva** para ejecutar el Asistente para nueva directiva.

Se iniciará el Asistente para nueva directiva. Siga las instrucciones del asistente.

Puede crear varias directivas para una aplicación desde el grupo; no obstante, solo una directiva puede estar activa por vez. Cuando se crea una nueva directiva activa, la directiva activa anterior pasa a estar inactiva.

Cuando se crea una directiva, puede especificar un conjunto mínimo de parámetros requeridos para el funcionamiento correcto de la aplicación. El resto de los valores se establecen en los valores predeterminados aplicados en la instalación local de la aplicación. Puede modificar la directiva una vez que está creada.

La configuración de las aplicaciones Kaspersky Lab modificada luego de aplicar las directivas se describe en detalle en las guías respectivas.

Una vez creada la directiva, la configuración con modificación prohibida (marcada con un "bloqueo") entran en vigencia en los equipos cliente sin importar qué configuración se especificó anteriormente para la aplicación.

MOSTRAR DIRECTIVA HEREDADA EN UN SUBGRUPO

Para habilitar la visualización de directivas heredadas para un grupo de administración heredado:

1. En el árbol de consola, seleccione el grupo de administración para el que se deben mostrar las directivas heredadas.
2. En el espacio de trabajo del grupo seleccionado, seleccione la pestaña **Directivas**.
3. En el menú contextual de la lista de directivas, seleccione **Ver** → **Directivas heredadas**.

Como resultado, las directivas heredadas se muestran en la lista de directivas con el icono (icono claro). Cuando está habilitado el modo de herencia de configuración, la modificación de las directivas heredadas solo está disponibles en el grupo en que se crearon. La modificación de esas directivas heredadas no está disponible en el grupo que las hereda.

ACTIVAR UNA DIRECTIVA

Para activar una directiva para el grupo seleccionado:

1. En el espacio de trabajo del grupo, en la pestaña **Directivas** seleccione la directiva que necesita activar.
2. Para activar la directiva, realice una de las siguientes acciones:
   - En el menú contextual de la directiva, seleccione **Directiva activa**.
   - En la ventana de propiedades de la directiva, abra la sección **General** y seleccione **Directiva activa** en el grupo de configuración **Estado de la directiva**.

Como resultado, la directiva pasa a estar activa para el grupo de administración seleccionado.

Cuando se aplica una directiva a un gran número de clientes, tanto la carga en el Servidor de administración como el tráfico de red aumentarán significativamente para un período de tiempo.

ACTIVAR UNA DIRECTIVA AUTOMÁTICAMENTE EN EL EVENTO DE FOCO DE VIRUS

Para que una directiva realice la activación automática ante el evento Foco de virus:

1. En la ventana de propiedades del Servidor de administración, abra la sección **Foco de virus**.
2. Abra la ventana **Activación de directiva** mediante un clic en el enlace **Configurar directivas para activar en el evento "Foco de Virus"** y agregue la directiva a la lista seleccionada de directivas activadas al detectar un foco del virus.

Si se activó una directiva en el evento de *Foco de virus*, el modo manual es la única forma en que puede regresar a la directiva anterior.

IMPLEMENTACIÓN DE UNA DIRECTIVA FUERA DE LA OFICINA

Una directiva fuera de la oficina entra en vigencia en un equipo en el caso de que dicho equipo se desconecte de la red empresarial.

Para aplicar la directiva fuera de la oficina seleccionada,

en la ventana de propiedades de la directiva, abra la sección **General** y seleccione **Directiva fuera de la oficina** en el grupo de configuración **Estado de la directiva**.

Como resultado, la directiva se aplica a los equipos en el caso de que se desconecten de la red empresarial.

ELIMINAR UNA DIRECTIVA

Para eliminar una directiva:

1. En el espacio de trabajo de un grupo, en la pestaña **Directivas** seleccione la directiva que debe eliminar.
2. Elimine la directiva mediante uno de los siguientes métodos:
   - Seleccione **Eliminar** en el menú contextual de la directiva.
   - Con un clic en el enlace **Eliminar directiva** ubicado en el espacio de trabajo, en la sección diseñada para manipular la directiva seleccionada.

COPIAR UNA DIRECTIVA

Para copiar una directiva:

1. En el espacio de trabajo del grupo requerido, en la pestaña **Directivas**, seleccione una directiva.
2. En el menú contextual de la directiva, seleccione **Copiar**.
3. En el árbol de consola, seleccione un grupo para el cual desea agregar la directiva.

   Puede agregar la directiva al grupo desde el cual se copió.
4. En el menú contextual de la lista de directivas para el grupo seleccionado, en la pestaña **Directivas** seleccione **Pegar**.

Como resultado, la directiva se copiará con toda su configuración y se implementará en los equipos del grupo en el que se la copió. Si pega la directiva en el mismo grupo en que se copió, el índice **(<número de secuencia>)** se agrega automáticamente al nombre de la directiva: **(1)**, **(2)**.

Una directiva activa pasa a estar inactiva mientras se copia. Si es necesario, se puede activar.

EXPORTACIÓN DE UNA DIRECTIVA

Para exportar una directiva:

1. Exporte una directiva de una de las siguientes formas:
   - Seleccione **Todas las tareas** → **Exportar** en el menú contextual de la directiva.
   - Con un clic en el enlace **Exportar directiva a archivo** ubicado en el espacio de trabajo, en la sección diseñada para manipular la directiva seleccionada.
2. En la ventana **Guardar como** que se abrirá, especifique el nombre del archivo de la directiva y la ruta para guardarlo. Haga clic en el botón **Guardar**.

IMPORTACIÓN DE UNA DIRECTIVA

Para importar una directiva:

1. En el espacio de trabajo del grupo requerido, en la pestaña **Directivas**, seleccione uno de los siguientes métodos para importar directivas:
   - Seleccione **Todas las tareas** → **Importar** en el menú contextual de la lista de directivas.
   - Con un clic en el enlace **Importar directiva desde archivo** en el bloque de administración de la lista de directivas.
2. En la ventana que se abrirá, especifique la ruta al archivo desde el cual desea importar una directiva. Haga clic en el botón **Abrir**.

A continuación, la directiva se muestra en la lista de directivas.

Si ya está incluida una directiva con un nombre que coincide con el de la directiva importada en la lista de directivas, el nombre de la directiva importada se expandirá con un sufijo **(<siguiente número>)**, por ejemplo: **(1)**, **(2)**.

CONVERTIR DIRECTIVAS

Kaspersky Security Center puede convertir las directivas de versiones anteriores de aplicaciones Kaspersky Lab en directivas de versiones actualizadas de las mismas aplicaciones.

La conversión está disponible para directivas de las siguientes aplicaciones:

- Kaspersky Anti-Virus 6.0 para Windows Workstations MP4
- Kaspersky Endpoint Security 8 para Windows
- Kaspersky Endpoint Security 10 para Windows

Para convertir directivas:

1. En el árbol de consola seleccione el Servidor de administración para el que desea convertir directivas.
2. En el menú contextual del Servidor de administración, seleccione **Todas las tareas** → **Asistente de conversión de directivas y tareas**.

Esto iniciará el Asistente de conversión de directivas y tareas. Siga las instrucciones del asistente.

Luego de que finalice la operación del asistente, se crearán nuevas directivas que utilizan la configuración de directivas de versiones anteriores de aplicaciones Kaspersky Lab.

ADMINISTRACIÓN DE PERFILES DE DIRECTIVAS

En esta sección se proporciona información sobre los perfiles de directivas que se usan para la administración eficaz de grupos de equipos cliente. Se describen las ventajas de los perfiles de directivas, así como las formas de aplicarlos. En esta sección también se proporcionan instrucciones sobre cómo crear, configurar y eliminar perfiles de directivas.

ACERCA DE LOS PERFILES DE DIRECTIVAS

Un perfil de directiva es un conjunto designado de parámetros variables de una directiva que se activa en un equipo cliente cuando se cumplen condiciones específicas. La activación de un perfil modifica la configuración de la directiva que había estado activa en el equipo antes de que se active el perfil. Dicha configuración tomará los valores que se habían especificado en el perfil.

Los perfiles de directiva solo son compatibles con Kaspersky Endpoint Security 10 para Windows y Kaspersky Mobile Device Management 10 Service Pack 1.

Ventajas de los perfiles de directivas

Los perfiles de directivas simplifican la administración de los equipos cliente que usan directivas:

- Los perfiles contienen solo los parámetros que difieren de la directiva básica.
- No es necesario que mantenga y aplique manualmente varias instancias de una sola directiva que difiera solamente en unos pocos parámetros.
- No es necesario que asigne una directiva fuera de la oficina individual a usuarios.
- Los perfiles de directivas nuevos son fáciles de crear, ya que están admitidas la exportación e importación de perfiles, así como la creación de perfiles nuevos basados en los existentes por medio del copiado.
- Puede haber varios perfiles de directivas activos en un solo equipo cliente al mismo tiempo.
- La jerarquía de directivas está admitida.

Reglas de activación del perfil. Prioridades de los perfiles

Un perfil de directiva se activa en un equipo cliente cuando se desencadena una regla de activación. Una regla de activación puede contener las siguientes condiciones:

- El Agente de red de un equipo cliente se conecta al servidor con un conjunto de parámetros de conexión, como el número de puerto, la dirección del servidor, etc.
- El equipo cliente está funcionando en modo independiente.
- Al equipo cliente se le han asignado etiquetas específicas.
- El equipo cliente está ubicado en una unidad específica de Active Directory®; el equipo o su propietario están ubicados en un grupo de seguridad de Active Directory.

Los perfiles que se han creado para una directiva están ordenados de forma descendente por prioridad. Si el perfil *X* precede al perfil *Y* en la lista de perfiles, significa que *X* tiene mayor prioridad que *Y*. Las prioridades de los perfiles son necesarias porque puede haber varios perfiles activos en un equipo cliente al mismo tiempo.

Directivas en la jerarquía de los grupos de administración

Si bien las directivas se influyen mutuamente de acuerdo con la jerarquía de los grupos de administración, los perfiles con nombres idénticos se combinan. Los perfiles de una directiva "más alta" tienen una prioridad más alta. Por ejemplo, en el grupo de administración *A*, la directiva *P(A)* tiene los perfiles *X1*, *X2* y *X3* (en orden descendente de prioridad). En el grupo de administración *B*, que es un subgrupo del grupo *A*, la directiva *P(B)* se ha creado con los perfiles *X2*, *X4*, *X5*. Por lo tanto, la directiva *P(B)* se modificará junto con la directiva *P(A)*, de modo que la lista de perfiles en la directiva *P(B)* se verá así: *X1*, *X2*, *X3*, *X4*, *X5* (en orden descendente de prioridad). La prioridad del perfil *X2* dependerá del estado inicial de *X2* de la directiva *P(B)* y *X2* de la directiva *P(A)*.

La directiva activa es la suma de la directiva principal y todos los perfiles activos de esa directiva, es decir, los perfiles para los que se desencadenan las reglas de activación. La directiva activa se vuelve a calcular cuando inicia el Agente de red, habilita y deshabilita el modo fuera de la oficina o edita la lista de etiquetas asignadas al equipo cliente.

Propiedades y restricciones de los perfiles de directivas

Los perfiles tienen las siguientes propiedades:

- Los perfiles de una directiva inactiva no afectan los equipos cliente.
- Si una directiva está activa en el modo independiente, los perfiles de esa directiva también se aplicarán en modo independiente únicamente.
- Los perfiles no admiten el análisis estático del acceso a los archivos ejecutables.

- Una directiva no puede contener parámetros de notificación.
- Si el puerto UDP 15000 se usa para conectar un equipo cliente al Servidor de administración, debe activar el perfil de directiva correspondiente en el término de un minuto cuando asigna una etiqueta al equipo cliente.
- Cuando crea reglas de activación del perfil, puede usar reglas de conexión entre el Agente de red y el Servidor de administración.

CREAR UN PERFIL DE DIRECTIVA

La creación de perfiles de directivas solo está disponible para las directivas de Kaspersky Endpoint Security 10 para Windows.

Para crear un perfil de directiva para un grupo de administración:

1. En el árbol de consola, seleccione el grupo de administración para el que desea crear un perfil de directiva.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. Seleccione una directiva y cambie a la ventana de propiedades de la directiva usando el menú contextual.
4. Abra la sección **Perfil de directiva** en la ventana de propiedades de la directiva y haga clic en el botón **Agregar**.
5. En la ventana **Propiedades: Perfil nuevo**, configure el perfil de la directiva:
   - En la sección **General**, especifique el nombre del perfil.

     El nombre de un perfil no puede contener más de 100 caracteres.
   - Habilite o deshabilite el perfil usando la casilla **Habilitar perfil**.

     Si esta casilla está desactivada, el perfil no se puede usar para administrar el equipo cliente.
6. En la sección **Reglas de activación**, cree reglas de activación para el perfil.
   - Haga clic en el botón **Agregar**.
   - Defina las reglas de activación del perfil de directiva en la ventana **Propiedades:** Ventana **Nueva regla**.
   - Haga clic en **Aceptar**.
7. Edite la configuración de la directiva en las secciones correspondientes.
8. Después de que se haya configurado el perfil y se hayan creado las reglas de activación, guarde los cambios haciendo clic en el botón **Aceptar**.

Como resultado, se guardará el perfil. El perfil se activará en el equipo cliente cuando se desencadenen las reglas de activación.

Los perfiles que se han creado para una directiva se muestran en las propiedades de la directiva, en la sección **Perfiles de directivas**. Puede modificar un perfil de directiva y cambiar la prioridad del perfil (consulte la sección "Editar un perfil de directiva" en la página 63), como así también eliminar el perfil (consulte la sección "Eliminar un perfil de directiva" en la página 64).

Se pueden activar varios perfiles de directivas al mismo tiempo cuando se desencadenan las reglas de activación.

MODIFICAR UN PERFIL DE DIRECTIVA

Editar la configuración de un perfil de directiva

La edición de perfiles de directivas solo está disponible para las directivas de Kaspersky Endpoint Security 10 para Windows.

Para modificar un perfil de directiva:

1. En el árbol de consola, seleccione el grupo de administración para el que se debe modificar el perfil de directiva.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. Seleccione una directiva y cambie a la ventana de propiedades de la directiva usando el menú contextual.

4. Abra la sección **Perfil de directiva** en las propiedades de la directiva.

   Esta sección contiene una lista de perfiles que se han creado para la directiva. Los perfiles se muestran en la lista de acuerdo con sus prioridades.

5. Seleccione un perfil de directiva y haga clic en el botón **Propiedades**.
6. Configure el perfil en la ventana de propiedades.
   - Si es necesario, en la sección **General**, cambie el nombre del perfil, y habilite o deshabilite el perfil usando la casilla **Habilitar perfil**.
   - En la sección **Reglas de activación**, edite las reglas de activación del perfil.
   - Edite la configuración de la directiva en las secciones correspondientes.
7. Haga clic en **Aceptar**.

La configuración que ha modificado se aplicará ya sea después de que el equipo cliente se sincronice con el Servidor de administración (si el perfil de directiva está activo) o después de que se desencadene la activación de la regla (si el perfil de directiva está inactivo).

Cambiar la prioridad de un perfil de directiva

Las prioridades de los perfiles de directivas definen el orden de activación de los perfiles en un equipo cliente. Las prioridades se usan si se establecen reglas de activación idénticas para diferentes perfiles de directivas.

Por ejemplo, se han creado dos perfiles de directivas: *Perfil 1* y *Perfil 2,* que difieren en los valores respectivos de un solo parámetro (*Valor 1* y *Valor 2)*. La prioridad del *Perfil 1* es más alta que la del *Perfil 2*. Además, también hay perfiles con prioridades más bajas que la del *Perfil 2*. Las reglas de activación de esos perfiles son idénticas.

Cuando se desencadena una regla de activación, se activará el *Perfil 1*. El parámetro en el equipo cliente tomará el *Valor 1*. Si elimina el *Perfil 1,* el *Perfil 2* tendrá la prioridad más alta y el parámetro tomará el *Valor 2*.

En la lista de perfiles de directivas, los perfiles se muestran de acuerdo con sus prioridades respectivas. El perfil con la prioridad más alta ocupa el primer lugar. Puede cambiar la prioridad de un perfil usando los siguientes botones:  y  .

ELIMINAR UN PERFIL DE DIRECTIVA

Para eliminar un perfil de directiva:

1. En el árbol de consola, seleccione el grupo de administración para el que desea eliminar un perfil de directiva.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. Seleccione una directiva y cambie a la ventana de propiedades de la directiva usando el menú contextual.
4. Abra la sección **Perfil de directiva** en las propiedades de la directiva de Kaspersky Endpoint Security 10 para Windows.
5. Seleccione el perfil de directiva que desea eliminar y haga clic en el botón **Eliminar**.

Como resultado, se eliminará el perfil de la directiva. El estado activo se transferirá a otro perfil de directiva cuyas reglas de activación se desencadenan en el equipo cliente, o a la directiva.

ADMINISTRACIÓN DE TAREAS

Kaspersky Security Center administra la aplicación instalada en equipos cliente mediante la creación y ejecución de tareas. Las tareas se requieren para instalar, iniciar y detener aplicaciones, escanear archivos, actualizar bases de datos y módulos de software y para realizar otras acciones en las aplicaciones.

Las tareas se subdividen en los siguientes tipos:

- *Tareas de grupo*. Tareas que se realizan en equipos cliente del grupo de administración seleccionado.
- *Tareas del Servidor de administración*. Tareas que se realizan en el Servidor de administración.
- *Tareas para equipos específicos*. Tareas que se realizan en equipos seleccionados, sin importar si están o no incluidos en algún grupo de administración.
- *Tareas locales*. Tareas que se realizan en un equipo cliente individual.

Una tarea de la aplicación solo se puede crear si el complemento de administración para esa aplicación está instalado en el equipo administrador.

Puede compilar una lista de equipos para la que se debe crear una tarea, mediante uno de los métodos siguientes:

- Seleccionar equipos detectados por el Servidor de administración en la red.
- Especificar manualmente una lista de equipos. Puede utilizar como dirección del equipo una dirección IP (o un intervalo de direcciones IP), un nombre NetBIOS o un nombre DNS.
- Importar una lista de equipos desde un archivo TXT que contenga las direcciones de los equipos que se agregarán (cada dirección debe colocarse en una línea individual).

  Si importa una lista de equipos desde un archivo o crea una manualmente, y se identifican los equipos cliente por sus nombres, la lista debe incluir solamente equipos para los que ya se ha agregado información a la base de datos del Servidor de administración durante la conexión de los equipos o durante un sondeo de red.

Para cada aplicación puede crear cualquier cantidad de tareas de grupo, tareas para equipos específicos o tareas locales.

El intercambio de información acerca de las tareas entre una aplicación instalada en un equipo cliente y la base de datos de Kaspersky Security Center se lleva a cabo apenas se conecta el Agente de red al Servidor de administración.

Puede realizar cambios a la configuración de tareas, ver el progreso, copiarlas, exportarlas, importarlas y eliminarlas.

Las tareas se inician en un cliente solo si la aplicación para la que se creó está en ejecución. Cuando la aplicación no está en ejecución, se anulan todas las tareas en curso

Los resultados de las tareas ejecutadas se guardan en el registro de eventos de Microsoft Windows y Kaspersky Security Center (también de modo centralizado en el Servidor de administración, y de modo local en cada equipo cliente).

CREAR UNA TAREA DE GRUPO

Para crear una tarea de grupo:

1. En el espacio de trabajo del grupo de administración para el que necesita crear una tarea, seleccione la pestaña **Tareas**.
2. Ejecute la creación de la tarea con un clic en el enlace **Crear una tarea**.

Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente.

CREAR UNA TAREA DEL SERVIDOR DE ADMINISTRACIÓN

El Servidor de administración realiza las siguientes tareas:

- Distribución automática de informes
- Descarga de actualizaciones en el repositorio
- Copia de seguridad de los datos del servidor de administración
- Sincronización de Windows Update
- Creación de un paquete de instalación basado en la imagen del SO de un equipo de referencia

En un Servidor de administración virtual, solo se encuentran disponibles la tarea de entrega automática de informes y la tarea de creación de paquetes de instalación a partir de la imagen del SO del equipo de referencia. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas al Servidor de administración maestro. La copia de seguridad de los datos del Servidor virtual se realiza junto con la copia de seguridad de los datos del Servidor de administración maestro.

Para crear una tarea del Servidor de administración:

1. En el árbol de consola, seleccione la carpeta **Tareas del Servidor de administración**.
2. Comience a crear la tarea en una de las siguientes formas:
   - En el árbol de consola, en el menú contextual de la carpeta **Tareas del Servidor de administración**, seleccione **Nuevo** → **Tarea**.
   - Haga clic en el enlace **Crear una tarea** en el espacio de trabajo.

Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente.

Las tareas **Descargar actualizaciones en el repositorio**, **Realizar la sincronización con Windows Update** y **Copia de seguridad de los datos del Servidor de administración** se pueden crear una sola vez. Si las tareas **Descargar actualizaciones en el repositorio**, **Realizar copia de seguridad de los datos del Servidor de administración** y **Realizar la sincronización de Windows Update** ya fueron creadas para el Servidor de administración, no se mostrarán en la selección del tipo de tarea del Asistente para nueva tarea.

CREACIÓN DE UNA TAREA PARA UN CONJUNTO DE EQUIPOS

En Kaspersky Security Center puede crear tareas para equipos específicos. Los equipos agrupados en un conjunto se pueden incluir en distintos grupos de administración o estar fuera de todos los grupos de administración. Kaspersky Security Center puede realizar las siguientes tareas principales:

- Instalar aplicación de forma remota (para obtener más información, consulte la *Guía de implementación de Kaspersky Security Center*).
- Enviar mensaje para usuario (ver sección “Enviar un mensaje a los usuarios de equipos cliente” en la página 78).
- Cambiar Servidor de administración (ver sección "Cambio del Servidor de administración para equipos cliente" en la página 77).
- Administrar equipo cliente (ver sección "Encendido, apagado y reinicio remoto de equipos cliente" en la página 78).
- Comprobar actualizaciones (ver sección "Comprobación de actualizaciones descargadas" en la página147).
- Distribuir paquete de instalación (para obtener más información, consulte la *Guía de implementación* de Kaspersky Security Center).
- Instalar la aplicación de forma remota en Servidores de administración secundarios (para obtener más información, consulte la *Guía de implementación de Kaspersky Security Center*).
- Desinstalar aplicación de forma remota (para obtener más información, consulte la *Guía de implementación de Kaspersky Security Center*).

Para crear una tarea para un conjunto de equipos:

1. En el árbol de consola seleccione la carpeta **Tareas para equipos específicos**.
2. Comience a crear la tarea en una de las siguientes formas:
   - En el menú contextual de la carpeta del árbol de consola denominada **Tareas para equipos específicos**, seleccione **Nuevo** → **Tarea**.
   - Haga clic en el enlace **Crear una tarea** en el espacio de trabajo.

Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente.

CREAR UNA TAREA LOCAL

Para crear una tarea local para un equipo cliente:

1. Seleccione la pestaña **Equipos** en el espacio de trabajo del grupo que incluye el equipo cliente.
2. En la lista de equipos de la pestaña **Equipos** seleccione el equipo para el que se debe crear una tarea local.
3. Comience a crear la tarea para el equipo seleccionado en una de las siguientes formas:
   - Haciendo clic en el enlace **Crear una tarea** en el espacio de trabajo del equipo.
   - En la ventana de propiedades del equipo, del siguiente modo:
     a. En el menú contextual del equipo, seleccione **Propiedades**.
     b. En la ventana de propiedades de equipo que se abre, seleccione la sección **Tareas** y haga clic en **Agregar**.

Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente.

Las instrucciones detalladas sobre cómo crear y configurar tareas locales se proporcionan en las guías de las aplicaciones Kaspersky Lab respectivas.

MOSTRAR UNA TAREA DE GRUPO HEREDADA EN EL ESPACIO DE TRABAJO DE UN GRUPO ANIDADO

Para habilitar la visualización de tareas heredadas de un grupo anidado en el espacio de trabajo:

1. Seleccione la pestaña **Tareas** en el espacio de trabajo de un grupo anidado.
2. Seleccione **Ver** → **Tareas heredadas** en el menú contextual de la lista de tareas.

Como resultado, las tareas heredadas se muestran en la lista de tareas con el icono  . Si está habilitado el modo de herencia de configuración, las tareas heredadas solo se pueden modificar en el grupo en que se crearon. Las tareas heredadas no se pueden modificar en el grupo que hereda las tareas.

INICIAR EQUIPOS CLIENTE AUTOMÁTICAMENTE ANTES DE INICIAR UNA TAREA

Kaspersky Security Center le permite ajustar la configuración de una tarea de modo que el sistema operativo comience a cargarse en equipos cliente, que están apagados, antes de que se inicie la tarea.

Para configurar el inicio automático de equipos cliente antes de iniciar una tarea:

1. En la ventana de propiedades de tareas, seleccione la sección **Programación**.
2. Abra la ventana correspondiente a la configuración de acciones en equipos cliente, haciendo clic en el enlace **Avanzado**.
3. En la ventana **Avanzado** que se abre, seleccione la casilla **Activar equipo antes de que la tarea se inicie con la función Wake On LAN (min.)** y especifique el intervalo de tiempo en minutos.

Como resultado, el sistema operativo comenzará a cargarse en equipos cliente, apagados, en el intervalo de tiempo especificado antes de que la tarea se inicie.

La carga automática del sistema operativo solo está disponible en equipos que admiten la característica Wake On Lan.

APAGAR EL EQUIPO UNA VEZ QUE SE HAYA COMPLETADO LA TAREA

Kaspersky Security Center permite ajustar la configuración de una tarea de modo que los equipos cliente a los que se aplica la tarea, se apague automáticamente una vez que se haya completado.

Para apagar los equipos cliente una vez que se haya completado la tarea:

1. En la ventana de propiedades de tareas, seleccione la sección **Programación**.
2. Abra la ventana correspondiente a la configuración de acciones en equipos cliente, haciendo clic en el enlace **Avanzado**.
3. En la ventana **Avanzado** que se abre, seleccione la casilla **Apagar el equipo una vez que se haya completado la tarea**.

LIMITAR EL TIEMPO DE EJECUCIÓN DE LA TAREA

Para limitar el tiempo de ejecución de la tarea en equipos cliente:

1. En la ventana de propiedades de tareas, seleccione la sección **Programación**.
2. Abra la ventana correspondiente a la configuración de acciones en equipos cliente, haciendo clic en el enlace **Avanzado**.
3. En la ventana **Avanzado** que se abre, marque la casilla **Detener si la tarea tarda más de (min.)** y especifique el intervalo de tiempo en minutos.

Como resultado, si la tarea no se ha completado al caducar el intervalo de tiempo especificado, Kaspersky Security Center detiene la ejecución de la tarea automáticamente.

EXPORTAR UNA TAREA

Puede exportar tareas de grupo y tareas para equipos específicos a un archivo. Las tareas del Servidor de administración y las tareas locales no están disponibles para exportación.

Para exportar una tarea:

1. Exporte la tarea mediante uno de los siguientes métodos:
   - Seleccionando **Todas las tareas** → **Exportar** en el menú contextual de la tarea.
   - Haciendo clic en el enlace **Exportar tarea a archivo** ubicado en el espacio de trabajo, en la sección diseñada para manipular la directiva seleccionada.
2. En la ventana **Guardar como** que se abrirá, especifique el nombre del archivo y la ruta para guardarlo. Haga clic en el botón **Guardar**.

Los permisos de los usuarios locales no se exportan.

IMPORTAR UNA TAREA

Puede importar tareas de grupo y tareas para equipos específicos. Las tareas del Servidor de administración y las tareas locales no están disponibles para importación.

Para importar una tarea:

1. Seleccione la lista de tareas a la que se debe importar la tarea:
   - Si desea importar la tarea a la lista de tareas de grupo, en el espacio de trabajo del grupo requerido seleccione la pestaña **Tareas**.
   - Si desea importar una tarea en la lista de tareas para equipos específicos, seleccione la carpeta **Tareas para equipos específicos** del árbol de consola.
2. Seleccione una de las siguientes opciones para importar la tarea:
   - En el menú contextual de la lista de tareas, seleccione **Todas las tareas** → **Importar**.
   - Haga clic en el enlace **Importar tarea desde archivo** en el bloque de administración de la lista de tareas.
3. En la ventana que se abrirá, especifique la ruta al archivo desde el cual desea importar una tarea. Haga clic en el botón **Abrir**.

A continuación, la tarea se muestra en la lista de tareas.

Si una tarea con el mismo nombre que la tarea importada ya se encuentra incluida en la lista seleccionada, se agregará un índice con el formato **(<número de serie>)** al nombre de la tarea importada, por ejemplo: **(1)**, **(2)**.

CONVERTIR TAREAS

Puede usar Kaspersky Security Center para convertir tareas de versiones anteriores de aplicaciones Kaspersky Lab en tareas de versiones actualizadas de las aplicaciones.

La conversión está disponible para tareas de las siguientes aplicaciones:

- Kaspersky Anti-Virus 6.0 para Windows Workstations MP4
- Kaspersky Endpoint Security 8 para Windows
- Kaspersky Endpoint Security 10 para Windows

Para convertir tareas:

1. En el árbol de consola seleccione el Servidor de administración para el que desea convertir tareas.
2. En el menú contextual del Servidor de administración, seleccione **Todas las tareas** → **Asistente de conversión de directivas y tareas**.

Esto iniciará el Asistente de conversión de directivas y tareas. Siga las instrucciones del asistente.

Luego de que finalice la operación del asistente, se crearán nuevas tareas que utilizan la configuración de tareas de versiones anteriores de las aplicaciones.

INICIAR Y DETENER UNA TAREA MANUALMENTE

Puede iniciar y detener tareas usando uno de los dos métodos siguientes: Desde el menú contextual de la tarea o en la ventana de propiedades del equipo cliente al que se ha asignado la tarea.

La ejecución de tareas de grupo desde el menú contextual de un equipo cliente está permitida para los usuarios incluidos en el **Grupo KLAdmins** (consulte la sección **"Derechos de acceso al Servidor de Administración y a sus objetos"** en la página 47).

- *Para iniciar o detener una tarea desde el menú contextual o la ventana de propiedades de la tarea, haga lo siguiente:*

  1. En la lista de tareas, seleccione una tarea.
  2. Inicie o detenga la tarea en una de las siguientes formas:
     - En el menú contextual de la tarea, seleccione **Iniciar** o **Detener**.
     - En la ventana de propiedades de tareas, en la sección **General**, haga clic en **Iniciar** o **Detener**.

- *Para iniciar o detener una tarea desde el menú contextual o la ventana de propiedades del equipo cliente, haga lo siguiente:*

  1. Seleccione un equipo de la lista de equipos.
  2. Inicie o detenga la tarea en una de las siguientes formas:
     - En el menú contextual del equipo cliente, seleccione **Todas las tareas** → **Ejecutar tarea**. Seleccione la tarea correspondiente de la lista de tareas.

       La lista de equipos a los que está asignada la tarea será reemplazada por el equipo que ha seleccionado. La tarea se inicia.

     - En la ventana de propiedades del equipo cliente, en la sección Tareas, haga clic en el botón  o  .

PAUSAR Y REANUDAR UNA TAREA MANUALMENTE

- *Para pausar o reanudar la ejecución de una tarea:*

  1. En la lista de tareas, seleccione una tarea.
  2. Pause o reanude la tarea mediante uno de los siguientes métodos:
     - En el menú contextual de la tarea, seleccione **Pausar** o **Reanudar**.
     - En la ventana de propiedades de tareas, seleccione la sección **General** y haga clic en **Pausar** o **Reanudar**.

SUPERVISAR LA EJECUCIÓN DE TAREAS

- *Para supervisar la ejecución de tareas,*

  seleccione la sección **General** de la ventana propiedades de tarea.

En la parte media de la sección **General**, se muestra el estado de la tarea actual.

VER RESULTADOS DE LA EJECUCIÓN DE TAREAS ALMACENADOS EN EL SERVIDOR DE ADMINISTRACIÓN

Kaspersky Security Center permite ver resultados de la ejecución para tareas de grupos, tareas para equipos específicos y tareas del Servidor de administración. No se pueden ver resultados de la ejecución para tareas locales.

- *Para ver resultados de tareas,*

  en la ventana propiedades de tareas, seleccione la sección **General** y haga clic en el enlace **Resultados** para abrir la ventana **Resultados de tarea**.

CONFIGURAR EL FILTRADO DE INFORMACIÓN SOBRE RESULTADOS DE LA EJECUCIÓN DE TAREAS

Kaspersky Security Center permite filtrar información sobre resultados de ejecución para tareas de grupos, tareas para equipos específicos y tareas del Servidor de administración. El filtrado no está disponible para tareas locales.

Para configurar el filtrado de información sobre resultados de ejecución de tareas:

1. En la ventana propiedades de tareas, seleccione la sección **General** y haga clic en el enlace **Resultados** para abrir la ventana **Resultados de tarea**.

   La tabla situada en la parte superior de la ventana contiene todos los equipos cliente para los que se asignó la tarea.

   La tabla situada en la parte inferior de la ventana muestra los resultados de la tarea realizada en el equipo cliente seleccionado.

2. En la ventana **Resultados de tarea** de la tabla requerida, seleccione el elemento **Filtro** del menú contextual.

3. En el ventana **Establecer filtro** que se abre, configure el filtro en las secciones **Eventos**, **Equipos** y **Hora**. Haga clic en **Aceptar**.

Como resultado, la ventana **Resultados de tarea** muestra información que coincide con la configuración especificada en el filtro.

VER Y MODIFICAR LA CONFIGURACIÓN LOCAL DE LA APLICACIÓN

El sistema de administración de Kaspersky Security Center permite la administración remota de la configuración local de la aplicación en equipos remotos a través de la Consola de administración.

La configuración local de la aplicación se refiere a la configuración de una aplicación, específica para un equipo cliente. Puede usar Kaspersky Security Center para especificar la configuración local de una aplicación en equipos cliente incluidos en los grupos de administración.

Las descripciones detalladas de la configuración de aplicaciones Kaspersky Lab se proporcionan en las guías respectivas.

Para ver o modificar la configuración local de la aplicación:

1. En el espacio de trabajo del grupo al que pertenece el equipo cliente requerido, seleccione la pestaña **Equipos**.

2. En la ventana de propiedades del equipo cliente, en la sección **Aplicaciones**, seleccione la aplicación requerida.

3. Abra la ventana de propiedades de la aplicación mediante doble clic en el nombre de la aplicación o con un clic en el botón **Propiedades**.

Como resultado, se abrirá la ventana de configuración local de la aplicación seleccionada, de modo que pueda ver y editar esa configuración.

Puede cambiar los valores de la configuración que no tienen prohibida la modificación mediante una directiva de grupo (es decir, aquellos valores no marcados con “bloqueo” en una directiva).

ADMINISTRACIÓN DE EQUIPOS CLIENTE

Esta sección proporciona información sobre cómo manejar equipos cliente.

EN ESTA SECCIÓN:

Conexión de equipos cliente al Servidor de administración 71
Conexión manual de un equipo cliente al Servidor de administración. Utilidad klmover 72
Creación de un túnel de conexión entre un equipo cliente y el Servidor de administración 73
Conexión remota al escritorio de un equipo cliente 73
Configurar el reinicio de un equipo cliente 74
Auditoría de acciones en un equipo cliente remoto 75
Comprobación de la conexión entre un equipo cliente y el Servidor de administración 75
Identificación de equipos cliente en el Servidor de Administración 76
Agregar equipos a un grupo de administración 77
Cambio del Servidor de administración para equipos cliente 77
Encendido, apagado y reinicio remoto de equipos cliente 78
Enviar un mensaje a los usuarios de equipos cliente 78
Controlar los cambios en el estado de las máquinas virtuales 79
Diagnóstico remoto de los equipos cliente. Utilidad de diagnóstico remoto de Kaspersky Security Center 79

CONEXIÓN DE EQUIPOS CLIENTE AL SERVIDOR DE ADMINISTRACIÓN

La conexión del equipo cliente al Servidor de administración se establece a través del Agente de red instalado en el equipo cliente.

Cuando un equipo cliente se conecta al Servidor de administración, se realizan las siguientes operaciones:

- Sincronización automática de datos:
  - sincronización de aplicaciones instaladas en un equipo cliente;
  - sincronización de las directivas, configuración de la aplicación, tareas y configuración de la tarea;
- Recuperación de información actualizada sobre la condición de las aplicaciones, ejecución de tareas y estadísticas de funcionamiento de aplicaciones a través del Servidor.
- Envío de la información sobre eventos al Servidor de administración para su procesamiento.

La sincronización automática de datos se realiza regularmente, de acuerdo con la configuración del Agente de red (por ejemplo, cada 15 minutos). Puede especificar el intervalo de conexión manualmente.

La información sobre un evento se envía al Servidor de administración inmediatamente después de producirse el evento.

Kaspersky Security Center permite configurar la conexión entre un equipo cliente y un Servidor de administración de modo que la conexión permanezca activa una vez que se completaron todas las operaciones. La conexión ininterrumpida es necesaria en casos en que se requiere el control en tiempo real del estado de la aplicación y el Servidor de administración no sea capaz de establecer una conexión con el cliente por algún motivo (conexión protegida por firewall, no se permite abrir puertos en el equipo cliente, dirección IP del cliente desconocida, etc.). Puede establecer una conexión continua entre un equipo cliente y el Servidor de administración en la sección **General** de la ventana de propiedades del equipo cliente.

Sólo se establecerá una conexión continua con los equipos cliente más importantes puesto que el Servidor de administración sólo admite un número limitado de conexiones simultáneas (varios cientos).

Al sincronizar manualmente, el sistema utiliza un método de conexión auxiliar, con el cual la conexión es iniciada por el Servidor de administración. Antes de establecer la conexión, debe abrir el puerto UDP. El Servidor de administración envía una solicitud de conexión al puerto UDP del equipo cliente. En respuesta, se verifica el certificado del Servidor de administración. Si el certificado del Servidor coincide con la copia del certificado almacenada en el equipo cliente, comienza a establecerse la conexión.

El inicio manual de la sincronización también se utiliza para obtener información actualizada sobre la condición de las aplicaciones, la ejecución de tareas y las estadísticas de operación de las aplicaciones.

CONEXIÓN MANUAL DE UN EQUIPO CLIENTE AL SERVIDOR DE ADMINISTRACIÓN. UTILIDAD KLMOVER

Si desea conectar un equipo cliente al Servidor de administración, puede utilizar la utilidad klmover del equipo cliente.

Al instalar el Agente de red en un equipo cliente, la utilidad se copia automáticamente a la carpeta de instalación del Agente de red.

Para conectar manualmente un equipo cliente al Servidor de administración mediante la utilidad klmover,

en el equipo cliente, inicie la utilidad klmover desde la línea de comandos.

Al iniciarse desde la línea de comandos, la utilidad klmover puede realizar las siguientes acciones (dependiendo de las claves en uso):

- conecta el Agente de red al Servidor de administración con la configuración especificada;
- registra los resultados de la operación en el archivo de registro del evento o los muestra en pantalla.

Sintaxis de línea de comandos de la utilidad:

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

Los parámetros de la línea de comandos son los siguientes:

- `-logfile <nombre de archivo>`: registra los resultados de ejecución de la utilidad en un archivo de registro.

  De forma predeterminada, la información se guarda en el flujo saliente estándar (stdout). Si la clave no está en uso, los resultados y mensajes de error se muestran en pantalla.

- `-address <dirección del servidor>`: la dirección del Servidor de administración para la conexión.

  Puede especificar como dirección una dirección IP, el nombre NetBIOS o el nombre DNS de los equipos.

- `-pn <número de puerto>`: número del puerto a través del cual se establecerá la conexión no cifrada al Servidor de administración.

  El número de puerto predeterminado es el 14000.

- `-ps <número de puerto SSL>`: número del puerto SSL a través del cual se establece la conexión al Servidor de administración, utilizando el protocolo SSL.

  El número de puerto predeterminado es el 13000.

- `-nossl`: usar conexión no cifrada al Servidor de administración.

  Si la clave no está en uso, el Agente de red se conecta al Servidor de administración mediante el protocolo cifrado SSL.

- `-cert <ruta al archivo del certificado>`: usa el archivo de certificado especificado para la autenticación del acceso al Servidor de administración.

  Si la clave no está en uso, el Agente de red recibe un certificado en la primera conexión al Servidor de administración.

- `-silent`: ejecutar la utilidad en modo silencio.

  El uso de la clave puede ser útil, por ejemplo, si la utilidad se inicia desde el archivo de comando de inicio de sesión al momento del registro del usuario.

- `-dupfix`: la clave se usa si el Agente de red se instaló mediante un método que difiere del usual (con el paquete de distribución); por ejemplo, si se recuperó a partir de una imagen de disco ISO.

CREACIÓN DE UN TÚNEL DE CONEXIÓN ENTRE UN EQUIPO CLIENTE Y EL SERVIDOR DE ADMINISTRACIÓN

La creación de un túnel de conexión entre un equipo cliente y el Servidor de administración es necesaria si el puerto para la conexión al Servidor de administración no está disponible en el equipo cliente. El puerto del equipo cliente puede no estar disponible en los casos que se enumeran a continuación:

- El equipo remoto está conectado a una red local que utiliza un mecanismo NAT.
- El equipo remoto es parte de la red local del Servidor de administración, pero su puerto está cerrado por un firewall.

Para crear un túnel de conexión entre un equipo cliente y el Servidor de administración:

1. En el árbol de consola seleccione el grupo de administración que incluye el equipo cliente.
2. En la pestaña **Equipos**, seleccione el equipo cliente.
3. En el menú contextual del equipo cliente, seleccione **Todas las tareas** → **Túnel de conexión**.
4. Cree un túnel en la ventana **Túnel de conexión** que se abre.

CONEXIÓN REMOTA AL ESCRITORIO DE UN EQUIPO CLIENTE

El administrador puede obtener acceso remoto al escritorio de un equipo cliente a través de un Agente de red instalado en el equipo cliente. La conexión remota al equipo cliente a través del Agente de red también es posible si los puertos TCP y UDP del equipo cliente están cerrados.

Al establecer la conexión con el equipo cliente, el administrador obtiene acceso completo a la información almacenada en este equipo, de manera que puede administrar las aplicaciones instaladas en él.

La conexión remota con un equipo cliente se puede establecer mediante uno de estos dos métodos:

- Uso de un componente estándar de Microsoft Windows denominado Conexión con escritorio remoto. La conexión con un escritorio remoto se establece a través de la utilidad estándar de Windows mstsc.exe, de acuerdo con la configuración de la utilidad.

  La conexión a la sesión de escritorio remoto actual del usuario se establece sin el conocimiento de este. Una vez que el administrador se conecta a la sesión, el usuario del equipo cliente queda desconectado de la sesión sin notificación previa.

- Uso de la tecnología Windows Desktop Sharing. Al conectarse con una sesión existente del escritorio remoto, el usuario de la sesión en el equipo cliente recibe una solicitud de conexión del administrador. No hay información acerca de la actividad remota del equipo, y los resultados se guardarán en informes creados por Kaspersky Security Center.

  El administrador se puede conectar a una sesión existente en un equipo cliente sin desconectar al usuario que está trabajando en esta sesión. En este caso, el administrador y el usuario de la sesión en el equipo cliente compartirán el acceso al escritorio.

  El administrador puede configurar una auditoría de la actividad del usuario en un equipo cliente remoto. Durante la auditoría, la aplicación guarda la información acerca de los archivos en el equipo cliente que ha abierto y/o modificado el administrador (consulte la sección "Auditoría de acciones en un equipo remoto cliente" en la página 75).

Para conectarse al escritorio de un equipo cliente a través de Windows Desktop Sharing, debe cumplir las siguientes condiciones:

- El equipo cliente tiene Microsoft Windows Vista o un sistema operativo posterior de Windows instalado.
- La estación de trabajo del administrador tiene Microsoft Windows Vista o un sistema operativo posterior de Windows instalado. El tipo de sistema operativo del equipo que alberga al Servidor de administración no impone restricciones con respecto a la conexión a través de Windows Desktop Sharing.
- Kaspersky Security Center usa una licencia para la Administración de sistemas.

Para conectarse al escritorio de un equipo cliente a través del componente de Conexión con el escritorio remoto:

1. En el árbol de Consola de administración, seleccione un equipo cliente al que debe obtener acceso.
2. En el menú contextual del equipo cliente, seleccione **Todas las tareas Conectar al equipo RDP**.

   Como resultado, se inicia la utilidad estándar de Windows mstsc.exe, que ayuda a establecer la conexión con el escritorio remoto.
3. Siga las instrucciones que se muestran en los cuadros de diálogo de la utilidad.

Una vez establecida la conexión con el equipo cliente, el escritorio estará disponible en la ventana de conexión remota de Microsoft Windows.

Para conectarse al escritorio de un equipo cliente a través de la tecnología Windows Desktop Sharing:

1. En el árbol de Consola de administración, seleccione un equipo cliente al que debe obtener acceso.
2. En el menú contextual del equipo cliente, seleccione **Todas las tareas** → **Conectar al equipo** → **Windows Desktop Sharing**.
3. En la ventana **Seleccionar sesión de escritorio remoto** que se abre, seleccione la sesión en el equipo cliente a la que debe conectarse.

   Si la conexión al equipo cliente se establece correctamente, el escritorio del equipo cliente estará disponible en la ventana **Visor de sesiones del escritorio remoto de Kaspersky**.
4. Para iniciar la interacción con el equipo cliente, en el menú principal de la ventana **Visor de sesiones del escritorio remoto de Kaspersky**, seleccione **Acciones** → **Modo interactivo**.

CONSULTE TAMBIÉN:

Opciones de licencias de Kaspersky Security Center 34

CONFIGURAR EL REINICIO DE UN EQUIPO CLIENTE

Mientras usa, instala o elimina Kaspersky Security Center, se puede requerir un reinicio del equipo cliente. La aplicación le permite configurar el reinicio de equipos cliente.

Para configurar el reinicio de un equipo cliente:

1. En el árbol de consola, seleccione el grupo de administración para el que desea configurar el reinicio.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. Seleccione una directiva en la lista del Agente de red de Kaspersky Security Center y luego seleccione **Propiedades** en el menú contextual de la directiva.
4. En la ventana de propiedades de la directiva, seleccione la sección **Administración de reinicio**.
5. Seleccione la acción que se debe realizar si se requiere un reinicio del equipo cliente:
   - Seleccione **No reiniciar el sistema operativo** para bloquear el reinicio automático.
   - Seleccione **Reiniciar el sistema operativo automáticamente si es necesario** para permitir el reinicio automático.
   - Seleccione **Solicitar al usuario** para habilitar la solicitud al usuario para permitir el reinicio.

   Al seleccionar las casillas correspondientes puede especificar la frecuencia de las solicitudes de reinicio, habilitar el reinicio y cierre forzados de aplicaciones durante sesiones bloqueadas en un equipo cliente.
6. Haga clic en el botón **OK** para guardar los cambios y cierre la ventana de propiedades de la directiva.

Como resultado, se configurará el reinicio del equipo cliente.

AUDITORÍA DE ACCIONES EN UN EQUIPO CLIENTE REMOTO

La aplicación permite que se realice la auditoría de las acciones del administrador en un equipo cliente remoto. Durante la auditoría, la aplicación guarda información acerca de los archivos del equipo cliente que han sido abiertos o modificados por el administrador. La auditoría de las acciones del administrador está disponible cuando se cumplen las siguientes condiciones:

- Hay una licencia de Administración de sistemas activa disponible.
- El administrador tiene permiso para ejecutar el acceso compartido al escritorio del equipo remoto.

Para habilitar la auditoría de acciones en un equipo cliente remoto:

1. En el árbol de consola, seleccione el grupo de administración para el que se debe configurar la auditoría de las acciones del administrador.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. Seleccione una directiva del Agente de red de Kaspersky Security Center y luego seleccione **Propiedades** en el menú contextual de la directiva.
4. En la ventana de propiedades de directivas, seleccione la sección **Uso compartido de escritorio**.
5. Seleccione la casilla **Habilitar auditoría**.
6. En las listas **Máscaras de archivos cuya lectura debe monitorizarse** y **Máscaras de archivos cuyas modificaciones deben monitorizarse**, agregue las máscaras de archivos en las que se deben monitorear las acciones durante la auditoría.

   De forma predeterminada, la aplicación monitorea las acciones en los archivos con extensiones txt, rtf, doc, xls, docx y xlsx.
7. Haga clic en el botón **OK** para guardar los cambios y cierre la ventana de propiedades de la directiva.

De esta manera, se configura la auditoría de las acciones del administrador en el equipo remoto del usuario con acceso compartido al escritorio.

Los registros de las acciones del administrador en el equipo remoto se computan:

- En el registro de eventos en el equipo remoto
- En un archivo con la extensión syslog ubicado en la carpeta de instalación del Agente de red en el equipo remoto
- en la base de datos de eventos de Kaspersky Security Center.

COMPROBACIÓN DE LA CONEXIÓN ENTRE UN EQUIPO CLIENTE Y EL SERVIDOR DE ADMINISTRACIÓN

Kaspersky Security Center permite comprobar automática o manualmente las conexiones entre un equipo y el Servidor de administración.

La comprobación automática de la conexión se ejecuta en el Servidor de Administración. La comprobación manual de la conexión se ejecuta en el equipo cliente.

EN ESTA SECCIÓN:

Comprobación automática de la conexión entre un equipo cliente y el Servidor de administración 76

Comprobación manual de la conexión entre un equipo cliente y el Servidor de administración. Utilidad klnagchk 76

COMPROBACIÓN AUTOMÁTICA DE LA CONEXIÓN ENTRE UN EQUIPO CLIENTE Y EL SERVIDOR DE ADMINISTRACIÓN

Para iniciar una comprobación automática de la conexión entre un equipo cliente y el Servidor de administración:

1. En el árbol de consola seleccione el grupo de administración que incluye el equipo cliente.
2. En el espacio de trabajo del grupo de administración, en la pestaña **Equipos** seleccione el equipo cliente.
3. Seleccione **Comprobar conexión** en el menú contextual del equipo cliente.

Como resultado se abrirá una ventana con la información sobre la accesibilidad del equipo.

COMPROBACIÓN MANUAL DE LA CONEXIÓN ENTRE UN EQUIPO CLIENTE Y EL SERVIDOR DE ADMINISTRACIÓN. UTILIDAD KLNAGCHK

Puede comprobar la conexión y obtener información detallada sobre la configuración de la conexión entre un equipo cliente y el Servidor de administración mediante la utilidad klnagchk.

Al instalar el Agente de red en un equipo cliente, la utilidad klnagchk se copia automáticamente a la carpeta de instalación del Agente de red.

Al iniciarse desde la línea de comandos, la utilidad klnagchk puede realizar las siguientes acciones (dependiendo de las claves en uso):

- Muestra en pantalla o registra en un archivo de registro del evento los valores de la configuración de conexión del Agente de red instalado en el equipo cliente en el Servidor de administración.
- Registra en un archivo de registro del evento las estadísticas del Agente de red (desde el último inicio) y los resultados de la operación de la utilidad, o bien muestra la información en pantalla.
- Realiza el intento de establecer conexión entre el Agente de red y el Servidor de administración.

  Si falla el intento de conexión, la utilidad envía un paquete ICMP para comprobar el estado del equipo donde está instalado el Servidor de administración.

Para comprobar la conexión entre un equipo cliente y el Servidor de Administración mediante la utilidad klnagchk,

en el equipo cliente, inicie la utilidad klnagchk desde la línea de comandos.

Sintaxis de línea de comandos de la utilidad:

```
klnagchk [-logfile <nombre de archivo>] [-sp] [-savecert <ruta al archivo de certificado>] [-restart]
```

Los parámetros de la línea de comandos son los siguientes:

- `-logfile <nombre de archivo>`: registra en un archivo de registro los valores de la configuración de conexión entre el Agente de red y el Servidor de administración y los resultados de la operación de la utilidad.

  De forma predeterminada, la información se guarda en el flujo saliente estándar (stdout). Si la clave no está en uso, la configuración, los resultados y mensajes de error se muestran en pantalla.
- `-sp`: muestra la contraseña para la autenticación del usuario en el servidor proxy.

  La configuración está en uso si la conexión al Servidor de administración se establece a través de un servidor proxy.
- `-savecert <ruta al archivo de certificado>`: guarda el certificado utilizado para acceder al Servidor de administración en el archivo especificado.
- `-restart`: reinicia el Agente de red una vez que la utilidad ha concluido.

IDENTIFICACIÓN DE EQUIPOS CLIENTE EN EL SERVIDOR DE ADMINISTRACIÓN

La identificación de los equipos cliente se basa en sus nombres. El nombre de un equipo cliente es único entre todos los nombres de los equipos conectados al Servidor de administración.

El nombre de un equipo cliente se transfiere al Servidor de administración cuando se sondea la red de Windows y se detecta un nuevo equipo, o bien durante la primera conexión del Agente de red instalado en un equipo cliente al Servidor de administración. De forma predeterminada, el nombre coincide con el nombre del equipo en la red de Windows (nombre NetBIOS). Si un equipo cliente con este nombre ya está registrado en el Servidor de administración, se agregará un índice con el siguiente número de secuencia al nombre del nuevo equipo cliente, por ejemplo: **<Nombre>-1**, **<Nombre>-2**. El equipo cliente se agregará al grupo de administración con este nombre.

AGREGAR EQUIPOS A UN GRUPO DE ADMINISTRACIÓN

Para incluir uno o varios equipos en un grupo de administración seleccionado:

1. Abra la carpeta **Equipos administrados** en el árbol de consola.
2. En la carpeta **Equipos administrados** seleccione la carpeta anidada que se corresponde con el grupo, que debería incluir los equipos cliente.

   Si desea incluir los equipos cliente en el grupo **Equipos administrados**, puede omitir este paso.
3. En el espacio de trabajo del grupo de administración seleccionado, en la pestaña **Equipos**, ejecute el proceso de inclusión de equipos cliente en el grupo, mediante uno de los siguientes métodos:
   - Agregue los equipos al grupo haciendo clic en el enlace **Agregar equipos** de la sección correspondiente a la administración de la lista de equipos.
   - Seleccionando **Nuevo Equipo** en el menú contextual de la lista de equipos.

   Esto iniciará el Asistente para agregar equipos cliente. Siguiendo sus instrucciones, seleccione un método para agregar los equipos cliente al grupo y crear una lista de equipos que se incluirán en el grupo.

   Si crea una lista de equipos en forma manual, puede utilizar una dirección IP (o un intervalo IP), un nombre NetBIOS o un nombre DNS como dirección del equipo. Solo puede agregar manualmente a la lista equipos para los cuales ya se agregó información a la base de datos del Servidor de administración cuando se conectó el equipo o luego del sondeo de la red.

   Para importar la lista desde un archivo, especifique un archivo .txt con una lista de direcciones de los equipos que se agregarán. Cada dirección debe ser especificada en una línea separada.

Una vez finalizado el asistente, los equipos cliente seleccionados se incluyen en el grupo de administración y se muestran en la lista de equipos con nombres generados por el Servidor de administración.

Puede agregar un equipo cliente al grupo de administración seleccionado arrastrándolo desde la carpeta **Equipos no asignados** a la carpeta del grupo de administración.

CAMBIO DEL SERVIDOR DE ADMINISTRACIÓN PARA EQUIPOS CLIENTE

Puede cambiar el Servidor de administración que administra los equipos cliente por otro, mediante la tarea **Cambiar Servidor de administración**.

Para cambiar el Servidor de administración que administra equipos cliente por otro:

1. Conéctese al Servidor de administración que administra los equipos cliente.
2. Cree la tarea de cambio del Servidor de administración mediante uno de los siguientes métodos:
   - Si necesita cambiar el Servidor de administración para los equipos incluidos en el grupo de administración seleccionado, cree una tarea de grupo (ver sección “Crear una tarea de grupo” en la página 65).
   - Si necesita cambiar el Servidor de administración para equipos incluidos en grupos de administración diferentes o que no están en ningún grupo, cree una tarea para equipos específicos (ver sección “Crear una tarea para equipos específicos” en la página 66).

   Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente. En la ventana **Tipo de tarea** del Asistente para nueva tarea, seleccione el nodo **Kaspersky Security Center**, abra la carpeta **Avanzado** y seleccione la tarea **Cambiar Servidor de administración**.
3. Ejecute la tarea creada.

Una vez que se completó la tarea, los equipos cliente para la que se crearon pasan al ámbito de administración del Servidor de administración especificado en la configuración de la tarea.

Si el Servidor de administración admite la función de cifrado y protección de datos, al crear la tarea **Cambiar Servidor de administración**, se mostrará una notificación que indica que, en el caso de que los datos cifrados se almacenen en equipos, se le proporcionará acceso solamente a datos cifrados que ha gestionado anteriormente, después de cambiar los equipos de acuerdo con la administración del nuevo servidor. En otros casos, no se brindará acceso a datos cifrados. Para conocer las descripciones detalladas de situaciones en las que no se proporciona acceso a datos cifrados, consulte la Guía del administrador de Kaspersky Endpoint Security 10 para Windows.

ENCENDIDO, APAGADO Y REINICIO REMOTO DE EQUIPOS CLIENTE

Kaspersky Security Center le permite administrar equipos cliente en forma remota: encenderlos, apagarlos y reiniciarlos.

Para administrar equipos cliente en forma remota:

1. Conéctese al Servidor de administración que administra los equipos cliente.
2. Cree la tarea de administración para un equipo cliente mediante uno de los siguientes métodos:
   - Si necesita encender, apagar o reiniciar equipos incluidos en el grupo de administración seleccionado, cree una tarea de grupo (ver sección “Crear una tarea de grupo” en la página 65).
   - Si necesita encender, apagar o reiniciar equipos incluidos en distintos grupos de administración o que no pertenecen a ninguno, cree una tarea para equipos específicos (ver sección “Crear una tarea para equipos específicos” en la página 66).

   Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente. En la ventana **Tipo de tarea** del Asistente para nueva tarea, seleccione el nodo **Kaspersky Security Center**, abra la carpeta **Avanzado** y seleccione la tarea **Administrar equipo cliente**.
3. Ejecute la tarea creada.

Luego de finalizar la tarea, se ejecutará el comando seleccionado (encender, apagar o reiniciar) en los equipos cliente seleccionados.

ENVIAR UN MENSAJE A LOS USUARIOS DE EQUIPOS CLIENTE

Para enviar un mensaje a los usuarios de equipos cliente:

1. Conéctese al Servidor de administración que administra los equipos cliente.
2. Cree la tarea de envío de mensaje para usuarios de equipos cliente de una de las siguientes formas:
   - Si desea enviar un mensaje a los usuarios de equipos cliente que pertenecen al grupo de administración seleccionado, cree una tarea para el grupo seleccionado (ver sección “Crear una tarea de grupo” en la página 65).
   - Si desea enviar un mensaje a los usuarios de equipos cliente que pertenecen a diferentes grupos de administración o no pertenecen a ninguno, cree una tarea para equipos específicos (ver sección “Crear una tarea para equipos específicos” en la página 66).

   Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente. En la ventana **Tipo de tarea**, seleccione el nodo **Kaspersky Security Center**, abra la carpeta **Avanzado** y seleccione la tarea **Notificación al usuario**.
3. Ejecute la tarea creada.

Una vez finalizada la tarea, el mensaje creado se enviará a los usuarios de los equipos cliente seleccionados.

CONTROLAR LOS CAMBIOS EN EL ESTADO DE LAS MÁQUINAS VIRTUALES

El Servidor de administración almacena información sobre el estado de los equipos administrados, como el registro de hardware y la lista de aplicaciones instaladas, o la configuración de las aplicaciones, tareas y directivas gestionadas. Si una máquina virtual funciona como un equipo administrado, el usuario puede restaurar su estado en cualquier momento con una imagen instantánea de la máquina virtual. Como resultado, la información sobre el estado de la máquina virtual en el Servidor de administración puede volverse desactualizada.

Por ejemplo, el administrador ha creado una directiva de protección en el Servidor de administración a las 12:00 p.m., la cual comenzó a funcionar en la máquina virtual VM_1 a las 12:01 p. m. A las 12:30 p. m., el usuario de la máquina virtual VM_1 cambió el estado al restaurarla de una imagen instantánea tomada a las 11:00 p. m. Como resultado, la directiva de protección deja de funcionar en la máquina virtual. Sin embargo, la información desactualizada en el Servidor de administración asegura que la directiva de protección en la máquina virtual VM_1 continúa en funcionamiento.

Kaspersky Security Center ayuda a controlar todos los cambios en el estado de las máquinas virtuales.

Después de cada sincronización con el equipo cliente, el Servidor de administración genera un ID único, que se almacena tanto del lado del equipo cliente como del Servidor de administración. Antes de iniciar la siguiente sincronización, el Servidor de administración compara los valores de esos ID de ambos lados. Si los valores de los ID no coinciden, el Servidor de administración reconoce a la máquina virtual como restaurada de una imagen instantánea. El Servidor de administración restablece toda la configuración de las directivas y tareas activas en la máquina virtual y le envía las directivas actualizadas y la lista de las tareas de grupo.

DIAGNÓSTICO REMOTO DE LOS EQUIPOS CLIENTE. UTILIDAD DE DIAGNÓSTICO REMOTO DE KASPERSKY SECURITY CENTER

La utilidad para diagnóstico remoto de Kaspersky Security Center (de aquí en adelante, utilidad de diagnóstico remoto) está diseñada para la ejecución remota de las siguientes operaciones en equipos cliente:

- habilitación y deshabilitación del seguimiento, cambio del nivel de seguimiento, descarga del archivo de seguimiento;
- descarga de configuraciones de aplicaciones;
- descarga de registros de eventos;
- inicio de los diagnósticos y descarga de los resultados;
- inicio y detención de aplicaciones.

La utilidad de diagnóstico remoto se instala en el equipo automáticamente junto con la Consola de administración.

EN ESTA SECCIÓN:

Conexión de la utilidad de diagnóstico remoto a un equipo cliente 80

Habilitar y deshabilitar el seguimiento, descargar el archivo de seguimiento 81

Descargar configuraciones de aplicaciones 82

Descarga de registros de eventos 82

Inicio de los diagnósticos y descarga de los resultados 82

Inicio, detención y reinicio de las aplicaciones 82

CONEXIÓN DE LA UTILIDAD DE DIAGNÓSTICO REMOTO A UN EQUIPO CLIENTE

Para conectar la utilidad de diagnóstico remoto a un equipo cliente:

1. Seleccione cualquier grupo de administración del árbol de consola.
2. En el espacio de trabajo, en la pestaña **Equipos**, en el menú contextual de cualquier equipo cliente, seleccione **Herramientas personalizadas** → **Diagnósticos remotos**.

   Como resultado, se abre la ventana principal de la utilidad de diagnósticos remotos.
3. En el primer campo de la ventana principal de la utilidad de diagnósticos remotos, especifique las herramientas que desea utilizar para conectarse con el equipo cliente:
   - **Acceso mediante la Red de Microsoft Windows**.
   - **Acceso mediante el Servidor de administración**.
4. Si seleccionó **Acceso mediante la Red de Microsoft Windows** en el primer campo de la ventana principal de la utilidad, realice las siguientes acciones:
   - En el campo **Equipo** especifique el equipo al que debe conectarse.

     Puede utilizar una dirección IP, nombre NetBIOS o DNS como la dirección del equipo.

     El valor predeterminado es la dirección del equipo del menú contextual en el cual se ejecutó la utilidad.
   - Especifique una cuenta para conectar al equipo:
     - **Conectar como usuario actual** (seleccionado de forma predeterminada). Conectar con la cuenta de usuario actual.
     - **Utilizar el nombre de usuario y la contraseña proporcionados para conectar**. Conectar con la cuenta de usuario proporcionada. Especifique el **Nombre de usuario** y la **Contraseña** de la cuenta requerida.

   La conexión a un equipo cliente solo es posible a través de la cuenta del administrador local del equipo cliente.
5. Si seleccionó **Acceso mediante el Servidor de administración** en el primer campo de la ventana principal de la utilidad, realice las siguientes acciones:
   - En el campo **Servidor de administración**, especifique la dirección del Servidor de administración desde la cual intenta conectarse al equipo cliente.

     Puede utilizar una dirección IP, un nombre NetBIOS o DNS como dirección del servidor.

     El valor predeterminado es la dirección del Servidor del que se ejecutó la utilidad.
   - Si es necesario, seleccione las casillas **Utilizar SSL**, **Comprimir tráfico** y **El Equipo pertenece al Servidor de administración secundario**.

     Si está seleccionada la casilla **El equipo pertenece al Servidor de administración secundario**, puede completar el campo **Servidor secundario** con el nombre del Servidor de administración secundario que administra el equipo cliente. Para ello, haga clic en el botón **Examinar**.
6. Para conectar al equipo cliente, haga clic en el botón **Intro**.

Esto abre la ventana destinada para realizar diagnósticos remotos del equipo cliente (ver la siguiente figura). La parte izquierda de la ventana contiene enlaces a las operaciones de diagnóstico del equipo cliente. La parte derecha de la ventana contiene el árbol de objetos del equipo cliente que la utilidad puede manejar. La parte inferior de la ventana muestra el progreso de las operaciones de la utilidad.

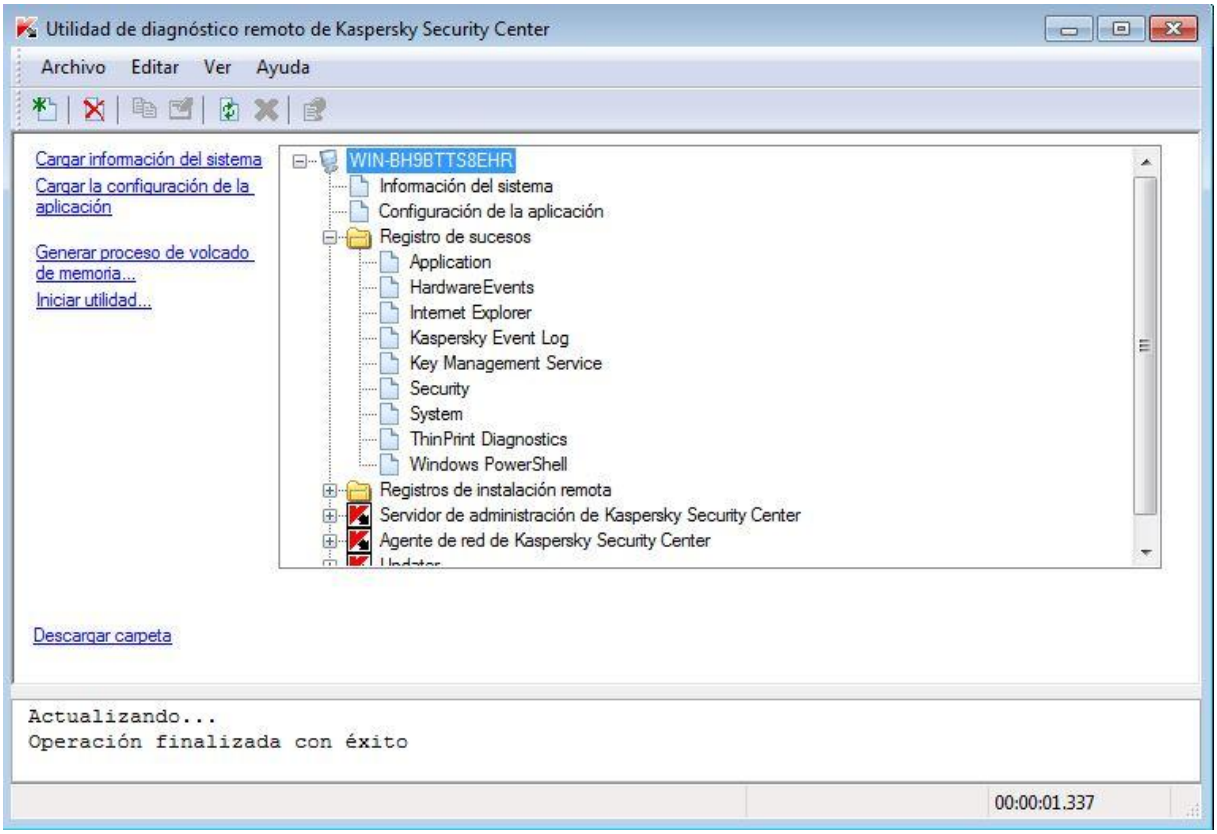


Figura 12. Utilidad de diagnósticos remotos. Ventana de diagnósticos remotos del equipo cliente

La utilidad de diagnósticos remotos guarda los archivos descargados desde los equipos cliente al escritorio del equipo desde el que haya sido ejecutada.

HABILITAR Y DESHABILITAR EL SEGUIMIENTO, DESCARGAR EL ARCHIVO DE SEGUIMIENTO

Para habilitar el seguimiento, descargar el archivo de seguimiento y deshabilitar el seguimiento:

1. Ejecute la utilidad de diagnóstico remoto y conecte al equipo requerido.
2. En el árbol de objetos del equipo cliente, seleccione la aplicación para la cual necesita desarrollar un seguimiento y habilite el seguimiento mediante un clic en el enlace **Habilitar seguimiento** ubicado a la izquierda de la ventana de la utilidad de diagnóstico remoto.

   El seguimiento se puede habilitar y deshabilitar para aplicaciones con protección automática solo si el equipo cliente está conectado mediante herramientas del Servidor de administración.

   En algunos casos, la aplicación antivirus y su tarea deben reiniciarse para poder habilitar el seguimiento.
3. En el nodo de la aplicación para la cual se habilitó el seguimiento, seleccione en la carpeta **Archivos de rastreo** el archivo requerido y descárguelo mediante un clic en el enlace **Descargar archivo**. Para archivos de gran tamaño solo se pueden descargar las partes de seguimiento más recientes.

   Puede eliminar el archivo de seguimiento resaltado. El archivo puede eliminare una vez que el seguimiento está deshabilitado.
4. Deshabilite el seguimiento para la aplicación seleccionada mediante un clic en el enlace **Deshabilitar seguimiento**.

DESCARGAR CONFIGURACIONES DE APLICACIONES

Para descargar configuraciones de aplicaciones:

1. Ejecute la utilidad de diagnóstico remoto y conecte al equipo requerido.
2. En el árbol de objetos de la ventana de diagnóstico remoto seleccione el nodo superior con el nombre del equipo y seleccione la acción requerida en la parte izquierda de la ventana:
   - **Cargar información del sistema**.
   - **Cargar la configuración de la aplicación**.
   - **Generar proceso de volcado de memoria**.

     En la ventana que se abrirá al hacer clic en este enlace, especifique el archivo ejecutable de la aplicación seleccionada para la cual necesita generar un archivo de volcado de memoria.
   - **Iniciar utilidad**.

     En la ventana que se abrirá al hacer clic en este enlace, especifique el archivo ejecutable de la utilidad seleccionada y su configuración de inicio.

     Como resultado, la utilidad seleccionada se descarga y se ejecuta en el equipo cliente.

DESCARGA DE REGISTROS DE EVENTOS

Para descargar un registro de eventos:

1. Ejecute la utilidad de diagnóstico remoto y conecte al equipo requerido.
2. En la carpeta **Registro de eventos** del árbol de objetos del equipo seleccione el registro seleccionado y descárguelo mediante un clic en el enlace **Descargar el Registro de eventos de Kaspersky** en la parte izquierda de la ventana de la utilidad de diagnóstico remoto.

INICIO DE LOS DIAGNÓSTICOS Y DESCARGA DE LOS RESULTADOS

Para iniciar el diagnóstico de una aplicación y descargar los resultados:

1. Ejecute la utilidad de diagnóstico remoto y conecte al equipo requerido.
2. En el árbol de objetos del equipo cliente seleccione la aplicación requerida e inicie el diagnóstico mediante un clic en el enlace **Ejecutar diagnóstico**.

   Como resultado, aparece un informe de diagnóstico en el nodo de la aplicación seleccionada en el árbol de objetos.
3. Seleccione el informe de diagnóstico recién generado en el árbol de objetos y descárguelo mediante un clic en el enlace **Descargar archivo**.

INICIO, DETENCIÓN Y REINICIO DE LAS APLICACIONES

Solo puede iniciar, detener y reiniciar aplicaciones si ha conectado el equipo cliente mediante herramientas del Servidor de administración.

Para iniciar, detener o reiniciar una aplicación:

1. Ejecute la utilidad de diagnóstico remoto y conecte al equipo cliente requerido.
2. En el árbol de objetos del equipo cliente seleccione la aplicación requerida y seleccione una acción en la parte izquierda de la ventana:
   - **Detener aplicación**
   - **Reiniciar aplicación**
   - **Iniciar aplicación**

De acuerdo con la acción seleccionada, la aplicación se iniciará, se detendrá o se reiniciará.

ADMINISTRACIÓN DE CUENTAS DE USUARIO

Esta sección brinda información sobre las cuentas de usuario y los roles admitidos por la aplicación. Esta sección contiene instrucciones sobre cómo crear cuentas y roles para los usuarios de Kaspersky Security Center. Esta sección también contiene instrucciones sobre cómo manejar la lista de los certificados y dispositivos móviles del usuario y cómo enviar mensajes a los usuarios.

EN ESTA SECCIÓN:

Manejo de cuentas de usuario 83

Agregar una cuenta de usuario 83

Configuración de permisos Roles de usuarios 84

Enviar mensajes a los usuarios 85

Ver la lista de dispositivos móviles de un usuario 85

Instalar un certificado para un usuario 86

Ver la lista de certificados entregados a un usuario 86

MANEJO DE CUENTAS DE USUARIO

Kaspersky Security Center permite administrar cuentas de usuario y grupos de cuentas. La aplicación admite dos tipos de cuentas:

- Cuentas de empleados de la organización. El Servidor de administración recupera datos de las cuentas de esos usuarios cuando sondea la red de la organización.
- Cuentas de usuarios internos (consulte la sección "Manejo de usuarios internos" en la página 53). Estas se aplican cuando se manejan los Servidores de administración virtuales. Las cuentas de usuarios internos se crean (consulte la sección "Agregar una cuenta de usuario" en la página 83) y se utilizan solo dentro de Kaspersky Security Center.

Todas las cuentas del usuario se pueden ver en la carpeta **Cuentas de usuario**, en el árbol de consola.

Puede realizar las siguientes acciones en las cuentas de usuario y grupos de cuentas:

- Configure los permisos de acceso de los usuarios a las características de la aplicación mediante roles (consulte la sección "Configuración de derechos. Roles de los usuarios" en la página 84)
- Envíe mensajes a los usuarios mediante correo electrónico y SMS (consulte la sección "Envío de mensajes a los usuarios" en la página 85)
- Vea la lista de los dispositivos móviles de los usuarios (consulte la sección "Visualización de la lista de los dispositivos móviles de los usuarios" en la página 85)
- Entregue e instale certificados en los dispositivos móviles del usuario (consulte la sección "Instalación de un certificado para un usuario" en la página 86)
- Vea la lista de certificados entregados a un usuario (ver la sección "Ver la lista de certificados entregados a un usuario" en la página 86).

AGREGAR UNA CUENTA DE USUARIO

Para agregar una nueva cuenta de usuario de Kaspersky Security Center:

1. En el árbol de consola, abra la carpeta **Cuentas de usuario**.
2. En el espacio de trabajo haga clic en el enlace **Agregar usuario nuevo** para abrir la ventana **Propiedades**.

3. Especifique la configuración de la cuenta y establezca una contraseña para que el usuario se conecte a Kaspersky Security Center.

   No hay requisitos especiales para la contraseña.

   Si selecciona la casilla **Deshabilitar cuenta**, el usuario no podrá conectarse a la aplicación. Puede seleccionar esta casilla, por ejemplo, en caso de despido de un empleado. Esta casilla se desactiva de forma predeterminada.

4. Haga clic en **Aceptar**.

Como resultado, la cuenta de usuario recientemente creada se mostrará en el espacio de trabajo de la carpeta **Cuentas de usuario**.

CONFIGURACIÓN DE DERECHOS. ROLES DE USUARIOS

De manera flexible, puede configurar el acceso a diversas características de la aplicación por parte de usuarios y grupos de usuarios. Puede proporcionarles a los usuarios permisos de acceso a las características de la aplicación, mediante uno de estos dos métodos:

- Configure los permisos para cada usuario o grupo de usuarios en forma individual.
- Cree roles de usuarios estándar con un conjunto predefinido de permisos y asigne esos roles a los usuarios en función del ámbito de sus actividades.

Un *rol de usuario* es un conjunto predefinido y creado de manera exclusiva de permisos de acceso a las características de la aplicación. Un rol se puede otorgar a un usuario de un grupo de usuarios. Al aplicar roles, se simplifican y reducen los procedimientos rutinarios de configuración de los permisos de los usuarios para acceder a la aplicación. Los permisos de acceso dentro de un rol se configuran de acuerdo con las tareas "estándar" y el ámbito de las actividades de los usuarios. Por ejemplo, un rol de usuario solo puede tener permisos para leer y enviar comandos de información a los dispositivos móviles de otros usuarios a través del Portal de autoservicio.

A los roles de usuarios se les pueden asignar nombres que correspondan con sus fines respectivos. Puede crear una cantidad ilimitada de roles en la aplicación.

AGREGAR UN ROL DE USUARIO

Para agregar un rol de usuario:

1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Roles de usuarios** y haga clic en el botón **Agregar**.
4. En la ventana **Propiedades: Rol nuevo**, configure el rol:
   - En la sección **General**, especifique el nombre del rol.

     El nombre de un rol no puede contener más de 100 caracteres.
   - En la sección **Derechos**, configure el conjunto de permisos seleccionando las casillas **Permitir** y **Denegar** que se encuentran junto a las características de la aplicación.
5. Haga clic en **Aceptar**.

Como resultado, se guardará el rol.

Los roles de usuarios que se han creado para el Servidor de administración se muestran en la ventana de propiedades del servidor, en la sección **Roles de usuarios**. Puede editar y eliminar roles de usuarios, como así también asignar roles a grupos de usuarios (consulte la sección "Asignación de un rol a un usuario o a un grupo de usuarios" en la página 85) o a usuarios individuales.

La sección **Roles de usuarios** está disponible si la casilla **Mostrar secciones de configuración de seguridad** está seleccionada en la ventana de configuración de la interfaz. (consulte la sección "Configuración de la interfaz" en la página 31)

ASIGNACIÓN DE UN ROL A UN USUARIO O GRUPO DE USUARIOS

- *Para asignar un rol a un usuario o grupo de usuarios:*

  1. En el árbol de consola, seleccione el nodo con el nombre del Servidor de administración requerido.
  2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
  3. En la ventana de propiedades del Servidor de administración, seleccione la sección **Seguridad**.
  4. En el campo **Nombres de grupos o usuarios**, seleccione un usuario o grupo de usuarios a los que se les debe asignar un rol.

     Si el usuario o el grupo no están incluidos en el campo, puede agregarlos haciendo clic en el botón **Agregar**.

     Cuando agrega un usuario haciendo clic en el botón Agregar, puede seleccionar el tipo de autenticación del usuario (Microsoft Windows o Kaspersky Security Center). La autenticación de Kaspersky Security Center se usa para seleccionar las cuentas de los usuarios internos que se usan para manejar Servidores de Administración virtuales.
  5. Abra la pestaña **Roles** y haga clic en el botón **Agregar**.

     Se abre la ventana **Roles de usuarios**. En esta ventana se muestran los roles de usuarios que se han creado.
  6. En la ventana **Roles de usuarios**, seleccione un rol para el grupo de usuarios.
  7. Haga clic en **Aceptar**.

Como resultado, el rol con un conjunto de permisos para manejar el Servidor de administración se asignará al usuario del grupo de usuarios. Los roles que se han asignado se muestran en la pestaña **Roles** en la sección **Seguridad** de la ventana de propiedades del Servidor de administración.

La sección **Seguridad** está disponible si la casilla **Mostrar secciones con configuración de seguridad** está seleccionada en la ventana de configuración de la interfaz (consulte la sección "**Configuración de la interfaz**" en la página 31).

ENVIAR MENSAJES A LOS USUARIOS

- *Para enviar un mensaje por correo electrónico a un usuario:*

  1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione un usuario.
  2. En el menú contextual del usuario, seleccione **Enviar mensaje por correo electrónico**.
  3. Complete los campos relevantes en la ventana **Enviar mensaje a usuario** y haga clic en el botón **Aceptar**.

  Como resultado, el mensaje se enviará al correo electrónico que se especificó en las propiedades del usuario.
- *Para enviar un mensaje SMS a un usuario:*

  1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione un usuario.
  2. En el menú contextual del usuario, seleccione **Enviar mensaje SMS**.
  3. Complete los campos correspondientes en la ventana **Mensaje SMS** y haga clic en el botón **Aceptar**.

  Como resultado, el mensaje se enviará al dispositivo móvil con el número que se especificó en las propiedades del usuario.

VER LA LISTA DE DISPOSITIVOS MÓVILES DE UN USUARIO

- *Para ver la lista de dispositivos móviles de un usuario:*

  1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione un usuario.
  2. En el menú contextual de la cuenta de usuario, seleccione **Propiedades**.
  3. En la ventana de propiedades de la cuenta de usuario, seleccione la sección **Dispositivos móviles**.

En la sección **Dispositivos móviles**, puede ver la lista de dispositivos móviles del usuario y la información sobre cada uno de ellos. Puede hacer clic en el botón **Exportar a archivo** para guardar la lista de dispositivos móviles en un archivo.

INSTALAR UN CERTIFICADO PARA UN USUARIO

Puede instalar tres tipos de certificados para un usuario:

- Certificado general, que es necesario para identificar el dispositivo móvil del usuario.
- Certificado de correo, que es necesario para configurar el correo corporativo en el dispositivo móvil del usuario.
- Certificado de correo, que es necesario para configurar la red privada virtual en el dispositivo móvil del usuario.

Para entregar un certificado a un usuario y luego instalarlo:

1. En el árbol de consola, abra la carpeta **Cuentas de usuario** y seleccione una cuenta de usuario.
2. En el menú contextual de la cuenta de usuario, seleccione **Instalar certificado**.

Se inicia el Asistente de instalación del Certificado. Siga las instrucciones del asistente.

Después de que haya finalizado el Asistente de instalación de certificados, el certificado se creará e instalará para el usuario. Puede ver la lista de certificados instalados de un usuario y exportarla a un archivo (consulte la sección "Visualización de la lista de certificados entregados a un usuario" en la página 86).

VER LA LISTA DE CERTIFICADOS ENTREGADOS A UN USUARIO

Para ver una lista de todos los certificados entregados a un usuario:

1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione un usuario.
2. En el menú contextual de la cuenta de usuario, seleccione **Propiedades**.
3. En la ventana de propiedades de la cuenta de usuario, seleccione la sección **Certificados**.

En la sección **Certificados**, puede ver la lista de los certificados del usuario y la información sobre cada uno de ellos. Puede hacer clic en el botón **Exportar a archivo** para guardar la lista de certificados en un archivo.

TRABAJO CON INFORMES, ESTADÍSTICAS Y NOTIFICACIONES

Esta sección provee información sobre cómo manejar informes, estadísticas y selecciones de eventos y equipos cliente en Kaspersky Security Center y, además, sobre cómo configurar las notificaciones del Servidor de administración.

EN ESTA SECCIÓN:

Trabajo con informes 87
Manejo de la información estadística 89
Configurar los parámetros de notificación 89
Selecciones de eventos 90
Exportación de eventos a un sistema SIEM 91
Selecciones de equipos 92
Selecciones de directivas 94
Selecciones de tarea 94

TRABAJO CON INFORMES

Los informes en Kaspersky Security Center tienen información acerca de la condición del sistema de protección antivirus. Los informes son generados según la información almacenada en el Servidor de administración. Puede crear informes para los siguientes tipos de objetos:

- Para una selección de equipos cliente
- para equipos de un grupo de administración específico;
- para un conjunto de equipos cliente de diferentes grupos de administración;
- para todos los equipos en la red (disponible para el informe de distribución).

La aplicación incluye un conjunto de plantillas de informe estándar. También soporta la creación de plantillas de informe definidas por el usuario. Los informes se muestran en la ventana principal de la aplicación, en la carpeta **Informes y notificaciones** del árbol de consola.

EN ESTA SECCIÓN:

Crear una plantilla de informe 87
Crear y ver un informe 88
Guardar un informe 88
Crear una tarea de envío de informes 88

CREAR UNA PLANTILLA DE INFORME

Para crear una plantilla de informe,

seleccione la carpeta **Informes y notificaciones** en el árbol de consola y realice una de las siguientes acciones:

- Seleccione **Nuevo** → **Plantilla de informe** en el menú contextual de la carpeta Informes y notificaciones.
- En el espacio de trabajo de la carpeta **Informes y notificaciones**, en la pestaña **Informes** ejecute el proceso de creación de plantilla de informe mediante un clic en el enlace **Crear una plantilla de informe**.

Como resultado, se iniciará el Asistente para nueva plantilla de informe. Siga las instrucciones del asistente.

Una vez que el asistente finaliza su operación, la plantilla de informe recién creada se agrega a la carpeta **Informes y notificaciones** del árbol de consola. Puede utilizar esta plantilla para generar y ver informes.

CREAR Y VER UN INFORME

Para crear y ver un informe:

1. En el árbol de consola, abra la carpeta **Informes y notificaciones** en la que están indicadas las plantillas de informes.
2. Seleccione la plantilla de informe requerida en el árbol de consola o el espacio de trabajo en la pestaña **Informes**.

   Como resultado, el espacio de trabajo mostrará un informe creado en la plantilla seleccionada.

El informe muestra los siguientes datos:

- El nombre y tipo de informe, su breve descripción y el período de creación de informes, así como también información sobre el grupo de dispositivos para los que se genera el informe;
- diagrama gráfico que refleja los datos más importantes del informe;
- tabla con resumen de datos que refleja los valores calculados a partir del informe;
- tabla de datos detallados del informe.

GUARDAR UN INFORME

Para guardar un informe creado:

1. En el árbol de consola, abra la carpeta **Informes y notificaciones** en la que están indicadas las plantillas de informes.
2. Seleccione la plantilla de informe requerida en el árbol de consola o el espacio de trabajo en la pestaña **Informes**.
3. En el menú contextual de la plantilla de informe seleccionada, seleccione **Guardar**.

Se inicia el Asistente para guardar informes. Siga las instrucciones del asistente.

Después de finalizada la operación del Asistente, la carpeta se abre en el lugar en que se guardó el archivo de informe.

CREAR UNA TAREA DE ENVÍO DE INFORMES

El envío de informes en Kaspersky Security Center se realiza mediante la tarea de envío de informes. Puede enviar informes por correo electrónico o guardarlos en una carpeta dedicada, por ejemplo, en una carpeta compartida en el Servidor de administración o un equipo local.

Para crear una tarea de envío para un informe:

1. En el árbol de consola, abra la carpeta **Informes y notificaciones** en la que están indicadas las plantillas de informes.
2. Seleccione la plantilla de informe requerida en el árbol de consola o el espacio de trabajo en la pestaña **Informes**.
3. En el menú contextual de la plantilla de informe, seleccione el elemento **Enviar informes**.

Esto iniciará el Asistente para la creación de tareas de envío de informes. Siga las instrucciones del asistente.

Para crear una tarea de envío de varios informes:

1. En el árbol de consola, seleccione la carpeta **Tareas del Servidor de administración**.
2. Comience a crear la tarea en una de las siguientes formas:
   - En el árbol de consola, en el menú contextual de la carpeta **Tareas del Servidor de administración**, seleccione **Nuevo** → **Tarea**.
   - Haga clic en el enlace **Crear una tarea** en el espacio de trabajo.

Como resultado, se iniciará el Asistente para la creación de tareas del Servidor de administración. Siga las instrucciones del asistente. En la ventana del asistente **Tipo de tarea**, seleccione **Entregar informes**.

La tarea de envío de informes creada se muestra en el árbol de consola, en la carpeta **Tareas del Servidor de administración**.

La tarea de envío de informes se crea automáticamente si se especificó la configuración de correo electrónico durante la instalación de Kaspersky Security Center.

MANEJO DE LA INFORMACIÓN ESTADÍSTICA

La información estadística sobre el estado del sistema de protección se muestra en el espacio de trabajo de la carpeta **Informes y notificaciones**, en la pestaña **Estadísticas**. La pestaña **Estadísticas** contiene varias páginas; cada una se compone de paneles informativos que muestran información estadística. La información estadística se muestra en forma de tabla o gráfico (de barras o circular). Los datos en los paneles de información se actualizan mientras se ejecuta la aplicación, reflejando la condición actual del sistema de protección antivirus.

Puede cambiar la cantidad y la estructura de las páginas en la pestaña **Estadísticas**, el número de paneles de información en cada página y también el modo de visualización de datos en los paneles.

Los siguientes botones sirven para editar la configuración de visualización y la configuración de impresión para estadísticas:

-  - ubicado en la esquina superior derecha de la pestaña **Estadísticas**. Configure la estructura de la pestaña **Estadísticas**: agregue o elimine páginas de estadísticas, cambie sus posiciones.
-  - ubicado a la derecha del nombre de página. Configure la página de estadísticas.
-  - ubicado a la derecha del nombre del panel de información. Configure el panel de información.
-  - ubicado a la derecha del nombre del panel de información. Minimice el panel de información.
-  - ubicado a la derecha del nombre del panel de información. Maximice el panel de información.
-  - ubicado en la esquina superior derecha de la pestaña **Estadísticas**. Imprima la página de estadísticas actual.

CONFIGURAR LOS PARÁMETROS DE NOTIFICACIÓN

Kaspersky Security Center le permite configurar la notificación del administrador de los eventos que ocurrieron en los equipos cliente y seleccionar un método de notificación:

- Correo electrónico. Cuando ocurre un evento, la aplicación envía una notificación a las direcciones de correo electrónico especificadas. Puede editar el texto de la notificación.
- NET SEND (servicio de mensajes). Cuando ocurre un evento, la aplicación envía una notificación usando el servicio de mensajería

La notificación a través del servicio de mensajes solo está disponible para los sistemas operativos Windows 5.X (Windows XP, Windows Server® 2003).

- SMS. Cuando ocurre un evento, la aplicación envía una notificación a los números de teléfono especificados. Puede configurar que las notificaciones de SMS se envíen a través de la puerta de enlace de correo o mediante la Utilidad de difusión de SMS.
- Archivo ejecutable. Cuando ocurre un evento en un equipo cliente, se inicia el archivo ejecutable en la estación de trabajo del administrador. El administrador puede recibir los parámetros del evento que ha ocurrido mediante el archivo ejecutable.

Para configurar notificaciones de eventos que ocurrieron en los dispositivos cliente:

1. Abra la ventana de propiedades de la carpeta **Informes y notificaciones** del árbol de consola de alguna de las siguientes formas:
   - Seleccione **Propiedades** del menú contextual de la carpeta **Informes y notificaciones** del árbol de consola.

- En el espacio de trabajo de la carpeta **Informes y notificaciones**, en la pestaña **Notificaciones**, haga clic en el enlace **Modificar la configuración del envío de notificaciones** para abrir la ventana.

2. En la sección **Notificación** de la ventana de propiedades de la carpeta **Informes y notificaciones**, seleccione el método de notificación y establezca la configuración de notificaciones.

Como resultado, se implementa la configuración de notificación modificada en todos los eventos que ocurrieron en dispositivos cliente.

Se puede configurar la notificación de un evento en la ventana de propiedades de ese evento. Puede obtener un acceso rápido a las configuraciones de eventos haciendo clic en los enlaces **Configurar eventos de Kaspersky Endpoint Security** y **Modificar la configuración de los eventos del Servidor de administración**.

CONSULTE TAMBIÉN:

Configuración de parámetros de procesamiento de eventos 51

SELECCIONES DE EVENTOS

La información sobre los eventos del funcionamiento de Kaspersky Security Center se guarda en el registro del sistema de Microsoft Windows y también en el registro de eventos de Kaspersky Security Center. Puede ver información del registro de eventos de Kaspersky Security Center en la carpeta **Informes y notificaciones** del árbol de consola, la subcarpeta **Eventos**.

La información de la carpeta **Eventos** se representa en selecciones. Cada selección incluye eventos que cumplen las condiciones especificadas. Después de la instalación de la aplicación, la carpeta contiene algunas selecciones estándar. Puede crear selecciones adicionales de eventos o exportar información de eventos a archivo.

EN ESTA SECCIÓN:

Ver una selección de eventos 90
Personalizar una selección de eventos 90
Crear una selección de eventos 91
Exportar una selección de eventos a un archivo de texto 91
Eliminar eventos de la selección 91

VISUALIZAR UNA SELECCIÓN DE EQUIPOS

Para ver una selección de eventos:

1. En el árbol de consola, expanda la carpeta **Informes y notificaciones** y ubique **Eventos**.
2. Abra la selección de eventos de una de las siguientes formas:
   - Abra la carpeta **Eventos** y seleccione la carpeta que contiene la selección de eventos requerida.
   - En el espacio de trabajo de la carpeta **Eventos** haga clic en el enlace que corresponde a la selección de eventos que necesita.

Como resultado, el espacio de trabajo mostrará una lista de eventos, almacenados en el Servidor de administración, del tipo seleccionado.

Puede ordenar la información en la lista de eventos, tanto en orden ascendente como descendente, en cualquier columna.

PERSONALIZAR UNA SELECCIÓN DE EVENTOS

Para personalizar una selección de eventos:

1. En el árbol de consola, expanda la carpeta **Informes y notificaciones** y ubique **Eventos**.
2. Abra la selección de eventos requerida en la carpeta **Eventos**.

3. Abra las propiedades de selección de eventos de una de las siguientes formas:
   - En el menú contextual de la selección de eventos, seleccione **Propiedades**.
   - Haga clic en **Propiedades de selección** en el bloque de administración de selección de eventos.

   En la ventana de propiedades de selección de eventos que se abre, puede configurar la selección de eventos.

CREAR UNA SELECCIÓN DE EVENTOS

Para crear una selección de eventos:

1. En el árbol de consola, expanda la carpeta **Informes y notificaciones** y ubique **Eventos**.
2. Comience a crear la selección de eventos de una de las siguientes formas:
   - En el menú contextual de la carpeta, seleccione **Nuevo** → **Selección**.
   - Haga clic en el enlace **Crear selección** en el espacio de trabajo de la carpeta **Eventos**.
3. En la ventana **Nueva selección de eventos** que se abre, introduzca el nombre de la nueva selección y haga clic en **Aceptar**.

   Como resultado, aparecerá una nueva carpeta con el nombre que introdujo, en la carpeta **Eventos** del árbol de consola.

De forma predeterminada, una selección de eventos creada contiene todos los eventos almacenados en el Servidor de administración. Para que la selección muestre solo los eventos que son de especial interés, debe personalizar la selección.

EXPORTAR UNA SELECCIÓN DE EVENTOS A UN ARCHIVO DE TEXTO

Para exportar una selección de eventos a un archivo de texto:

1. En el árbol de consola, expanda la carpeta **Informes y notificaciones** y ubique **Eventos**.
2. Abra la selección de eventos requerida en la carpeta **Eventos**.
3. Comience la exportación de eventos de una de las siguientes formas:
   - En el menú contextual de la selección, seleccione **Todas las tareas** → **Exportar**.
   - Haga clic en el enlace **Exportar eventos a archivo** en el bloque de administración de selección de eventos.

   Se iniciará el Asistente de exportación de eventos. Siga las instrucciones del asistente.

ELIMINAR EVENTOS DE LA SELECCIÓN

Para eliminar eventos:

1. En el árbol de consola, expanda la carpeta **Informes y notificaciones** y ubique **Eventos**.
2. Abra la selección de eventos requerida en la carpeta **Eventos**.
3. Seleccione los eventos que desea eliminar, mediante el mouse o las teclas **Mayús** o **Ctrl**.
4. Elimine los eventos seleccionados de una de las siguientes formas:
   - En el menú contextual de algunos de los eventos seleccionados, seleccione **Eliminar**.

     Si selecciona el elemento **Eliminar todo** del menú contextual, se eliminarán todos los eventos mostrados de la selección, independientemente de cuáles eventos seleccionó.
   - Haga clic en el enlace **Eliminar evento** si selecciona un evento, o bien en **Eliminar eventos** si selecciona varios eventos en el bloque de trabajo para estos eventos.

   Como resultado, se eliminarán los eventos seleccionados de la carpeta **Eventos**.

EXPORTACIÓN DE EVENTOS A UN SISTEMA SIEM

La aplicación permite exportar eventos que se han registrado en la operación del Servidor de administración y otras aplicaciones de Kaspersky Lab instaladas en equipos cliente, a un sistema SIEM (donde SIEM significa Administración de información de seguridad y eventos).

Para configurar la exportación de eventos a un sistema SIEM:

1. En el árbol de consola, expanda la carpeta **Informes y notificaciones** y ubique **Eventos**.
2. En el menú contextual de la carpeta **Eventos**, seleccione **Propiedades**.

   Se abre la ventana propiedades de eventos, mostrando la sección **Exportación de eventos**.
3. Seleccione la casilla **Exportar eventos a la base de datos del sistema SIEM automáticamente**.
4. En la lista desplegable de **Sistema SIEM** seleccione el sistema al cual necesita exportar los eventos.

   Los eventos pueden ser exportados a sistemas SIEM como *QRadar* y *ArcSight*. De forma predeterminada, el sistema ArcSight está seleccionado.
5. En los campos correspondientes especifique la dirección de un servidor de sistema SIEM y un puerto para la conexión a ese servidor.

   Hacer clic en el botón **Exportar archivo** ocasiona que la aplicación exporte los eventos recientemente creados a la base de datos del sistema SIEM a partir de la fecha especificada. De forma predeterminada, la aplicación exporta eventos a partir de la fecha actual.
6. Haga clic en **Aceptar**.

Como resultado, luego de que seleccione la casilla **Exportar eventos a la base de datos del sistema SIEM automáticamente** y configure la conexión con el servidor, la aplicación exportará automáticamente todos los eventos al sistema SIEM cuando se registren en la operación del Servidor de administración y otras aplicaciones de Kaspersky Lab.

SELECCIONES DE EQUIPOS

La información sobre los estados de los equipos cliente está disponible en la carpeta **Informes y notificaciones** del árbol de consola, en la subcarpeta **Selecciones de equipos**.

En la carpeta **Selecciones de equipos**, los datos están representados como un conjunto de selecciones; cada uno muestra información sobre los equipos que cumplen las condiciones especificadas. Después de la instalación de la aplicación, la carpeta contiene algunas selecciones estándar. Puede crear selecciones de equipos adicionales, exportar la configuración de la selección a un archivo o crear selecciones con la configuración importada desde otro archivo.

EN ESTA SECCIÓN:

Visualizar una selección de equipos 92
Configurar una selección de equipos 93
Crear una selección de equipos 93
Exportar una configuración de selección de equipos a un archivo 93
Crear una selección de equipos mediante una configuración importada 93
Eliminación de equipos de los grupos de administración en una selección 94

VISUALIZAR UNA SELECCIÓN DE EQUIPOS

Para ver una selección de equipos:

1. En la carpeta **Informes y notificaciones** del árbol de consola, seleccione la subcarpeta **Selecciones de equipos**.
2. Abra la selección de equipos de una de las siguientes formas:
   - Abra la carpeta **Selecciones de equipos** y seleccione la carpeta que contiene la selección de equipos requerida.
   - En el espacio de trabajo de la carpeta **Selecciones de equipos**, usando el vínculo que corresponde con la selección de equipos requeridos.

El espacio de trabajo mostrará la lista de equipos que corresponde al filtro de la selección.

Puede ordenar la información en la lista de equipos, tanto en orden ascendente como descendente, en cualquier columna.

CONFIGURAR UNA SELECCIÓN DE EQUIPOS

Para personalizar una selección de equipos:

1. En la carpeta **Informes y notificaciones** del árbol de consola, seleccione la subcarpeta **Selecciones de equipos**.
2. Abra la selección de equipos requerida en la carpeta **Selecciones de equipos**.
3. Abra las propiedades de selección de equipos de una de las siguientes formas:
   - En el menú contextual de la selección de equipos, seleccione **Propiedades**.
   - Haga clic en **Propiedades de selección** en el bloque de administración de selección de equipos.

En la ventana de propiedades de selección de equipos que se abre, puede configurar la selección de equipos.

CREAR UNA SELECCIÓN DE EQUIPOS

Para crear una selección de equipos:

1. En la carpeta **Informes y notificaciones** del árbol de consola, seleccione la subcarpeta **Selecciones de equipos**.
2. Comience a crear la selección de equipos de una de las siguientes formas:
   - En el menú contextual de la carpeta, seleccione **Nuevo** → **Selección**.
   - Haga clic en el enlace **Crear selección** en el espacio de trabajo de la carpeta **Selecciones de equipos**.
3. En la ventana **Nueva selección de equipos** que se abre, introduzca el nombre de la nueva selección y haga clic en **Aceptar**.

Como resultado, aparecerá una nueva carpeta con el nombre que introdujo, en la carpeta **Selecciones de equipos** del árbol de consola.

De forma predeterminada, la nueva selección de equipos contiene todos los equipos incluidos en los grupos de administración del Servidor en el que se creó la selección. Para que la selección muestre solo los equipos que son de especial interés, debe personalizar la selección.

EXPORTAR UNA CONFIGURACIÓN DE SELECCIÓN DE EQUIPOS A UN ARCHIVO

Para exportar las configuraciones de una selección de equipos a un archivo de texto:

1. En la carpeta **Informes y notificaciones** del árbol de consola, seleccione la subcarpeta **Selecciones de equipos**.
2. Abra la selección de equipos requerida en la carpeta **Selecciones de equipos**.
3. En el menú contextual de la selección de equipo, seleccione **Todas las tareas** → **Exportar configuración**.
4. En la ventana **Guardar como** que se abre, especifique un nombre para el archivo de exportación de la configuración de selección, seleccione una carpeta para guardarlo y haga clic en el botón **Guardar**.

La configuración de la selección de equipos se guardará en el archivo especificado.

CREAR UNA SELECCIÓN DE EQUIPOS MEDIANTE UNA CONFIGURACIÓN IMPORTADA

Para crear una selección de equipos utilizando las configuraciones importadas:

1. En la carpeta **Informes y notificaciones** del árbol de consola, seleccione la subcarpeta **Selecciones de equipos**.
2. Crear una selección de equipos utilizando las configuraciones importadas del archivo de una de las siguientes maneras:
   - En el menú contextual de la carpeta, seleccione **Todas las tareas** → **Importar**.

- Haga clic en el enlace **Importar selección desde archivo** en el bloque de administración de la carpeta.

3. En la ventana que se abre, especifique la ruta del archivo desde el cual desea importar las configuraciones de selección. Haga clic en el botón **Abrir**.

Como resultado, en la carpeta **Selecciones de equipos** se crea la carpeta **Nueva selección**. Sus configuraciones se importan del archivo especificado.

Si ya existe una selección llamada **Nueva selección** en la carpeta **Selecciones de equipos**, se agrega un índice en formato **(<número de serie>)** al nombre de la selección que se crea, por ejemplo: **(1)**, **(2)**.

ELIMINACIÓN DE EQUIPOS DE LOS GRUPOS DE ADMINISTRACIÓN EN UNA SELECCIÓN

Cuando se trabaja con selecciones de equipos, puede eliminar los equipos de los grupos de administración, sin cambiar a los grupos de administración en los que se ubican estos equipos.

Para eliminar los equipos de los grupos de administración:

1. En la carpeta **Informes y notificaciones** del árbol de consola, seleccione la subcarpeta **Selecciones de equipos**.
2. Abra la selección de equipos requerida en la carpeta **Selecciones de equipos**.
3. Seleccione los equipos que desea eliminar usando las teclas **Mayús** o **Ctrl**.
4. Eliminar los equipos seleccionados de los grupos de una de las siguientes maneras:
   - En el menú contextual de algunos de los equipos seleccionados, seleccione **Eliminar**.
   - Haga clic en el enlace **Eliminar del grupo** en el espacio de trabajo de los equipos seleccionados.

Como resultado, los equipos seleccionados serán eliminados de los grupos de administración correspondientes.

SELECCIONES DE DIRECTIVAS

La información sobre las directivas está disponible en la carpeta **Informes y notificaciones** del árbol de consola, en la subcarpeta **Selecciones de directivas**.

La carpeta **Selecciones de directivas** muestra una lista de directivas que se han creado en los grupos de administración. Después de la instalación de la aplicación, la carpeta contiene una lista de directivas que se han creado en forma automática. Puede actualizar la lista y ver las propiedades de cualquier directiva seleccionada de la lista.

SELECCIONES DE TAREA

La información sobre las tareas está disponible en la carpeta **Informes y notificaciones** del árbol de consola, en la subcarpeta **Selecciones de tarea**.

La carpeta **Selecciones de tarea** muestra una lista de tareas que se han asignado a los equipos cliente de los grupos de administración y al Servidor de administración. Después de la instalación de la aplicación, la carpeta contiene una lista de tareas que se han creado en forma automática. Puede actualizar la lista y ver las propiedades de las tareas, así como ejecutar y detener tareas.

EQUIPOS NO ASIGNADOS

Esta sección proporciona información sobre cómo administrar los equipos de una red empresarial si no están incluidos en un grupo de administración.

La información sobre los equipos de una red corporativa que no están incluidos en los grupos de administración se puede encontrar en la carpeta **Equipos no asignados**. La carpeta **Equipos no asignados** contiene tres subcarpetas: **Dominios**, **Subredes IP** y **Active Directory**.

La carpeta **Equipos no asignados** del Servidor de administración virtual no contiene la carpeta **Subredes IP**. Los equipos cliente detectados durante el sondeo de subredes IP en el Servidor de administración virtual se muestran en la carpeta **Dominios**.

La carpeta **Dominios** contiene la jerarquía de subcarpetas que muestran la estructura de dominios y grupos de trabajo de la red de Windows de la organización que no se incluyeron en los grupos de administración. Cada subcarpeta de la carpeta **Dominios** en el nivel inferior contiene una lista de equipos del dominio o del grupo de trabajo. Si agrega un equipo al grupo de administración, la información sobre este se elimina de la carpeta **Dominios**. Si elimina un equipo del grupo de administración, la información sobre este se muestra en la carpeta **Dominios**, en la subcarpeta del dominio o en el grupo de trabajo de este equipo.

La carpeta **Active Directory** muestra los equipos que reflejan la estructura de grupos del Active Directory.

La carpeta **Subredes IP** muestra los equipos que reflejan la estructura de las subredes IP creadas en la red corporativa. Puede cambiar la estructura de la carpeta **Subredes IP** creando y modificando la configuración de las subredes IP existentes.

EN ESTA SECCIÓN:

Descubrimiento de red 95

Trabajar con dominios de Windows. Ver y cambiar la configuración de dominio 97

Trabajar con subredes IP 97

Trabajar con los grupos de Active Directory. Ver y cambiar la configuración de grupo 98

Crear reglas para mover equipos a grupos de administración automáticamente 98

Usar el modo dinámico para VDI en los equipos cliente 98

DESCUBRIMIENTO DE RED

La información sobre la estructura de la red y los equipos en la misma es recibida por el Servidor de administración mediante sondeos regulares de la red de Windows, subredes IP y Active Directory dentro de la red corporativa de equipos. El contenido de la carpeta **Equipos no asignados** se actualiza en función de los resultados de este sondeo.

El Servidor de administración puede utilizar los siguientes tipos de escaneo de red:

- **Sondeo de la red de Windows**. Hay dos tipos de sondeo de red de Windows: rápido o completa. Durante el sondeo rápido, únicamente se recopilará la información de los equipos de la lista de nombre NetBIOS de todos los dominios y grupos de trabajo de la red. Durante el escaneo completo, se solicita la siguiente información de cada equipo cliente: sistema operativo, dirección IP, nombre DNS, nombre NetBIOS.
- **Sondeo de subredes IP**. El Servidor de administración sondeará las subredes IP especificadas mediante paquetes ICMP y recopilará un conjunto completo de datos en los hosts que se encuentran dentro de las subredes IP.
- **Sondeo de grupos de Active Directory**. La información en la estructura de unidad de Active Directory y los nombres DNS de los equipos de Active Directory se registra en la base de datos del Servidor de administración.

Kaspersky Security Center utiliza la información recopilada y los datos de la estructura de la red corporativa para actualizar el contenido de las carpetas **Equipos no asignados** y **Equipos administrados**. Si los equipos de la red corporativa están configurados para se movidos a los grupos de administración automáticamente, los equipos detectados se incluyen en los grupos de administración.

EN ESTA SECCIÓN:

Visualizar y modificar la configuración del sondeo de la red de Windows 96
Ver y modificar las propiedades de grupos de Active Directory 96
Visualizar y modificar los parámetros para el sondeo de la subred IP 96

VISUALIZAR Y MODIFICAR LA CONFIGURACIÓN DEL SONDEO DE LA RED DE WINDOWS

Para modificar la configuración para el sondeo de la red de Windows:

1. En el árbol de consola, seleccione la carpeta **Equipos no asignados** y la subcarpeta **Dominios**.
2. Abra la ventana **Propiedades: Dominios** de una de las siguientes formas:
   - En el menú contextual de la carpeta, seleccione **Propiedades**.
   - Haciendo clic en el enlace **Editar configuración de sondeo** en el bloque de administración de la carpeta.

   Esto abrirá **Propiedades**. **Dominios** en la que puede cambiar la configuración del sondeo de la red de Windows.

También puede cambiar la configuración del sondeo de la red de Windows en el espacio de trabajo de la carpeta **Equipos no asignados** mediante el enlace **Editar configuración de sondeo** en la sección de configuración de **Sondeo de la red de Windows**.

En el Servidor de administración virtual, puede ver y editar la configuración de sondeo de la red de Windows en la ventana de propiedades del agente de actualización, en la sección **Sondeo de red**.

VER Y MODIFICAR LAS PROPIEDADES DE GRUPOS DE ACTIVE DIRECTORY

Para modificar la configuración para el sondeo de grupos de Active Directory:

1. En el árbol de consola, seleccione la carpeta **Equipos no asignados** y la subcarpeta **Active Directory**.
2. Abra la ventana **Propiedades: Active Directory** de una de las siguientes formas:
   - En el menú contextual de la carpeta, seleccione **Propiedades**.
   - Haciendo clic en el enlace **Editar configuración de sondeo** en el bloque de administración de la carpeta.

   Esto abrirá **Propiedades**. **Active Directory** de la que puede cambiar la configuración del sondeo de Active Directory.

También puede cambiar la configuración del sondeo de grupos de Active Directory en el espacio de trabajo de la carpeta **Equipos no asignados** mediante el enlace **Editar configuración de sondeo** en el bloque **Sondeo de Active Directory**.

En el Servidor de administración virtual, puede ver y editar la configuración de sondeo de grupos de Active Directory, en la ventana de propiedades del agente de actualización, en la sección **Sondeo de red**.

VISUALIZAR Y MODIFICAR LOS PARÁMETROS PARA EL SONDEO DE LA SUBRED IP

Para modificar los parámetros de sondeo de las subredes IP:

1. En el árbol de consola, seleccione la carpeta **Equipos no asignados** y la subcarpeta **Subredes IP**.
2. Abra la ventana **Propiedades: Subredes IP** de una de las siguientes formas:
   - En el menú contextual de la carpeta, seleccione **Propiedades**.
   - Haciendo clic en el enlace **Editar configuración de sondeo** en el bloque de administración de la carpeta.

   Esto abrirá **Propiedades**. **Subredes IP** en la que puede cambiar la configuración del sondeo de subredes IP.

También puede cambiar la configuración del sondeo de subredes IP en el espacio de trabajo de la carpeta **Equipos no asignados** mediante el enlace **Editar configuración de sondeo** en el bloque **Sondeo de subredes IP**.

En el Servidor de administración virtual puede ver y editar la configuración de sondeo de subredes IP, en la ventana de propiedades del agente de actualización, en la sección **Sondeo de red**. Los equipos cliente detectados durante el sondeo de subredes IP se muestran en la carpeta **Dominios** del Servidor de administración virtual.

TRABAJAR CON DOMINIOS DE WINDOWS. VER Y CAMBIAR LA CONFIGURACIÓN DE DOMINIO

Para modificar la configuración de dominio:

1. En el árbol de consola, seleccione la carpeta **Equipos no asignados** y la subcarpeta **Dominios**.
2. Seleccione un dominio y abra su ventana de propiedades en una de las siguientes formas:
   - En el menú contextual del dominio, seleccione **Propiedades**.
   - Haciendo clic en el enlace **Mostrar propiedades de grupo**.

Esto abrirá la ventana **Propiedades: <Nombre de dominio>**en la que puede configurar las propiedades del dominio seleccionado.

TRABAJAR CON SUBREDES IP

Puede personalizar las subredes IP existentes y crear las nuevas.

EN ESTA SECCIÓN:

Crear una subred IP 97
Ver y modificar los parámetros de la subred IP 97

CREAR UNA SUBRED IP

Para crear una subred IP:

1. En el árbol de consola, seleccione la carpeta **Equipos no asignados** y la subcarpeta **Subredes IP**.
2. En el menú contextual de la carpeta, seleccione **Nuevo** → **Subred IP**.
3. En la ventana **Nueva subred IP** que se abre, personalice la nueva subred.

Como resultado, la nueva subred IP aparece en la carpeta **Subredes IP**.

VER Y MODIFICAR LOS PARÁMETROS DE LA SUBRED IP

Para modificar los parámetros de la subred IP:

1. En el árbol de consola, seleccione la carpeta **Equipos no asignados** y la subcarpeta **Subredes IP**.
2. Seleccione una subred IP y abra su ventana de propiedades en una de las siguientes formas:
   - En el menú contextual de la subred IP, seleccione **Propiedades**.
   - Haciendo clic en el enlace **Mostrar propiedades de grupo**.

Esto abrirá la ventana **Propiedades: <Nombre de la subred IP>** en la que puede configurar las propiedades de la subred IP seleccionada.

TRABAJAR CON LOS GRUPOS DE ACTIVE DIRECTORY. VER Y CAMBIAR LA CONFIGURACIÓN DE GRUPO

Para modificar la configuración del grupo de Active Directory:

1. En el árbol de consola, seleccione la carpeta **Equipos no asignados** y la subcarpeta **Active Directory**.
2. Seleccione un grupo de Active Directory y abra su ventana de propiedades en una de las siguientes formas:
   - En el menú contextual del grupo, seleccione **Propiedades**.
   - Haciendo clic en el enlace **Mostrar propiedades de grupo**.

   Esto abrirá la ventana **Propiedades: <Nombre del grupo de Active Directory>** en la que puede personalizar el grupo de Active Directory seleccionado.

CREAR REGLAS PARA MOVER EQUIPOS A GRUPOS DE ADMINISTRACIÓN AUTOMÁTICAMENTE

Puede configurar los equipos para que se muevan automáticamente a los grupos de administración después de que se hayan encontrado.

Para configurar reglas para mover automáticamente equipos a grupos de administración,

abra la ventana de propiedades de la carpeta **Equipos no asignados** de una de las siguientes maneras:

- En el menú contextual de la carpeta, seleccione **Propiedades**.
- Haga clic en el enlace **Configurar reglas de asignación de equipos a grupos de administración** en el espacio de trabajo de esta carpeta.

Esto abrirá **Propiedades**. **Equipos no asignados** Configure las reglas para mover equipos a los grupos de administración automáticamente en la sección **Reubicación del equipo**.

USAR EL MODO DINÁMICO PARA VDI EN LOS EQUIPOS CLIENTE

Una infraestructura virtual se puede implementar en una red corporativa mediante el uso de máquinas virtuales temporales. Kaspersky Security Center detecta las máquinas virtuales temporales y agrega información acerca de estas a la base de datos del Servidor de administración. Después de que un usuario termina de usar una máquina virtual temporal, esta máquina se elimina de la infraestructura virtual. Sin embargo, se puede guardar un registro sobre la máquina virtual eliminada en la base de datos del Servidor de administración. Además, las máquinas virtuales inexistentes se pueden visualizar en la Consola de administración.

Para evitar que se guarde información sobre máquinas virtuales inexistentes, Kaspersky Security Center admite el modo dinámico para la Infraestructura de Escritorio Virtual (VDI). El administrador puede habilitar la compatibilidad del modo dinámico para la Infraestructura de escritorio virtual (VDI) (consulte la sección "Habilitar el modo dinámico de VDI en las propiedades del paquete de instalación de un Agente de Red" en la página 99) en las propiedades del paquete de instalación de un Agente de Red que se instalará en una máquina virtual temporal.

Cuando se deshabilita una máquina virtual temporal, el Agente de red notifica al Servidor de administración que la máquina se ha deshabilitado. Después de que una máquina virtual se ha deshabilitado correctamente, se la elimina de la lista de equipos conectados al Servidor de administración. Si la máquina virtual se deshabilita con errores y el Agente de red no envía una notificación sobre la máquina virtual deshabilitada al Servidor de administración, se usa un escenario de copia de seguridad. Con este escenario, una máquina virtual se elimina de la lista de equipos conectados al Servidor de administración después de tres intentos infructuosos de sincronización con el Servidor de administración.

EN ESTA SECCIÓN:

Habilitación del modo dinámico VDI en las propiedades de un paquete de instalación para el Agente de red 99
Buscar equipos que formen parte de la VDI 99
Mover los equipos que forman parte de la VDI a un grupo de administración 99

HABILITACIÓN DEL MODO DINÁMICO VDI EN LAS PROPIEDADES DE UN PAQUETE DE INSTALACIÓN PARA EL AGENTE DE RED

Para habilitar el modo dinámico VDI:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. En el menú contextual del paquete de instalación del Agente de red, seleccione **Propiedades**.

   Aparecerá el cuadro de diálogo **Propiedades Agente de red de Kaspersky Security Center**.
3. En la ventana **Propiedades: Agente de red de Kaspersky Security Center**, seleccione la sección **Avanzado**.
4. En la sección **Avanzado**, seleccione la casilla **Habilitar modo dinámico para VDI**.

El equipo cliente en el que se instala el Agente de red formará parte de la Infraestructura de escritorio virtual.

BUSCAR EQUIPOS QUE FORMEN PARTE DE LA VDI

Para buscar equipos que forman parte de VDI:

1. En el espacio de trabajo de la carpeta **Equipos no asignados**, haga clic en el enlace **Buscar equipos no asignados** para abrir la ventana **Buscar**.
2. En la ventana **Buscar**, en la pestaña **Máquinas virtuales**, en la lista desplegable **Parte de la infraestructura de escritorio virtual** seleccione **Sí**.
3. Haga clic en el botón **Buscar ahora**.

La aplicación busca equipos que formen parte de la infraestructura de escritorio virtual.

MOVER LOS EQUIPOS QUE FORMAN PARTE DE LA VDI A UN GRUPO DE ADMINISTRACIÓN

Para mover los equipos que forman parte de la VDI a un grupo de administración, realice lo siguiente:

1. En el espacio de trabajo de la carpeta **Equipos no asignados**, haga clic en el enlace **Configurar reglas de asignación de equipos a grupos de administración** para abrir la ventana de propiedades de la carpeta **Equipos no asignados**.
2. En la ventana de propiedades de la carpeta **Equipos no asignados**, en la sección **Reubicación del equipo**, haga clic en el botón **Agregar**.

   Se abre la ventana **Nueva regla**.
3. En la ventana **Nueva regla**, seleccione la sección **Máquinas virtuales**.
4. En la lista desplegable **Parte de la infraestructura de escritorio virtual** seleccione **Sí**.

Se creará una regla para la reubicación del equipo a un grupo de administración.

ADMINISTRAR APLICACIONES EN EQUIPOS CLIENTE

Kaspersky Security Center permite la administración de aplicaciones desarrolladas por Kaspersky Lab y otros proveedores e instaladas en equipos cliente.

El administrador puede realizar las siguientes acciones:

- Crear categorías de aplicaciones basadas en criterios específicos.
- Administrar categorías de aplicaciones que usan reglas dedicadas.
- Administrar el inicio de aplicaciones en equipos cliente.
- Realizar inventarios y mantener un registro del software instalado en equipos cliente.
- Reparar vulnerabilidades en software instalado en equipos cliente.
- Instalar actualizaciones desde Windows Update y otros proveedores de software en equipos cliente.
- Rastrear el uso de claves para grupos de aplicaciones con licencia.

EN ESTA SECCIÓN:

Grupos de aplicaciones 100

Vulnerabilidades de las aplicaciones 104

Actualizaciones de software 106

GRUPOS DE APLICACIONES

Esta sección describe cómo manejar grupos de aplicaciones instaladas en los equipos cliente.

Creación de categorías de aplicaciones

Kaspersky Security Center permite la creación de categorías de aplicaciones instaladas en equipos cliente.

Puede crear categorías de aplicaciones mediante uno de los siguientes métodos:

- El administrador especifica una carpeta en la que se han incluido los archivos ejecutables de la categoría seleccionada.
- El administrador especifica un equipo a partir del cual los archivos ejecutables deberán incluirse dentro de la categoría seleccionada.
- El administrador establece los criterios que deben usarse para incluir las aplicaciones dentro de la categoría seleccionada.

Cuando se crea la categoría de aplicaciones, el administrador puede establecer reglas para esa categoría. La reglas definen el comportamiento de las aplicaciones pertenecientes a la categoría especificada. Por ejemplo, puede bloquear o permitir el inicio de las aplicaciones incluidas en la categoría.

Administración del inicio de aplicaciones en equipos cliente

Kaspersky Security Center permite administrar el inicio de las aplicaciones en los equipos cliente en el modo Lista blanca (para obtener más información, consulte la Guía del administrador de Kaspersky Endpoint Security 10 para Windows). Mientras está activado el modo Lista blanca, en los equipos cliente seleccionados solo puede iniciar las aplicaciones pertenecientes a las categorías especificadas. El administrador puede visualizar los resultados del análisis estadístico que se ha aplicado a las reglas de inicio de aplicaciones en equipos cliente para cada usuario.

Inventario de software instalado en equipos cliente

Kaspersky Security Center permite realizar inventario del software instalado en equipos cliente. El Agente de red recupera información acerca de todas las aplicaciones instaladas en los equipos cliente. La información recopilada durante el inventario se muestra en el espacio de trabajo de la carpeta **Registro de aplicaciones**. El administrador puede ver información detallada acerca de cualquier aplicación, incluso su versión y el fabricante.

Administrar grupos de aplicaciones con licencia

Kaspersky Security Center permite la creación de grupos de aplicaciones con licencia. Un grupo de aplicaciones con licencia incluye aplicaciones que cumplen con los criterios establecidos por el administrador. El administrador puede especificar los siguientes criterios para grupos de aplicaciones con licencia:

- Nombre de la aplicación
- Versión de la aplicación
- Fabricante
- Etiqueta de la aplicación

Las aplicaciones que cumplen con uno o varios de los criterios se incluyen automáticamente en un grupo. Para crear un grupo de aplicaciones con licencia, debe establecer por lo menos un criterio de inclusión de aplicaciones en ese grupo.

Cada grupo de aplicaciones con licencia tiene su propia clave. La clave de un grupo de aplicaciones con licencia define el número máximo permitido de instalaciones para las aplicaciones incluidas en este grupo. Si el número de instalaciones ha excedido el límite establecido por la clave, se registra un evento de información en el Servidor de administración. El administrador puede especificar una fecha de caducidad para la clave. Cuando llega la fecha, un evento de información se registra en el Servidor de administración.

Visualización de información sobre archivos ejecutables

Kaspersky Security Center recopila toda la información acerca de los archivos ejecutables que se han ejecutado en equipos cliente desde que se instalaron los sistemas operativos en estos equipos. La información recopilada sobre los archivos ejecutables se muestra en la ventana principal de la aplicación, en el espacio de trabajo de la carpeta **Archivos ejecutables**.

EN ESTA SECCIÓN:

Creación de categorías de aplicaciones 101

Configuración de administración de inicio de aplicaciones en los equipos cliente 102

Visualización de los resultados de los análisis estadísticos de las reglas de inicio aplicadas a los archivos ejecutables 102

Visualización del registro de aplicaciones 103

Crear grupos de aplicaciones con licencia 103

Administración de claves para los grupos de aplicaciones con licencia 103

Visualización de información sobre archivos ejecutables 104

CREACIÓN DE CATEGORÍAS DE APLICACIONES

Para crear una categoría de aplicación:

1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Categorías de aplicaciones**.
2. Haga clic en el vínculo **Crear una categoría** para ejecutar el Asistente de creación de categorías de usuario.
3. En la ventana del Asistente, seleccione un tipo de categoría de usuario:
   - **Categoría con contenido agregado de forma manual**. En este caso, puede especificar manualmente una carpeta desde la cual los archivos ejecutables serán agregados automáticamente en la categoría que se creará.
   - **Categoría con contenido agregado de forma automática**. En este caso, puede especificar una carpeta desde la cual los archivos ejecutables serán agregados automáticamente en la categoría que se creará.
   - **Categoría que incluye los archivos ejecutables de los equipos seleccionados**. En este caso, puede especificar un equipo. Los archivos ejecutables detectados en un equipo se agregarán de forma automática en la categoría.
4. Siga las instrucciones del asistente.

Cuando haya finalizado el Asistente, se crea una categoría de usuario de las aplicaciones. Puede visualizar las categorías creadas en la carpeta **Categorías de aplicaciones**.

CONFIGURACIÓN DE ADMINISTRACIÓN DE INICIO DE APLICACIONES EN LOS EQUIPOS CLIENTE

Para configurar la administración de inicio de aplicaciones en los equipos cliente:

1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Categorías de aplicaciones**.
2. En el espacio de trabajo de la carpeta **Categorías de aplicaciones**, cree una categoría de aplicaciones (ver la sección “Creación de categorías de aplicaciones” en la página 101) que desee administrar.
3. En la carpeta **Equipos administrados**, en la pestaña **Directivas**, haga clic en el enlace **Crear directiva de Kaspersky Endpoint Security 10 for Windows** para ejecutar el Asistente para nueva directiva de Kaspersky Endpoint Security 10 para Windows y siga las instrucciones del Asistente.

   Si esa directiva ya existe, puede omitir este paso. Puede configurar la administración de inicio de aplicaciones en una categoría especificada a través de la configuración de la directiva. La directiva recién creada se muestra en la carpeta **Equipos administrados**, en la pestaña **Directivas**.
4. Seleccione **Propiedades** en el menú contextual de la directiva de Kaspersky Endpoint Security 10 para Windows.

   Se abre la ventana Propiedades de la directiva de Kaspersky Endpoint Security 10 para Windows.
5. En la ventana de Propiedades de la directiva de Kaspersky Endpoint Security 10 para Windows, en la sección **Control de inicio de aplicaciones**, haga clic en el botón **Agregar**.

   Se abre la ventana **Control de inicio de aplicaciones**.
6. En la ventana de **regla de Control de inicio de aplicaciones**, en la lista desplegable **Categoría**, seleccione una categoría de aplicaciones que abarque la regla de inicio. Configure la regla de inicio para la categoría de aplicaciones seleccionada.

   Para obtener más información sobre las reglas de control de inicio de aplicaciones, consulte la Guía del administrador de Kaspersky Endpoint Security 10 para Windows.
7. Haga clic en **Aceptar**.

El inicio de las aplicaciones que pertenezcan a la categoría especificada se realizará en los equipos cliente de acuerdo con la regla que usted haya creado. La regla creada se muestra en la ventana de Propiedades de la directiva de Kaspersky Endpoint Security 10 para Windows, en la sección **Control de inicio de aplicaciones**.

VISUALIZACIÓN DE LOS RESULTADOS DE LOS ANÁLISIS ESTADÍSTICOS DE LAS REGLAS DE INICIO APLICADAS A LOS ARCHIVOS EJECUTABLES

Para ver información acerca de los archivos ejecutables que los usuarios no están autorizados a ejecutar:

1. En la carpeta **Equipos administrados** del árbol de consola, seleccione la pestaña **Directivas**.
2. En el menú contextual de **Directivas de protección**, seleccione **Propiedades**.

   Se abre la ventana de propiedades de la directiva de protección.
3. En la ventana de propiedades de la directiva de protección, seleccione la sección **Control de inicio de aplicaciones** y haga clic en el botón **Análisis estadístico**.

   Se abre la ventana **Análisis de la lista de permisos de acceso**.
4. La parte izquierda de la ventana **Análisis de la lista de permisos de acceso** muestra una lista de usuarios basada en los datos de Active Directory.
5. Seleccione un usuario de la lista.

   La parte derecha de la ventana muestra las categorías de aplicaciones asignadas a este usuario.
6. Para ver los archivos ejecutables que el usuario no está autorizado a ejecutar, en la ventana **Análisis de la lista de permisos de acceso** haga clic en el botón **Ver archivos**.

   Se abre una ventana que muestra una lista de archivos ejecutables, que el usuario no está autorizado a ejecutar.
7. Para ver la lista de archivos ejecutables incluidos en una categoría, seleccione una categoría de aplicaciones y haga clic en el botón **Ver archivos de la categoría**.

Se abre una ventana que muestra una lista de archivos ejecutables incluidos en la categoría de aplicaciones.

VISUALIZACIÓN DEL REGISTRO DE APLICACIONES

Para visualizar el registro de las aplicaciones instaladas en equipos cliente,

En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Registro de aplicaciones**.

El espacio de trabajo de la carpeta **Registro de aplicaciones** muestra una lista de aplicaciones que fueron detectadas por el Agente de red instalado en los equipos cliente.

La recopilación de información acerca de las aplicaciones instaladas está disponible solo para equipos que se ejecutan en Microsoft Windows.

Para visualizar las propiedades de una aplicación seleccionada,

seleccione **Propiedades** en el menú contextual de la aplicación.

Se abre una ventana que muestra los detalles de la aplicación e información acerca de sus archivos ejecutables, así como también una lista de equipos en los que está instalada la aplicación.

Para visualizar aplicaciones que cumplan con criterios especificados, puede usar los campos de filtrado en el espacio de trabajo de la carpeta **Registro de aplicaciones**.

La información sobre las aplicaciones instaladas en los equipos cliente conectados a los Servidores de Administración esclavos y virtuales también se almacena en el registro de aplicaciones del Servidor de administración patrón. Utilice un informe del registro de aplicaciones para ver esta información. Para ello, habilite la recopilación de datos desde los Servidores de administración secundarios y virtuales al informe.

Para incluir información de los Servidores de administración secundarios en el informe:

1. En la carpeta **Informes y notificaciones**, seleccione **Informe de la versión de software de Kaspersky Lab**.
2. Seleccione **Propiedades** en el menú contextual del informe.

   Aparecerá el cuadro de diálogo **Propiedades Informe de la versión de software de Kaspersky Lab**.
3. En la sección **Jerarquía de los Servidores de administración**, seleccione la casilla **Incluir datos de los Servidores de administración secundarios y virtuales**.

CREAR GRUPOS DE APLICACIONES CON LICENCIA

Para crear un grupo de aplicaciones con licencia:

1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Uso de licencias de terceros**.
2. Haga clic en el enlace **Agregar un grupo de aplicaciones con licencia** para ejecutar el **Asistente de incorporación de grupos de aplicaciones con licencia**.
3. Siga las instrucciones del asistente.

Después de que el Asistente complete su operación, se crea y se muestra un grupo de aplicaciones con licencia en la carpeta **Uso de licencias de terceros**.

ADMINISTRACIÓN DE CLAVES PARA LOS GRUPOS DE APLICACIONES CON LICENCIA

Para crear una clave para un grupo de aplicaciones con licencia:

1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Uso de licencias de terceros**.
2. En el espacio de trabajo de la carpeta **Uso de licencias de terceros**, haga clic en el enlace **Administrar claves de aplicaciones con licencia** para abrir la ventana **Administración de claves de aplicaciones con licencia**.
3. En la ventana **Administración de claves de aplicaciones con licencia** , haga clic en el botón **Agregar**.

   Se abre la ventana **Clave**.

4. En la ventana **Clave**, especifique la configuración de la clave y las restricciones que la clave impone a grupo de aplicaciones con licencia.
   - **Nombre**. Nombre de la clave.
   - **Comentario**. Notas sobre la clave seleccionada
   - **Restricción**. El número de equipos cliente en los cuales se puede instalar la aplicación que usa esta clave.
   - **Fecha de caducidad**. Fecha de caducidad de la clave.

Las claves creadas se muestran en la ventana **Administración de claves de aplicaciones con licencia**.

Para aplicar una clave a un grupo de aplicaciones con licencia:

1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Uso de licencias de terceros**.
2. En la carpeta **Uso de licencias de terceros**, seleccione un grupo de aplicaciones con licencia al cual desea aplicar una clave.
3. Seleccione **Propiedades** en el menú contextual del grupo de aplicaciones con licencia.

   Se abre la ventana Propiedades del grupo de aplicaciones con licencia.
4. En la ventana Propiedades del grupo de aplicaciones con licencia, en la sección **Claves**, seleccione **Controlar si se excede el límite de licencia**.
5. Haga clic en el botón **Agregar**.

   Se abre la ventana **Selección de una clave**.
6. En la ventana **Selección de una clave**, seleccione una que desee aplicar al grupo de aplicaciones con licencia.
7. Haga clic en **Aceptar**.

Las restricciones impuestas a un grupo de aplicaciones con licencia y especificadas en la clave también abarcarán al grupo de aplicaciones con licencia seleccionado.

VISUALIZACIÓN DE INFORMACIÓN SOBRE ARCHIVOS EJECUTABLES

Para visualizar una lista de todos los archivos ejecutables detectados en equipos cliente,

En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Archivos ejecutables**.

El espacio de trabajo de la carpeta **Archivos ejecutables** muestra una lista de los archivos ejecutables que se ejecutaron en equipos cliente desde que se instaló el sistema operativo, o que se detectaron mientras se ejecutaba la tarea de inventario de Kaspersky Endpoint Security 10 para Windows.

Para visualizar los datos en archivos ejecutables que cumplen criterios especificados, puede usar el filtrado.

Para visualizar las propiedades de un archivo ejecutable,

seleccione **Propiedades** en el menú contextual del archivo.

Se abre una ventana que contiene información del archivo ejecutable, junto con una lista de equipos cliente en los que se ha detectado el archivo ejecutable.

VULNERABILIDADES DE LA APLICACIÓN

La carpeta **Vulnerabilidades de software** incluida en la carpeta **Administración de aplicaciones** contiene una lista de vulnerabilidades en las aplicaciones que fueron detectadas por el Agente de red instalado en los equipos cliente.

La función de análisis de información acerca de las vulnerabilidades en las aplicaciones solo está disponible para equipos que funcionen con sistemas operativos Microsoft Windows.

Al abrir la ventana de propiedades de una aplicación seleccionada en la carpeta **Vulnerabilidades de software**, se puede obtener información general acerca de una vulnerabilidad, acerca de la aplicación en la que fue detectada, ver la lista de equipos en la que se encontró la vulnerabilidad e información acerca de la solución de esta vulnerabilidad.

VISUALIZACIÓN DE INFORMACIÓN ACERCA DE VULNERABILIDADES EN LAS APLICACIONES

- *Para ver una lista de las vulnerabilidades detectadas en equipos cliente,*

  En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Vulnerabilidades de software**.

  El espacio de trabajo de la carpeta muestra una lista de las vulnerabilidades que detecta el Agente de red en aplicaciones instaladas en equipos cliente.

- *Para obtener información sobre una vulnerabilidad seleccionada,*

  seleccione **Propiedades** en el menú contextual de la vulnerabilidad.

Se abrirá la ventana Propiedades de la vulnerabilidad, con la siguiente información:

- Aplicación en la que se detectó la vulnerabilidad.
- Lista de los equipos en los cuales se detectó la vulnerabilidad.
- Información sobre si se reparó o no la vulnerabilidad.

- *Para ver el informe sobre todas las vulnerabilidades detectadas,*

  haga clic en el enlace **Ver informe sobre vulnerabilidades de software** en la carpeta **Vulnerabilidades de software**.

  Se generará un informe sobre las vulnerabilidades de las aplicaciones instaladas en equipos cliente. Puede ver el informe en la carpeta **Informes y notificaciones**.

La función de análisis de información acerca de las vulnerabilidades en las aplicaciones solo está disponible para equipos que funcionen con sistemas operativos Microsoft Windows.

BÚSQUEDA DE VULNERABILIDADES EN LAS APLICACIONES

Si configuró la aplicación a través del Asistente de inicio rápido, la tarea de análisis de vulnerabilidades se creará automáticamente. Puede ver la tarea en la carpeta **Equipos administrados** en la pestaña **Tareas**.

- *Para crear una tarea de análisis de vulnerabilidades en aplicaciones instaladas en equipos cliente:*

  1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Vulnerabilidades de software**.
  2. Haga clic en el vínculo **Configurar análisis de vulnerabilidades** en el espacio de trabajo para ejecutar el Asistente de creación de la tarea de búsqueda de actualizaciones requeridas y de vulnerabilidades.

     Se abre la ventana del Asistente de creación de la tarea.
  3. Siga las instrucciones del asistente.

  Después de que termina el Asistente, se crea la tarea **Buscar vulnerabilidades y actualizaciones de la aplicación**, que ahora se muestra en la lista de tareas en la carpeta **Equipos administrados** en la pestaña **Tareas**.

REPARACIÓN DE VULNERABILIDADES EN LAS APLICACIONES

Si seleccionó **Buscar e instalar actualizaciones de la aplicación** en la ventana **Configuración de la administración de actualizaciones** del Asistente de inicio rápido, la tarea **Instalar actualizaciones de la aplicación y reparar vulnerabilidades** se crea automáticamente. La tarea se muestra en la carpeta **Equipos administrados**, en la pestaña **Tareas**.

- *Para crear la tarea de reparación de vulnerabilidades con las actualizaciones disponibles para las aplicaciones:*

  1. En el árbol de consola, seleccione la carpeta **Equipos administrados**, en la pestaña **Tareas**.
  2. Haga clic en el enlace **Crear una tarea** para ejecutar el Asistente para nueva tarea.
  3. En la ventana **Seleccione el tipo de tarea** del Asistente, especifique el tipo de tarea **Instalar actualizaciones de la aplicación y reparar vulnerabilidades**.
  4. Siga las instrucciones del asistente.

  Después de que el Asistente termina su operación, se crea la tarea **Instalar actualizaciones de la aplicación y reparar vulnerabilidades** y se muestra en la carpeta **Equipos administrados** en la pestaña **Tareas**.

ACTUALIZACIONES DE SOFTWARE

Kaspersky Security Center permite la administración de actualizaciones de software instaladas en equipos cliente y la reparación de vulnerabilidades en aplicaciones de Microsoft y productos de otros proveedores, mediante la instalación de actualizaciones requeridas.

Kaspersky Security Center busca actualizaciones a través de la tarea de búsqueda de actualizaciones y las descarga en el almacenamiento de actualizaciones. Luego de completar la búsqueda de actualizaciones, la aplicación le proporciona al administrador información de las actualizaciones disponibles y las vulnerabilidades en aplicaciones que pueden repararse usando esas actualizaciones.

El servicio de Windows Update proporciona información de las actualizaciones disponibles para Microsoft Windows. Se puede usar el Servidor de administración como el servidor de Windows Update (WSUS). Para usar el Servidor de administración como servidor de Windows Update, debe configurar la sincronización de actualizaciones con Windows Update. Una vez que haya configurado la sincronización de datos con Windows Update, el Servidor de administración proporciona actualizaciones para los servicios de Windows Update en equipos cliente, en modo centralizado y con la frecuencia definida.

También puede administrar las actualizaciones de software mediante una directiva del Agente de red. Para realizar esto, debe crear una directiva del Agente de red y configurar actualizaciones de software en la ventana correspondiente del Asistente para nueva directiva.

El administrador puede visualizar una lista de actualizaciones disponibles en la subcarpeta **Actualizaciones de software**, incluida en la carpeta **Administración de aplicaciones**. Esta carpeta contiene una lista de actualizaciones para aplicaciones de Microsoft y productos de otros proveedores, obtenida por el Servidor de administración y que puede ser distribuida a equipos cliente. Luego de ver la información de las actualizaciones disponibles, el administrador puede instalarlas en equipos cliente.

Antes de instalar las actualizaciones en todos los equipos cliente, puede realizar una instalación de prueba para asegurarse de que las actualizaciones instaladas no causarán fallas en el funcionamiento de las aplicaciones en los equipos cliente.

EN ESTA SECCIÓN:

Visualización de información sobre actualizaciones disponibles 106

Sincronización de las actualizaciones de Windows Update con el Servidor de administración 107

Instalación automática de actualizaciones en equipos cliente 107

Instalación manual de actualizaciones en equipos cliente 108

Configuración de actualizaciones de aplicaciones en una directiva del Agente de red 109

VISUALIZACIÓN DE INFORMACIÓN SOBRE ACTUALIZACIONES DISPONIBLES

- *Para ver una lista de las actualizaciones disponibles para las aplicaciones instaladas en equipos cliente,*

  En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.

  En el espacio de trabajo de la carpeta, puede visualizar una lista de las actualizaciones disponibles para las aplicaciones instaladas en equipos cliente.

- *Para ver las propiedades de una actualización,*

  en el espacio de trabajo de la carpeta **Actualizaciones de software** , seleccione **Propiedades** en el menú contextual de la actualización.

La siguiente información se encuentra disponible en la ventana Propiedades de la actualización:

- Lista de equipos cliente para los cuales se destina la actualización (*equipos de destino*).
- Lista de componentes del sistema (requisitos previos) que deben instalarse antes de la actualización (si hubiera)
- Vulnerabilidades en aplicaciones que la actualización debe reparar.

SINCRONIZACIÓN DE LAS ACTUALIZACIONES DE WINDOWS UPDATE CON EL SERVIDOR DE ADMINISTRACIÓN

Si ha seleccionado **Usar Servidor de administración como servidor WSUS** en la ventana **Configuración de la Administración de Actualizaciones** del Asistente de inicio rápido, se crea la tarea de sincronización de Windows Update de manera automática. Puede ejecutar la tarea en la carpeta **Tareas del Servidor de administración**. La funcionalidad de actualización del software solo se encuentra disponible luego de que la tarea **Realizar la sincronización con Windows Update** se complete correctamente.

Para crear una tarea para la sincronización de las actualizaciones de Windows con el Servidor de administración, haga lo siguiente:

1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.
2. Haga clic en el vínculo **Configurar la sincronización con Windows Update** para ejecutar el Asistente de creación de la tarea de recuperación de datos del centro de actualizaciones de Windows.
3. Siga las instrucciones del asistente.

El asistente crea la tarea **Realizar la sincronización de Windows Update** que se muestra en la carpeta **Tareas del Servidor de administración**.

También puede crear la tarea de sincronización de Windows Update en la carpeta **Tareas del Servidor de administración** con un clic en el vínculo **Crear una tarea**.

INSTALACIÓN AUTOMÁTICA DE ACTUALIZACIONES EN EQUIPOS CLIENTE

Puede configurar las actualizaciones automáticas de las bases de datos y los módulos de software de Kaspersky Endpoint Security en los equipos cliente.

Para configurar la descarga e instalación automática de las actualizaciones en los equipos cliente:

1. En el árbol de consola seleccione la carpeta **Tareas para equipos específicos**.
2. Cree una tarea **Actualizar** en una de las siguientes formas:
   - En el menú contextual de la carpeta del árbol de consola denominada **Tareas para equipos específicos**, seleccione **Nuevo** → **Tarea**.
   - Haga clic en el enlace **Crear una tarea** en el espacio de trabajo.

   Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente. Cuando finaliza el asistente se crea la tarea.
3. En el espacio de trabajo de la carpeta **Tareas para equipos específicos** seleccione una tarea de actualización que haya creado.
4. En el menú contextual de la tarea, seleccione **Propiedades**.
5. En la ventana de propiedades de tareas, seleccione la sección **Configuración**.

   En la sección **Configuración** puede configurar los ajustes de la tarea de actualización en el modo local o móvil:
   - **Ajustes de actualización en modo local**: se establece una conexión entre Kaspersky Security Center y el equipo cliente.
   - **Ajustes de actualización en modo móvil**: no se establece una conexión entre Kaspersky Security Center y el equipo cliente (por ejemplo, cuando el equipo no está conectado a Internet).
6. Haga clic en el botón **Configuración** para seleccionar el origen de la actualización.
7. Seleccione la casilla **Descargar actualizaciones de módulos de software** para descargar e instalar las actualizaciones de módulos de software junto a las bases de datos de la aplicación.

Si la casilla está seleccionada, Kaspersky Endpoint Security notifica al usuario acerca de las actualizaciones de módulos de software disponibles y las incluye en el paquete de actualización mientras ejecuta la tarea de actualización. La forma en que se aplican las actualizaciones de módulos de software está determinada por los siguientes ajustes:

- **Instalar actualizaciones críticas y aprobadas**. Si esta opción está seleccionada, cuando las actualizaciones de módulos de software están disponibles Kaspersky Endpoint Security instala las actualizaciones críticas automáticamente y todas las otras actualizaciones de módulos de software, solo después que su instalación se aprueba localmente a través de la interfaz de la aplicación o por parte de Kaspersky Security Center.
- **Instalar las actualizaciones aprobadas únicamente**. Si esta opción está seleccionada, cuando las actualizaciones de módulos de software están disponibles Kaspersky Endpoint Security las instala solo después que su instalación se aprueba localmente a través de la interfaz de la aplicación o por parte de Kaspersky Security Center.

Si las actualizaciones de módulos de software requieren revisar y aceptar los términos del Contrato de Licencia de usuario final, la aplicación instala las actualizaciones, después que el usuario ha aceptado los términos del Contrato de Licencia de usuario final.

8. Seleccione la casilla **Copiar actualizaciones a la carpeta** a fin de que la aplicación guarde las actualizaciones descargadas en la carpeta especificada al hacer clic en el botón **Examinar**.
9. Haga clic en **Aceptar**.

INSTALACIÓN MANUAL DE ACTUALIZACIONES EN EQUIPOS CLIENTE

Si seleccionó **Buscar e instalar actualizaciones de la aplicación** en la ventana **Configuración de la administración de actualizaciones** del Asistente de inicio rápido, la tarea **Instalar actualizaciones de la aplicación y reparar vulnerabilidades** se crea automáticamente. Puede iniciar o detener la tarea en la carpeta **Equipos administrados** en la pestaña **Tareas**.

Si seleccionó **Buscar actualizaciones críticas** en el Asistente de inicio rápido, puede instalar las actualizaciones de software en equipos cliente a través de la tarea **Instalar actualizaciones de la aplicación y reparar vulnerabilidades**.

Para crear una tarea de instalación de actualizaciones, realice lo siguiente:

1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.
2. En la carpeta **Actualizaciones de software**, abra el menú contextual de una actualización y seleccione **Instalar actualización** → **Nueva tarea**, o haga clic en el vínculo **Instalar actualización (crear tarea)** en la sección destinada para manejar las actualizaciones seleccionadas.

   Esto abre el Asistente de creación de tareas de instalación y reparación de vulnerabilidades.
3. Siga las instrucciones del asistente.

Después de que el Asistente termina su operación, se crea la tarea **Instalar actualizaciones de la aplicación y reparar vulnerabilidades** y se muestra en la carpeta **Equipos administrados** en la pestaña **Tareas**.

Puede habilitar la instalación automática de los componentes del sistema (requisitos previos) antes de la instalación de una actualización en las propiedades de la tarea Instalar aplicaciones y reparar vulnerabilidades. Cuando esta opción esté habilitada, todos los componentes del sistema requeridos se instalan antes de la actualización. Puede encontrarse una lista de los componentes requeridos en las propiedades de la actualización.

En las propiedades de la tarea Instalar aplicaciones y reparar vulnerabilidades, puede permitir la instalación de actualizaciones que actualizan la aplicación a una nueva versión.

La actualización a una nueva versión de una aplicación puede provocar el mal funcionamiento de las aplicaciones dependientes en los equipos cliente.

En la configuración de la tarea de instalación de actualizaciones, puede configurar una instalación de prueba de las actualizaciones.

Para configurar una instalación de prueba de las actualizaciones:

1. En el árbol de consola, seleccione la tarea **Instalar actualizaciones de la aplicación y reparar vulnerabilidades** en la pestaña **Tareas** de la carpeta **Equipos administrados**.
2. Seleccione **Propiedades** en el menú contextual de la tarea.

   Se abre la ventana propiedades de la tarea **Instalar actualizaciones de la aplicación y reparar vulnerabilidades**.

3. En la ventana Propiedades de la tarea, en la sección **Instalación de prueba**, seleccione una de las opciones disponibles para la instalación de prueba:
   - **No analizar**. Seleccione esta opción si no desea realizar una instalación de prueba de las actualizaciones.
   - **Analizar los equipos seleccionados**. Seleccione esta opción si desea probar la instalación de actualizaciones en equipos seleccionados. Haga clic en el botón **Agregar** y seleccione los equipos en los que desea realizar una instalación de prueba de las actualizaciones.
   - **Analizar los equipos del grupo especificado**. Seleccione esta opción si desea probar la instalación de actualizaciones en un grupo de equipos. En el campo **Especifique un grupo de prueba**, especifique un grupo de equipos en el que desee realizar una instalación de prueba.
   - **Instalar en el porcentaje especificado de equipos**. Seleccione esta opción si desea probar la instalación de actualizaciones en una parte de los equipos de destino. En el campo **Porcentaje de equipos de prueba en relación con todos los equipos de destino**, especifique el porcentaje de equipos en el que desea realizar una instalación de prueba de las actualizaciones.
4. Una vez que haya seleccionado alguna de estas opciones, siempre y cuando no sea la primera, en el campo **Tiempo para tomar la decisión de si se debe continuar la instalación**, especifique la cantidad de horas que deben transcurrir desde la instalación de prueba de las actualizaciones hasta el inicio de la instalación de las actualizaciones en todos los equipos de destino.

CONFIGURACIÓN DE ACTUALIZACIONES DE APLICACIONES EN UNA DIRECTIVA DEL AGENTE DE RED

Para configurar actualizaciones de Windows en equipos cliente en una directiva del Agente de red:

1. En la carpeta **Equipos administrados**, seleccione la pestaña **Directivas** y haga clic en el enlace **Crear una directiva** para ejecutar el Asistente para nueva directiva.
2. En la ventana **Seleccionar aplicación para la cual desea crear una directiva de grupo** del Asistente, elija el **Agente de red** de Kaspersky Security Center como aplicación.
3. En la ventana **Actualizaciones y vulnerabilidades de software** del Asistente, seleccione la casilla **Usar Servidor de administración como servidor WSUS**, si desea usar el Servidor de administración como el servidor de actualización.

   En este caso, las actualizaciones se descargarán en el Servidor de administración y se instalarán en los equipos cliente a través del Agente de red. Si la casilla de verificación está desactivada, el Servidor de administración no se usará para descargar e instalar las actualizaciones de Windows.
4. En la ventana **Actualizaciones y vulnerabilidades de software** del Asistente, en la sección **Modo de búsqueda de Windows Update**, seleccione una de las siguientes opciones:
   - **Activo**. El Servidor de administración con soporte del Agente de red inicia una solicitud desde Windows Update en un equipo cliente para un origen de actualizaciones: Servidores de Windows Update o WSUS. Después, el Agente de red pasa la información recibida de Windows Update al Servidor de administración.
   - **Pasivo**. Si selecciona esta opción, el Agente de red le pasará periódicamente al Servidor de administración la información de Windows Update sobre las actualizaciones que obtenga en la última sincronización de Windows Update con el origen de actualizaciones. Si no se realiza ninguna sincronización de Windows Update con el origen de actualizaciones, el Servidor de administración tendrá desactualizada la información sobre las actualizaciones.
   - **Deshabilitado**. El Servidor de administración no recopila información sobre las actualizaciones.

La directiva recién creada se muestra en la carpeta **Equipos administrados**, en la pestaña **Directivas**.

Si ya se creó la directiva del Agente de red, realice las siguientes acciones:

1. En la carpeta **Equipos administrados**, en la pestaña **Directivas**, seleccione una directiva del Agente de red.
2. En el menú contextual de la directiva, seleccione **Propiedades**. Abra la ventana Propiedades de la directiva del Agente de red.
3. En la ventana Propiedades de la directiva del Agente de red, configure Windows Update en la sección **Actualizaciones y vulnerabilidades de software**.

INSTALACIÓN REMOTA DE SISTEMAS OPERATIVOS Y APLICACIONES

Kaspersky Security Center permite crear imágenes de los sistemas operativos y distribuirlas en los equipos cliente de la red, como también permite realizar la instalación remota de las aplicaciones de Kaspersky Lab y de otros proveedores.

Capturar imágenes de sistemas operativos

Kaspersky Security Center puede capturar imágenes de los sistemas operativos de los equipos de destino y transferir esas imágenes al Servidor de administración. Estas imágenes de los sistemas operativos se almacenan en el Servidor de administración, en una carpeta dedicada. Se puede capturar y crear la imagen del sistema operativo de un equipo de referencia utilizando la tarea Agregar un nuevo paquete (ver la sección “Creación de un paquete de instalación de una aplicación” en la página 114).

Para crear imágenes de los sistemas operativos, debe instalarse en el Servidor de administración el Kit de instalación automatizada de Windows (WAIK).

La funcionalidad de la captura de imágenes de los sistemas operativos tiene las siguientes características:

- No se puede capturar una imagen de un sistema operativo en un equipo en el que está instalado el Servidor de administración.
- Mientras se captura una imagen del sistema operativo, una utilidad denominada sysprep.exe restablece la configuración del equipo de referencia. Si necesita restaurar la configuración del equipo de referencia, debe seleccionar la casilla **Guardar copia de seguridad del equipo** en el Asistente de creación de imágenes del sistema operativo.
- El proceso de captura de imágenes posibilita el reinicio del equipo de referencia.

Distribución de imágenes de sistemas operativos en equipos nuevos

El administrador puede usar esas imágenes para implementarlas en nuevos equipos de la red, sobre los cuales no se ha instalado ningún sistema operativo aún. En este caso se utiliza una tecnología denominada Preboot eXecution Environment (PXE). El administrador selecciona un equipo en red que se utilizará como servidor PXE. Este equipo debe reunir los siguientes requisitos:

- El Agente de red debe estar instalado en el equipo.
- No debe haber ningún servidor DHCP activo en el equipo, ya que el servidor PXE utiliza los mismos puertos que un servidor DHCP.
- El segmento de la red que abarca al equipo no debe contener ningún otro servidor PXE.

Deben reunirse las siguientes condiciones para distribuir un sistema operativo: el equipo debe tener montada una tarjeta de red, debe estar conectado a la red y al iniciarse, debe tener seleccionada en BIOS la opción Inicio de red.

La distribución de un sistema operativo se realiza de la siguiente manera:

1. El servidor PXE establece conexión con un equipo cliente nuevo mientras este se inicia.
2. El equipo cliente se incluye en el Entorno de preinstalación de Windows (WinPE).

   Agregar el equipo cliente al entorno WinPE puede requerir configuración del conjunto de controladores de WinPE.
3. El equipo cliente se registra en el Servidor de administración.
4. El administrador le asigna al equipo cliente un paquete de instalación con una imagen del sistema operativo.

   El administrador puede agregar controladores requeridos al paquete de instalación con la imagen del sistema operativo y especificar un archivo de configuración con la configuración del sistema operativo (archivo de respuesta) que debe aplicarse durante la instalación.
5. El sistema operativo se distribuye en el equipo cliente.

El administrador puede especificar manualmente las direcciones MAC de los equipos cliente que aún no se han conectado y asignarles el paquete de instalación con la imagen del sistema operativo. Cuando los equipos cliente seleccionados se conectan al servidor PXE, es sistema operativo se instala automáticamente en esos equipos.

Distribuir imágenes de sistemas operativos en equipos donde ya se ha instalado otro sistema operativo

La distribución de imágenes de sistemas operativos en equipos cliente donde ya se ha instalado otro sistema operativo se realiza a través de la tarea de instalación remota para equipos específicos.

Instalación de aplicaciones desarrolladas por Kaspersky Lab y otros proveedores

El administrador puede crear paquetes de instalación de cualquier aplicación, incluso aquellas especificadas por el usuario, e instalar estas aplicaciones en equipos cliente a través de la tarea de instalación remota.

EN ESTA SECCIÓN:

Crear imágenes de sistemas operativos 111
Agregar controladores para el Entorno de preinstalación de Windows (WinPE) 111
Agregar controladores a un paquete de instalación con una imagen del sistema operativo 112
Configurar la utilidad sysprep.exe 112
Distribuir sistemas operativos en los nuevos equipos de la red 113
Distribuir sistemas operativos en los equipos cliente 113
Crear paquetes de instalación de aplicaciones 114
Instalar aplicaciones en los equipos cliente 114

CREAR IMÁGENES DE SISTEMAS OPERATIVOS

Las imágenes de los sistemas operativos se crean por medio de la tarea de creación de imágenes del sistema operativo del equipo de referencia.

Para crear la tarea de creación de imágenes del sistema operativo del equipo de referencia:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. Haga clic en el enlace **Crear paquete de instalación** para ejecutar el Asistente de nuevo paquete.
3. En la ventana **Seleccionar el tipo de paquete de instalación** del Asistente, haga clic en el botón **Crear paquete de instalación basado en la imagen del SO del equipo de referencia**.
4. Siga las instrucciones del asistente.

Las actividades del Asistente crean una tarea del Servidor de administración que se denomina **Copiar la imagen del SO del equipo**. Puede visualizar la tarea en la carpeta **Tareas del Servidor de administración**.

Cuando se completa la tarea **Copiar la imagen del SO del equipo**, se crea un paquete de instalación que puede usar para distribuir el sistema operativo en los equipos cliente a través de un servidor PXE o de la tarea de instalación remota. Puede ver el paquete de instalación en la carpeta **Paquetes de instalación**.

AGREGAR CONTROLADORES PARA EL ENTORNO DE PREINSTALACIÓN DE WINDOWS (WINPE)

Para agregar controladores para WinPE, realice lo siguiente:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Distribución de imágenes de equipo**.
2. En el espacio de trabajo de la carpeta **Distribución de imágenes de equipo**, haga clic en el enlace **Configurar conjunto de controladores para el Entorno de preinstalación de Windows (WinPE)** para abrir la ventana **Controladores del Entorno de preinstalación de Windows**.
3. En la ventana **Controladores del Entorno de preinstalación de Windows**, haga clic en el botón **Agregar**.

   Se abre la ventana **Agregar controlador**.

4. En la ventana **Agregar controlador**, especifique el nombre de un controlador y la ruta del paquete de instalación. Puede especificar la ruta a un paquete de instalación haciendo clic en el botón **Seleccionar** en la ventana **Agregar controlador**.
5. Haga clic en **Aceptar**.

   El controlador se agregará al repositorio del Servidor de administración. Cuando se agrega al repositorio, el controlador se muestra en la ventana **Seleccionar controlador**.
6. Haga clic en **Aceptar** en la ventana **Seleccionar controlador**.

El controlador se agregará al Entorno de preinstalación de Windows (WinPE).

AGREGAR CONTROLADORES A UN PAQUETE DE INSTALACIÓN CON UNA IMAGEN DEL SISTEMA OPERATIVO

Para agregar controladores a un paquete de instalación con una imagen del sistema operativo, realice lo siguiente:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. Desde el menú contextual de un paquete de instalación con una imagen del sistema operativo, seleccione **Propiedades**.

   Se abre la ventana de propiedades del paquete de instalación.
3. En la ventana de propiedades del paquete de instalación, seleccione la sección **Controladores adicionales**.
4. Haga clic en el botón **Agregar** en la sección **Controladores adicionales**.

   Se abre la ventana **Seleccionar controlador**.
5. En la ventana **Seleccionar controlador**, seleccione los controladores que desea agregar al paquete de instalación con la imagen del sistema operativo.

   Puede agregar nuevos controladores al repositorio del Servidor de administración haciendo clic en el botón **Agregar** en la ventana **Seleccionar controlador**.
6. Haga clic en **Aceptar**.

Los controladores agregados se muestran en la sección **Controladores adicionales** de la ventana de propiedades del paquete de instalación con la imagen del sistema operativo.

CONFIGURAR LA UTILIDAD SYSPREP.EXE

La utilidad sysrep.exe está destinada a preparar al equipo para la creación de una imagen del sistema operativo.

Para configurar la utilidad sysprep.exe, realice lo siguiente:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. Desde el menú contextual de un paquete de instalación con una imagen del sistema operativo, seleccione **Propiedades**.

   Se abre la ventana de propiedades del paquete de instalación.
3. En la ventana de propiedades del paquete de instalación, seleccione la sección de **configuración de sysprep.exe**.
4. En la sección de **configuración de sysprep.exe**, especifique el archivo de configuración que se usará al momento de distribuir el sistema operativo en el equipo cliente:
   - **Usar archivo de configuración predeterminado**. Seleccione esta opción para usar el archivo de respuesta generado de forma predeterminada cuando se captura la imagen del sistema operativo.
   - **Personalizar valores de configuración principales**. Seleccione esta opción para especificar valores para la configuración a través de la interfaz de usuario.
   - **Especificar el archivo de configuración**. Seleccione esta opción para usar un archivo de respuesta personalizado.
5. Para aplicar los cambios realizados, haga clic en el botón **Aplicar**.

DISTRIBUIR SISTEMAS OPERATIVOS EN LOS NUEVOS EQUIPOS DE LA RED

- *Para distribuir un sistema operativo en equipos nuevos a los que aún no se les ha instalado ningún sistema operativo, realice lo siguiente:*

  1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Distribución de imágenes de equipo**.
  2. Haga clic en el enlace **Administrar la lista de servidores PXE en la red** en la carpeta **Distribución de imágenes del equipo** para abrir la ventana **Propiedades Distribución de imágenes de equipo** en la sección **Servidores PXE**.
  3. Haga clic en el botón **Agregar** en la sección **Servidores PXE**. En la ventana **servidores PXE** que se abre, seleccione el equipo que se utilizará como servidor PXE.

     El equipo agregado se mostrará en la sección servidores PXE.
  4. En la sección **Servidores PXE**, seleccione un servidor PXE y haga clic en el botón **Propiedades**.
  5. En la ventana Propiedades del servidor PXE seleccionado, en la pestaña **Configuración de conexión del servidor PXE** configure la conexión entre el Servidor de administración y el servidor PXE.
  6. Inicie el equipo cliente en el que desea distribuir el sistema operativo.
  7. En el BIOS del equipo cliente, seleccione la opción de instalación de inicio de red.

     El equipo cliente se conecta al servidor PXE y se muestra luego en el espacio de trabajo de la carpeta **Distribución de imágenes de equipo**.
  8. En la sección **Acciones**, haga clic en el enlace **Asignar paquete de instalación** para seleccionar un paquete de instalación que se utilizará para instalar el sistema operativo en el equipo seleccionado.

     Después de agregar un equipo y asignarle un paquete de instalación, la distribución del sistema operativo comienza automáticamente en este equipo.
  9. Para cancelar la distribución de un sistema operativo en un equipo cliente, haga clic en el enlace **Cancelar instalación de imagen de SO** en la sección **Acciones**.

- *Para agregar equipos por dirección MAC:*

  - Haga clic en el enlace **Agregar dirección MAC del equipo de destino** en la carpeta **Distribución de imágenes de equipo** para abrir la ventana **Nuevo equipo de destino** y especifique la dirección MAC del equipo que desea agregar.
  - Haga clic en el enlace **Importar direcciones MAC de los equipos de destino desde un archivo** en la carpeta **Distribución de imágenes de equipo** para seleccionar un archivo que contenga una lista de direcciones MAC de todos los equipos en los que desee distribuir un sistema operativo.

DISTRIBUIR SISTEMAS OPERATIVOS EN LOS EQUIPOS CLIENTE

- *Para distribuir un sistema operativo en equipos cliente con otro sistema operativo instalado:*

  1. En la carpeta **Instalación remota** del árbol de consola, haga clic en el enlace **Iniciar Asistente de instalación remota** para ejecutar el asistente.
  2. En la ventana **Seleccionar paquete de instalación** del Asistente, especifique los paquetes de instalación con una imagen del sistema operativo.
  3. Siga las instrucciones del asistente.

  Las actividades del Asistente crean una tarea de instalación remota para instalar el sistema operativo en los equipos cliente. Puede iniciar o detener la tarea en la carpeta **Tareas para equipos específicos**.

CREAR PAQUETES DE INSTALACIÓN DE APLICACIONES

Para crear un paquete de instalación de una aplicación:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. Haga clic en el enlace **Crear paquete de instalación** para ejecutar el Asistente de nuevo paquete.
3. En la ventana **Seleccionar el tipo de paquete de instalación** del Asistente, haga clic en uno de los siguientes botones:
   - **Crear paquete de instalación para una aplicación de Kaspersky Lab**. Seleccione esta opción si desea crear un paquete de instalación para una aplicación de Kaspersky Lab.
   - **Crear un paquete de instalación para el archivo ejecutable especificado**. Seleccione esta opción si desea crear un paquete de instalación para una aplicación solicitada por el usuario.
   - **Crear paquete de instalación basado en la imagen del SO del equipo de referencia**. Seleccione esta opción si desea crear un paquete de instalación con una imagen del sistema operativo de un equipo de referencia.

     Las actividades del Asistente crean una tarea del Servidor de administración que se denomina **Copiar la imagen del SO del equipo**. Cuando se completa esta tarea, se crea un paquete de instalación que puede usar para distribuir la imagen del sistema operativo a través de un servidor PXE o de la tarea de instalación remota.
4. Siga las instrucciones del asistente.

Las actividades del Asistente crean un paquete de instalación que puede usar para instalar la aplicación en los equipos cliente. Puede ver el paquete de instalación en la carpeta **Paquetes de instalación**.

Para obtener información detallada de los paquetes de instalación, consulte la *Guía de implementación de Kaspersky Security Center*.

INSTALAR APLICACIONES EN LOS EQUIPOS CLIENTE

Para instalar una aplicación en equipos cliente:

1. En la carpeta **Instalación remota** del árbol de consola, haga clic en el enlace **Iniciar Asistente de instalación remota** para ejecutar el asistente.
2. En la ventana **Seleccionar paquete de instalación** del Asistente, especifique el paquete de instalación de una aplicación que desee instalar.
3. Siga las instrucciones del asistente.

Las actividades del Asistente crean una tarea de instalación remota para instalar la aplicación en los equipos cliente. Puede iniciar o detener la tarea en la carpeta **Tareas para equipos específicos**.

ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES

Esta sección describe cómo administrar los dispositivos móviles conectados al Servidor de administración. Para conocer los detalles sobre cómo conectar dispositivos móviles, consulte la *Guía de implementación de Kaspersky Security Center*.

EN ESTA SECCIÓN:

Administración de dispositivos móviles mediante una directiva MDM 115

Manejo de comandos para dispositivos móviles 116

Manejo de certificados 119

Administración de dispositivos móviles de Exchange ActiveSync 121

Administración de dispositivos móviles con MDM de iOS 124

Administración de dispositivos KES 130

ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES MEDIANTE UNA DIRECTIVA MDM

Para administrar los dispositivos con MDM de iOS y EAS puede utilizar el complemento de administración de Kaspersky Mobile Device Management 10 Service Pack 1, que está incluido en el kit de distribución de Kaspersky Security Center. Kaspersky Mobile Device Management le permite crear directivas de grupo para especificar la configuración de dispositivos MDM de iOS y EAS. Una directiva de grupo que permite modificar la configuración de dispositivos con MDM de iOS y EAS sin usar la iPhone Configuration Utility y el perfil de administración de Exchange Active Sync, se llama directiva MDM.

Una directiva MDM proporciona al administrador las siguientes opciones:

- Para administrar dispositivos EAS:
  - Configuración de la contraseña de desbloqueo del dispositivo.
  - Configuración del almacenamiento de datos en el dispositivo en forma cifrada.
  - Configuración de la sincronización del correo corporativo.
  - Configuración de las características de hardware de los dispositivos móviles, tales como el uso de medios extraíbles, el uso de la cámara o de Bluetooth
  - Configuración de las restricciones sobre el uso de aplicaciones móviles en el dispositivo.
- Para administrar dispositivos MDM de iOS:
  - Configuración de la seguridad de la contraseña del dispositivo.
  - Configuración de restricciones en el uso de características de hardware del dispositivo, sobre la instalación y eliminación de aplicaciones móviles.
  - Configuración de restricciones en el uso de aplicaciones móviles preinstaladas, tales como YouTube, iTunes Store y Safari.
  - Configuración de las restricciones sobre contenido de medios visualizado (tal como películas y programas de televisión) por región en la que se encuentre el dispositivo.
  - Configuración de la conexión del dispositivo a Internet a través del servidor proxy (Proxy HTTP global).
  - Configuración de los ajustes de la cuenta con la que el usuario puede acceder a las aplicaciones y servicios corporativos (tecnología Single Sign On).
  - Monitoreo del uso de Internet (visitas a sitios web) en dispositivos móviles.

- Configuración de redes inalámbricas (Wi-Fi), puntos de acceso (APN) y redes privadas virtuales (VPN) que usan diferentes mecanismos de autenticación y protocolos de red.
- Configuración de la conexión a dispositivos AirPlay para la transmisión de fotos, música y videos.
- Configuración de la conexión a impresoras AirPrint para la impresión inalámbrica de documentos desde el dispositivo.
- Configuración de la sincronización con el servidor Microsoft Exchange y cuentas de usuario para usar correo electrónico corporativo en los dispositivos.
- Configuración de cuentas de usuario para la sincronización con el servicio de directorio LDAP.
- Configuración de las cuentas de usuario para la conexión con los servicios CalDAV y CardDAV que dan al usuario acceso a los calendarios y listas de contactos corporativos.
- Configuración de la interfaz iOS en el dispositivo del usuario, tal como fuentes o iconos para sitios web favoritos.
- Adición de nuevos certificados de seguridad en dispositivos.
- Configuración del servidor SCEP para la recuperación automática de certificados mediante el dispositivo del Centro de certificación.
- Adición de configuración personalizada para la operación de aplicaciones móviles.

Los principios operativos generales de una directiva MDM no difieren de los principios operativos de las directivas creadas para administrar otras aplicaciones. Una directiva MDM es especial porque se asigna a un grupo de administración que incluye el Servidor de dispositivos móviles con MDM de iOS y el servidor de dispositivos móviles Exchange Active Sync (en adelante, "servidores de dispositivos móviles"). Todos las configuraciones especificadas en una directiva MDM se aplican en primer lugar a los servidores de dispositivos móviles y luego a los dispositivos móviles administrados por estos. En el caso de una estructura jerárquica de grupos de administración, los servidores de dispositivos móviles secundarios reciben la configuración de directivas MSM de los servidores de dispositivos móviles maestros y la distribuyen a los dispositivos móviles.

Para obtener información detallada sobre cómo usar la directiva MDM en la Consola de administración de Kaspersky Security Center, consulte la Guía del administrador de Kaspersky Security Mobile.

MANEJO DE COMANDOS PARA DISPOSITIVOS MÓVILES

Esta sección brinda información sobre los comandos para administración de dispositivos móviles admitidos por la aplicación. La sección proporciona instrucciones sobre cómo enviar comandos a dispositivos móviles, además de cómo ver los estados de ejecución de los comandos en el registro de comandos.

COMANDOS PARA ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES

La aplicación admite comandos para la administración de dispositivos móviles.

Este tipo de comandos se usa para la administración remota de dispositivos móviles. Por ejemplo, en caso de perder su dispositivo móvil, puede eliminar todos los datos corporativos del dispositivo mediante el uso de un comando.

Los comandos se usan en tres tipos de dispositivos móviles:

- Dispositivos con MDM de iOS
- Dispositivos KES
- Dispositivos EAS.

Cada tipo de dispositivo admite un conjunto dedicado de comandos. La tabla siguiente muestra conjuntos de comandos para cada uno de los tipos de dispositivos.

Si el comando **Eliminar datos** se ejecuta exitosamente, todos los datos se eliminarán del dispositivo y la configuración del dispositivo se revertirá a sus valores originales, en todos los tipos de dispositivos.

Después de la ejecución exitosa del comando **Eliminar datos corporativos** en un dispositivo con MDM de iOS, todos los perfiles de configuración instalados, los perfiles de aprovisionamiento, el perfil de MDM de iOS y las aplicaciones para las que se ha seleccionado la casilla **Eliminar junto con el perfil MDM de iOS** se eliminan del dispositivo.

Si el comando **Eliminar datos corporativos** se ejecuta exitosamente en un dispositivo KES, todos los datos corporativos, la entradas en Contactos, el historial de mensajes SMS, el registro de llamadas, el calendario, la configuración de conexión a Internet y las cuentas del usuario, excepto por la cuenta de Google, se eliminarán del dispositivo. Para un dispositivo KES, también se eliminarán todos los datos de la tarjeta de memoria.

Tabla 10. Lista de comandos admitidos

TIPO DE DISPOSITIVO MÓVIL	COMANDOS	RESULTADO DE LA EJECUCIÓN DEL COMANDO
Dispositivo con MDM de iOS	Bloqueo	Dispositivo bloqueado.
	Desbloquear	El bloqueo del dispositivo con un código PIN está deshabilitado. Se ha restablecido el código PIN anteriormente especificado.
	Eliminar datos	Se han eliminado todos los datos del dispositivo, la configuración se revertió a sus valores originales.
	Eliminar datos corporativos	Todos los perfiles de configuración instalados, los perfiles de aprovisionamiento, el perfil de MDM de iOS y las aplicaciones para las que se ha seleccionado la casilla **Eliminar junto con el perfil MDM de iOS** se eliminan del dispositivo.
	Forzar sincronización	Datos del dispositivo sincronizados con el Servidor de administración.
	Instalar perfil	Perfil de configuración instalado en el dispositivo.
	Eliminar perfil	Perfil de configuración eliminado del dispositivo.
	Instalar perfil de aprovisionamiento	Perfil de aprovisionamiento instalado en el dispositivo.
	Eliminar perfil de aprovisionamiento	Perfil de aprovisionamiento eliminado del dispositivo.
	Instalar aplicación	Aplicación instalada en el dispositivo.
	Eliminar aplicación	Aplicación eliminada del dispositivo.
	Introducir código de canje	Código de canje ingresado para una aplicación paga.
	Configurar roaming	Roaming de datos y de voz habilitados o deshabilitados.
Dispositivo KES	Bloqueo	Dispositivo bloqueado.
	Desbloquear	El bloqueo del dispositivo con un código PIN está deshabilitado. Se ha restablecido el código PIN anteriormente especificado.
	Eliminar datos	Se han eliminado todos los datos del dispositivo, la configuración se revertió a sus valores originales.
	Eliminar datos corporativos	Se han eliminado los datos corporativos, las entradas en Contactos, el historial de mensajes SMS, el registro de llamadas, el calendario, la configuración de conexión a Internet, las cuentas de usuario (excepto la cuenta de Google). Se han borrado los datos de la tarjeta de memoria.
	Localizar	Dispositivo bloqueado. Dispositivos localizado y mostrado en Google Maps™. El operador de servicios móviles aplica un cargo por enviar el mensaje de texto y por proporcionar la conexión a Internet.
	Foto policial	Dispositivo bloqueado. Se ha tomado la foto mediante la cámara frontal del dispositivo y se ha guardado en el Servidor de administración. Las fotos pueden visualizarse en el registro de comandos. El operador de servicios móviles aplica un cargo por enviar el mensaje de texto y por proporcionar la conexión a Internet.

TIPO DE DISPOSITIVO MÓVIL	COMANDOS	RESULTADO DE LA EJECUCIÓN DEL COMANDO
	Alarma	Dispositivo bloqueado. El dispositivo emite una señal sonora.
	Forzar sincronización	Datos del dispositivo sincronizados con el Servidor de administración.
Dispositivo EAS	Eliminar datos	Se han eliminado todos los datos del dispositivo, la configuración se revertió a sus valores originales.

UTILIZANDO GOOGLE CLOUD MESSAGING

Para asegurar la entrega a tiempo de los comandos a los dispositivos KES administrados por sistemas operativos Android, Kaspersky Security Center utiliza el mecanismo de notificaciones push. Las notificaciones push se intercambian entre los dispositivos KES y el Servidor de Administración mediante Google Cloud Messaging. En la Consola de administración de Kaspersky Security Center, puede definir la configuración de Google Cloud Messaging para conectar los dispositivos KES al servicio.

Para recuperar la configuración de Google Cloud Messaging, el administrador debe tener una cuenta Google. Para más detalles sobre cómo recuperar la configuración de Google Cloud Messaging, diríjase al artículo correspondiente en la Base de Datos de Conocimientos en el sitio web de Soporte Técnico http://support.kaspersky.com/11770.

Para configurar Google Cloud Messaging:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.
2. En el menú contextual de la carpeta **Dispositivos Móviles**, seleccione **Propiedades**.

   Se abre la ventana de propiedades de la carpeta **Dispositivos Móviles**.
3. Seleccione la sección **Configuración de Google Cloud Messaging**.
4. En el campo **Id. del remitente**, especifique el número de un proyecto de API de Google que haya recibido al crearlo en la Consola del Desarrollador de Google.
5. En el campo **Clave API**, ingrese una clave de API común que haya creado en la Consola del Desarrollador de Google.

En la próxima sincronización con el servidor de administración, los dispositivos KES administrados por sistemas operativos Android conectados a Google Cloud Messaging.

Puede editar la configuración de Google Cloud Messaging al hacer clic en el botón **Restaurar configuración**.

ENVIAR COMANDOS

Para enviar un comando al dispositivo móvil del usuario:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. Seleccione el dispositivo móvil del usuario al que necesita enviar un comando.
3. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.
4. En la ventana **Comandos para administración de dispositivos móviles** vaya a la sección con el nombre del comando que necesita enviar al dispositivo móvil, luego haga clic en el botón **Enviar comando**.

   Según el comando que haya seleccionado, haga clic en el botón **Enviar comando** para abrir la ventana de configuración avanzada de la aplicación. Por ejemplo, cuando envía el comando para eliminar un perfil de aprovisionamiento de un dispositivo, la aplicación le solicita que seleccione el perfil de aprovisionamiento que debe eliminarse del dispositivo. Defina la configuración avanzada del comando en esa ventana y confirme su selección. Después de esto, el comando se enviará al dispositivo móvil.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo, con los estados de ejecución respectivos. Puede hacer clic en el botón **Actualizar** para actualizar la lista de comandos.

5. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para administración de dispositivos móviles**.

VER LOS ESTADOS DE LOS COMANDOS EN EL REGISTRO DE COMANDOS

La aplicación guarda en el registro de comandos la información acerca de todos los comandos que se han enviado a los dispositivos móviles. El registro de comandos contiene información acerca de la fecha y hora en que se envió cada comando al dispositivo, sus estados y las descripciones detalladas de los resultados de ejecución del comando. Por ejemplo, en caso de que el comando falle al ser ejecutado, el registro muestra la causa del error. Los registros se almacenan en el registro de comandos por 30 días como máximo.

Los comandos enviados a los dispositivos móviles pueden tener los siguientes estados:

- *En ejecución:* el comando se envió al dispositivo
- *Completado:* la ejecución del comando ha finalizado exitosamente
- *Completado con error:* la ejecución del comando falló
- *Eliminando:* el comando se está eliminando de la cola de comandos enviados al dispositivo móvil
- *Eliminado:* el comando se ha eliminado de la cola de comandos enviados al dispositivo móvil
- *Error al eliminar:* el comando no se pudo eliminar de la cola de comandos enviados al dispositivo móvil.

La aplicación mantiene un registro de comandos para cada dispositivo móvil.

➡ *Para ver el registro de comandos que se han enviado a un dispositivo móvil:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En la lista de dispositivos móviles, seleccione aquel para el que desee ver el registro de comandos.
3. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

   Se abre la ventana **Comandos para administración de dispositivos móviles**. Las secciones de la ventana **Comandos para administración de dispositivos móviles** corresponden a los comandos que pueden enviarse al dispositivo móvil.

4. Seleccione las secciones con los comandos que necesita y vea información acerca de cómo se envían y ejecutan los comandos al abrir la sección **Registro de comandos**.

En la sección **Registro de comandos**, puede ver la lista de comandos que se han enviado al dispositivo móvil y detalles sobre esos comandos. El filtro **Mostrar comandos** le permite mostrar solo los comandos con el estado seleccionado en la lista.

MANEJO DE CERTIFICADOS

Esta sección brinda información sobre cómo manejar los certificados de dispositivos móviles. Esta sección contiene instrucciones sobre cómo instalar certificados en los dispositivos móviles del usuario y cómo configurar las reglas para manejarlos. Esta sección también contiene instrucciones sobre cómo integrar la aplicación con la Infraestructura de claves públicas y cómo configurar la compatibilidad de Kerberos.

INSTALACIÓN DE UN CERTIFICADO

Puede instalar tres tipos de certificados en el dispositivo móvil de un usuario:

- Certificados generales para identificar el dispositivo móvil
- Certificados de correo para configurar el correo corporativo en el dispositivo móvil
- Certificado VPN para configurar el acceso a una red privada virtual en el dispositivo móvil

Para instalar un certificado en el dispositivo móvil de un usuario:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
2. En el espacio de trabajo de la carpeta **Certificados** haga clic en el enlace **Agregar certificado** para ejecutar el Asistente de instalación de certificados.

Siga las instrucciones del asistente.

Después de que el Asistente finalice sus actividades, se creará un certificado y se añadirá a la lista de certificados del usuario; además se le enviará una notificación con un enlace para descargar e instalar el certificado en el dispositivo móvil. Puede ver la lista de todos los certificados y exportarla a un archivo (consulte la sección "Visualización de la lista de certificados entregados a un usuario" en la página 86). Puede eliminar o volver a entregar certificados, así como ver sus propiedades.

CONFIGURAR REGLAS DE MANEJO DE CERTIFICADOS

Para configurar las reglas de manejo de certificados:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
2. En el espacio de trabajo de la carpeta **Certificados** haga clic en el enlace **Configurar reglas de manejo de certificados** para abrir la ventana **Reglas de generación de certificados**.
3. Vaya a la sección con el nombre de un tipo de certificado:

   Generación de certificados de tipo general: para configurar el manejo de certificados de tipo general.

   Generación de certificados de correo: para configurar el manejo de certificados de correo.

   Generación de certificados VPN: para configurar el manejo de certificados VPN.
4. En la sección **Configuración de generación** configure el manejo del certificado:
   - Seleccione una fuente de los certificados (**Servidor de administración** o **Los certificados se especifican manualmente**).

     El Servidor de administración está seleccionado como la fuente predeterminada de los certificados.
   - Especifique una plantilla de certificado (**Plantilla predeterminada**, **Otra plantilla**).

     La configuración de plantillas está disponible si la sección **Integración con PKI** cuenta con la integración con la infraestructura de claves públicas configurada (en la página 120).
5. En la sección **Configuración de actualización automática** configure las actualizaciones automáticas del certificado:
   - En el campo **Actualizar cuando el certificado caduque en (días)** especifique cuántos días deben restar hasta el vencimiento del plazo de validez, para actualizar el certificado.
   - Para habilitar las actualizaciones automáticas de los certificados seleccione la casilla **Renovar certificado automáticamente si es posible**.

     Un certificado de tipo general solo puede renovarse manualmente.
6. En la sección **Configuración de cifrado** habilite y configure el cifrado de los certificados generados.

   El cifrado solo está disponible para los certificados de tipo general.

   a. Seleccione la casilla **Habilitar cifrado de certificados**.

   b. Use el control deslizante para definir el número máximo de símbolos en la contraseña para cifrado.
7. Haga clic en **Aceptar**.

INTEGRACIÓN CON LA INFRAESTRUCTURA DE CLAVES PÚBLICAS

Para simplificar la generación de certificados de dominio para los usuarios se requiere la integración de la aplicación con la Infraestructura de claves públicas (PKI). A continuación de la integración, los certificados se emiten automáticamente.

Necesita configurar la cuenta para la integración con PKI. La cuenta debe reunir los siguientes requisitos:

- Ser un usuario de dominio y administrador del equipo que aloja al Servidor de administración.
- Tener el privilegio SeServiceLogonRight en el equipo que aloja al Servidor de administración.

Para crear un perfil de usuario permanente ingrese al menos una vez bajo la cuenta configurada en el equipo que aloja al Servidor de administración. En el repositorio de certificados de este usuario, en el equipo que aloja al Servidor de administración, instale el certificado de Agente de Inscripción provisto por los administradores del dominio.

Para configurar la integración con la infraestructura de claves públicas:

1. En el árbol de consola, abra la carpeta **Administración de dispositivos móviles** y seleccione la subcarpeta **Certificados**.
2. En el espacio de trabajo haga clic en el enlace **Integración con la infraestructura de claves públicas** para abrir la sección **Integración con PKI** de la ventana **Reglas de generación de certificados**.

   Esto abre la sección **Integración con PKI** de la ventana **Reglas de generación de certificados**.
3. Seleccione la casilla **Integrar el sumario de certificados con PKI**.
4. En el campo **Cuenta** especifique el nombre de la cuenta de usuario que se usará para la integración con la infraestructura de claves públicas.
5. En el campo **Contraseña** introduzca la contraseña de dominio para la cuenta.
6. En la lista **Especifique el nombre de la plantilla de certificado en el sistema PKI**, seleccione la plantilla según la cual se generarán los certificados para los usuarios de dominio.

   En Kaspersky Security Center se inicia un servicio dedicado bajo la cuenta especificada. Este servicio es responsable de emitir los certificados de dominio de los usuarios. El servicio comienza cuando se carga la lista de plantillas de certificados haciendo clic en el botón **Lista de actualizaciones** o cuando se genera un certificado.
7. Haga clic en **Aceptar** para guardar los ajustes.

A continuación de la integración, los certificados se emiten automáticamente.

HABILITAR EL SOPORTE DE KERBEROS CONSTRAINT DELEGATION

La aplicación admite el uso de Kerberos Constrained Delegation.

Para habilitar el soporte de Kerberos Constraint Delegation:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Administración de dispositivos móviles**, seleccione un Servidor de dispositivos móviles con MDM de iOS.
3. Seleccione **Propiedades** en el menú contextual del servidor de dispositivos móviles con MDM de iOS.

   Se abre la ventana de propiedades del servidor de dispositivos móviles.
4. En la ventana de propiedades del **Servidor de dispositivos móviles de MDM de iOS**, seleccione la sección **Configuración**.
5. En la sección **Configuración** seleccione la casilla **Asegurar compatibilidad con Kerberos Constraint Delegation**.
6. Haga clic en **Aceptar**.

ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES EXCHANGE ACTIVESYNC

Esta sección describe las características avanzadas para el manejo de dispositivos EAS a través de Kaspersky Security Center.

Además de la administración de dispositivos EAS por medio de comandos, el administrador puede usar las siguientes opciones:

- Crear perfiles de administración para dispositivos EAS, asignarlos a casillas de correo del usuario (consulte la página 122). *Perfil de administración de dispositivo EAS* es una directiva de Exchange ActiveSync que se usa en un servidor Microsoft Exchange para administrar dispositivos EAS. En un perfil de administración de dispositivo EAS, puede configurar los siguientes grupos de ajustes:
  - Ajustes de administración de la contraseña de usuario
  - Ajustes de sincronización de correo
  - Restricciones sobre el uso de las características del dispositivo
  - Restricciones sobre el uso de aplicaciones móviles en el dispositivo.

  Según el modelo del dispositivo, los ajustes de un perfil de administración pueden aplicarse parcialmente. El estado de una directiva de Exchange ActiveSync que se ha aplicado puede verse en las propiedades del dispositivo.
- Ver información acerca de la configuración de administración de dispositivos EAS (consulte la página 123). Por ejemplo, el administrador puede consultar las propiedades de un dispositivo móvil para saber la hora de la última sincronización con un servidor Microsoft Exchange, la ID del dispositivo EAS, el nombre de la directiva de Exchange ActiveSync y su estado actual en el dispositivo.
- Desconectar dispositivos EAS de la administración si están fuera de uso (consulte la página 123).
- Definir los ajustes del sondeo de Active Directory por el Servidor de dispositivos móviles Exchange ActiveSync, lo que permite actualizar la información acerca de las casillas de correo y dispositivos móviles de los usuarios.

Para obtener más información sobre cómo conectar dispositivos móviles Exchange ActiveSync a un servidor de dispositivos móviles de Exchange ActiveSync, consulte la *Guía de implementación de Kaspersky Security Center*.

AGREGAR UN PERFIL DE ADMINISTRACIÓN

Para administrar dispositivos EAS, puede crear perfiles de administración de dispositivos EAS y asignarlos a casillas de correo de Microsoft Exchange seleccionadas.

Solo se puede asignar un perfil de administración de dispositivos EAS a una casilla de correo de Microsoft Exchange.

Para agregar un perfil de administración de dispositivo EAS para una casilla de correo de Microsoft Exchange:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Administración de dispositivos móviles**, seleccione un Servidor de dispositivos móviles con MDM de iOS.
3. Seleccione **Propiedades** en el menú contextual del Servidor de dispositivos móviles Exchange ActiveSync.

   Se abre la ventana de propiedades del servidor de dispositivos móviles.
4. En la ventana de propiedades del **Servidor de dispositivos móviles Exchange ActiveSync**, seleccione la sección **Casillas de correo**.
5. Seleccione una casilla de correo y haga clic en el botón **Asignar perfil**.

   Se abre la ventana **Perfiles de directivas**.
6. En la ventana **Perfiles de directivas** haga clic en el botón **Agregar**.

   Se abre la ventana **Perfil nuevo**.
7. Configure el perfil en las pestañas de la ventana **Perfil nuevo**.
   - Si desea especificar el nombre del perfil y el intervalo de actualización, vaya a la pestaña **General**.
   - Si desea configurar la contraseña del usuario del dispositivo móvil, vaya a la pestaña **Contraseña**.
   - Si desea configurar la sincronización con el servidor de Microsoft Exchange, vaya a la pestaña **Configuración de sincronización**.
   - Si desea configurar restricciones para las características del dispositivo, vaya a la pestaña **Dispositivo**.
   - Si desea configurar restricciones del uso de aplicaciones móviles en el dispositivo, vaya a la pestaña **Aplicación en dispositivo**.

8. Haga clic en **Aceptar**.

   El perfil nuevo se mostrará en la lista de perfiles en la ventana **Perfiles de directivas**.

   Si desea que este perfil se asigne automáticamente a nuevas casillas de correo, así como a aquellas cuyos perfiles se han borrado, selecciónelo en la lista de perfiles y haga clic en el botón **Establecer como perfil predeterminado**.

   El perfil predeterminado no se puede eliminar. Para eliminar el perfil predeterminado actual, debe asignar el atributo “perfil predeterminado” a un perfil diferente.

9. Haga clic en **Aceptar** en la ventana **Perfiles de directivas**.

   La configuración del perfil de administración se aplicará al dispositivo EAS en la próxima sincronización del dispositivo con el Servidor de Dispositivos Móviles Exchange ActiveSync.

ELIMINACIÓN DE UN PERFIL DE ADMINISTRACIÓN

- *Para eliminar un perfil de administración de dispositivo EAS para una casilla de correo de Microsoft Exchange:*

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Administración de dispositivos móviles**, seleccione un Servidor de dispositivos móviles con MDM de iOS.
3. Seleccione **Propiedades** en el menú contextual del Servidor de dispositivos móviles Exchange ActiveSync.

   Se abre la ventana de propiedades del servidor de dispositivos móviles.
4. En la ventana de propiedades del **Servidor de dispositivos móviles Exchange ActiveSync**, seleccione la sección **Casillas de correo**.
5. Seleccione una casilla de correo y haga clic en el botón **Cambiar perfiles**.

   Se abre la ventana **Perfiles de directivas**.
6. En la ventana **Perfiles de directivas** seleccione el perfil que desea eliminar y haga clic en el botón de eliminación marcado con una cruz roja.

   El perfil seleccionado se eliminará de la lista de perfiles administrados. El perfil predeterminado actual se aplicará a los dispositivos EAS administrados por el perfil que se ha borrado.

   Si desea eliminar el perfil predeterminado actual, asigne la propiedad 'perfil predeterminado' a otro perfil, luego borre el primero.

VER LA INFORMACIÓN DE UN DISPOSITIVO EAS

- *Para ver la información acerca de un dispositivo EAS:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos EAS haciendo clic en el enlace **Exchange ActiveSync (EAS)**.
3. En el menú contextual del dispositivo móvil, seleccione **Propiedades**.

   Como resultado, se abre la ventana de propiedades del dispositivo EAS.

La ventana de propiedades del dispositivo móvil muestra información acerca del dispositivo EAS conectado.

DESCONECTAR DE LA ADMINISTRACIÓN UN DISPOSITIVO EAS

- *Para desconectar un dispositivo EAS de la administración del Servidor de dispositivos móviles Exchange ActiveSync:*

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos EAS haciendo clic en el enlace **Exchange ActiveSync (EAS)**.

3. Seleccione el dispositivo móvil que necesita desconectar de la administración del Servidor de dispositivos móviles Exchange ActiveSync.
4. En el menú contextual del dispositivo móvil, seleccione **Eliminar**.

Como resultado, el dispositivo EAS está marcado para eliminar con un icono de una cruz roja. El dispositivo se eliminará de la lista de dispositivos administrados después de que se elimine de la base de datos del Servidor de dispositivos móviles Exchange ActiveSync. Para hacerlo, el administrador debe eliminar la cuenta del usuario en el servidor Microsoft Exchange.

ADMINISTRACIÓN DE DISPOSITIVOS MÓVILES CON MDM DE IOS

Esta sección describe las características avanzadas para el manejo de dispositivos con MDM de iOS a través de Kaspersky Security Center. La aplicación admite las siguientes opciones para la administración de dispositivos móviles con MDM de iOS:

- Defina los ajustes de los dispositivos con MDM de iOS administrados en modo centralizado y restrinja sus características por medio de los perfiles de configuración. Puede agregar o modificar los perfiles de configuración e instalarlos en dispositivos móviles.
- Instale aplicaciones en dispositivos móviles evitando App Store por medio de perfiles de aprovisionamiento. Por ejemplo, puede usar perfiles de aprovisionamiento para instalar aplicaciones corporativas internas en los dispositivos del usuario. Un perfil de aprovisionamiento contiene información acerca de una aplicación y un dispositivo.
- Instale aplicaciones en un dispositivo móvil con MDM de iOS a través de App Store. Antes de instalar una aplicación en un dispositivo móvil con MDM de iOS, debe agregar la aplicación al servidor de dispositivos móviles con MDM de iOS.

Cada 24 horas se envía una notificación PUSH a todos los dispositivos móviles con MDM de iOS conectados a fin de sincronizar los datos con el Servidor de dispositivos móviles con MDM de iOS.

Para obtener más información sobre cómo instalar un Servidor de dispositivos móviles con MDM de iOS, consulte la Guía de implementación de Kaspersky Security Center.

Puede usar la ventana de propiedades del dispositivo para ver la información acerca del perfil de configuración y el perfil de aprovisionamiento, como así también las aplicaciones instaladas en el dispositivo MDM de iOS (consulte la sección "Visualización de la información acerca de un dispositivo iOS MDM" en la página 130).

AGREGAR UN PERFIL DE CONFIGURACIÓN

Para crear un perfil de configuración, debe instalar iPhone Configuration Utility en el equipo en el que instalará la Consola de administración. Debe descargar iPhone Configuration Utility del sitio web de Apple Inc. e instalarla con las herramientas estándar de su sistema operativo.

Para crear un perfil de configuración y agregarlo a un servidor de dispositivos móviles con MDM de iOS:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Administración de dispositivos móviles**, seleccione un Servidor de dispositivos móviles con MDM de iOS.
3. Seleccione **Propiedades** en el menú contextual del servidor de dispositivos móviles con MDM de iOS.

   Se abre la ventana de propiedades del servidor de dispositivos móviles.
4. En la ventana de propiedades del **Servidor de dispositivos móviles de MDM de iOS**, seleccione la sección **Perfiles de configuración**.
5. En la sección **Perfiles de configuración** haga clic en el botón **Crear**.

   Se abre la ventana **Agregar nuevo perfil de configuración**.
6. En la ventana **Agregar nuevo perfil de configuración** especifique el nombre e ID para el perfil.

   El ID del perfil de configuración debe ser único, se debe especificar el valor en el formato DNS inverso, por ejemplo, *com.companyname.identifier*.

7. Haga clic en **Aceptar**.

   Se iniciará una aplicación denominada iPhone Configuration Utility.

8. Vuelva a configurar el perfil en iPhone Configuration Utility.

   Para conocer una descripción de la configuración de perfiles e instrucciones sobre cómo configurar el perfil, consulte la documentación adjunta con iPhone Configuration Utility.

Después de haber configurado el perfil con iPhone Configuration Utility, el nuevo perfil de configuración se muestra en la sección **Perfiles de configuración** de la ventana de propiedades del Servidor de dispositivos móviles con MDM de iOS.

Puede hacer clic en el botón **Modificar** para modificar el perfil de configuración.

Puede hacer clic en el botón **Importar** para cargar el perfil de configuración a un programa.

Puede hacer clic en el botón **Exportar** para guardar perfil de configuración en un archivo.

El perfil que haya creado se debe instalar en los dispositivos iOS MDM (consulte la sección "Instalación de un perfil de configuración en un dispositivo" en la página 125).

INSTALACIÓN DE UN PERFIL DE CONFIGURACIÓN EN UN DISPOSITIVO

Para instalar un perfil de configuración en un dispositivo móvil:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el campo de trabajo, filtre los dispositivos con MDM de iOS haciendo clic en el enlace**MDM de iOS**.

3. Seleccione el dispositivo móvil del usuario en el que necesita instalar un perfil de configuración.

   Puede seleccionar múltiples dispositivos móviles para instalar el perfil simultáneamente.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.

5. En la ventana **Comandos para la administración de dispositivos móviles**, vaya a la sección **Instalar perfil** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo seleccionando **Todos los comandos** del menú contextual del dispositivo y después **Instalar perfil**.

   Como resultado, se abre la ventana **Seleccionar perfiles** que muestra una lista de los perfiles. Seleccione de la lista el perfil que necesita instalar en el dispositivo móvil. Puede seleccionar múltiples perfiles para instalarlos simultáneamente en el dispositivo. Para seleccionar el rango de perfiles, use la tecla **SHIFT**. Para combinar perfiles en un grupo, use la tecla **CTRL**.

6. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, el perfil de configuración seleccionado se instalará en el dispositivo móvil del usuario. Si el comando se ejecuta exitosamente, el estado actual de este, en el registro de comandos, se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo, con los estados de ejecución respectivos. Puede hacer clic en el botón **Actualizar** para actualizar la lista de comandos.

7. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para administración de dispositivos móviles**.

De ser necesario, el perfil que haya instalado se puede visualizar y eliminar, (consulte la sección "Eliminación de un perfil de configuración de un dispositivo" en la página 126).

ELIMINACIÓN DE UN PERFIL DE CONFIGURACIÓN DE UN DISPOSITIVO

Para eliminar un perfil de configuración de un dispositivo móvil:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.

2. En el campo de trabajo, filtre los dispositivos con MDM de iOS haciendo clic en el enlace**MDM de iOS**.
3. Seleccione el dispositivo móvil del usuario del que necesita eliminar el perfil de configuración.

   Puede seleccionar múltiples dispositivos móviles para eliminar el perfil simultáneamente.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.
5. En la ventana **Comandos para la administración de dispositivos móviles** vaya a la sección **Eliminar perfil** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo, y después seleccione **Eliminar perfil**.

   Como resultado, se abre la ventana **Eliminar perfil** que muestra la lista de los perfiles.

6. Seleccione de la lista el perfil que necesita eliminar del dispositivo móvil. Puede seleccionar múltiples perfiles para eliminarlos simultáneamente del dispositivo. Para seleccionar el rango de perfiles, use la tecla **SHIFT**. Para combinar perfiles en un grupo, use la tecla **CTRL**.
7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, el perfil de configuración seleccionado se eliminará del dispositivo móvil del usuario. Si el comando se ejecuta exitosamente, el estado actual de este se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo, con los estados de ejecución respectivos. Puede hacer clic en el botón **Actualizar** para actualizar la lista de comandos.

8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para administración de dispositivos móviles**.

ADICIÓN DE UN PERFIL DE APROVISIONAMIENTO

Para agregar un perfil de aprovisionamiento a un servidor de dispositivos móviles con MDM de iOS:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. En el espacio de trabajo de la carpeta **Administración de dispositivos móviles**, seleccione un Servidor de dispositivos móviles con MDM de iOS.
3. Seleccione **Propiedades** en el menú contextual del servidor de dispositivos móviles con MDM de iOS.

   Se abre la ventana de propiedades del servidor de dispositivos móviles.

4. En la ventana de propiedades del **Servidor de dispositivos móviles de MDM de iOS**, vaya a la sección **Perfiles de aprovisionamiento**.
5. En la sección **Perfiles de aprovisionamiento**, haga clic en el botón **Importar** y especifique la ruta a un perfil de aprovisionamiento.

El perfil se agregará a la configuración del servidor de dispositivos móviles con MDM de iOS.

Puede hacer clic en el botón **Exportar** para guardar perfil de aprovisionamiento en un archivo.

El perfil de aprovisionamiento que haya importado se debe instalar en los dispositivos iOS MDM (consulte la sección "Instalación de un perfil de configuración en un dispositivo" en la página 127).

INSTALACIÓN DE UN PERFIL DE APROVISIONAMIENTO EN UN DISPOSITIVO

Para instalar un perfil de aprovisionamiento en un dispositivo móvil:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos con MDM de iOS haciendo clic en el enlace**MDM de iOS**.
3. Seleccione el dispositivo móvil del usuario en el que necesita instalar el perfil de aprovisionamiento.

   Puede seleccionar múltiples dispositivos móviles para instalar el perfil de aprovisionamiento simultáneamente.
4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.
5. En la ventana **Comandos para la administración de dispositivos móviles** vaya a la sección **Instalar perfil de aprovisionamiento** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo, y después seleccione **Instalar perfil de aprovisionamiento**.

   Como resultado se abre la ventana **Seleccionar perfiles de aprovisionamiento** que muestra una lista de los perfiles de aprovisionamiento. Seleccione de la lista el perfil de aprovisionamiento que necesita instalar en el dispositivo móvil. Puede seleccionar múltiples perfiles de aprovisionamiento para instalarlos simultáneamente en el dispositivo. Para seleccionar el rango de perfiles de aprovisionamiento, use la tecla **SHIFT**. Para combinar perfiles de aprovisionamiento en un grupo, use la tecla **CTRL**.
6. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, el perfil de aprovisionamiento seleccionado se instalará en el dispositivo móvil del usuario. Si el comando se ejecuta exitosamente, el estado actual de este, en el registro de comandos, se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo, con los estados de ejecución respectivos. Puede hacer clic en el botón **Actualizar** para actualizar la lista de comandos.
7. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para administración de dispositivos móviles**.

De ser necesario, el perfil que haya instalado se puede visualizar y eliminar, (consulte la sección "Eliminación de un perfil de aprovisionamiento de un dispositivo" en la página 127).

ELIMINACIÓN DE UN PERFIL DE APROVISIONAMIENTO DE UN DISPOSITIVO

Para eliminar un aprovisionamiento de un dispositivo móvil:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos con MDM de iOS haciendo clic en el enlace**MDM de iOS**.
3. Seleccione el dispositivo móvil del usuario del que necesita eliminar el perfil de aprovisionamiento.

   Puede seleccionar múltiples dispositivos móviles para eliminar el perfil de aprovisionamiento simultáneamente.
4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.
5. En la ventana **Comandos para la administración de dispositivos móviles** vaya a la sección **Eliminar perfil de aprovisionamiento** y haga clic en el botón **Enviar comando**.

   También puede enviar el comando al dispositivo móvil seleccionando **Todos los comandos** del menú contextual, después seleccione **Eliminar perfil de aprovisionamiento**.

   Como resultado, se abre la ventana **Eliminar perfil de aprovisionamiento** que muestra la lista de los perfiles.

6. Seleccione de la lista el perfil de aprovisionamiento que necesita eliminar del dispositivo móvil. Puede seleccionar múltiples perfiles de aprovisionamiento para eliminarlos simultáneamente del dispositivo. Para seleccionar el rango de perfiles de aprovisionamiento, use la tecla **SHIFT**. Para combinar perfiles de aprovisionamiento en un grupo, use la tecla **CTRL**.
7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecuta, el perfil de aprovisionamiento seleccionado se eliminará del dispositivo móvil del usuario. Las aplicaciones relacionadas con el perfil de aprovisionamiento eliminado no funcionarán. Si el comando se ejecuta exitosamente, el estado actual de este se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo, con los estados de ejecución respectivos. Puede hacer clic en el botón **Actualizar** para actualizar la lista de comandos.
8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para administración de dispositivos móviles**.

AGREGAR UN APLICACIÓN ADMINISTRADA

Antes de instalar una aplicación en un dispositivo móvil con MDM de iOS, debe agregar la aplicación al servidor de dispositivos móviles con MDM de iOS. Una aplicación se considera administrada si ha sido instalada en un dispositivo a través de Kaspersky Security Center. Una aplicación administrada puede manejarse remotamente por medio de Kaspersky Security Center.

Para agregar una aplicación administrada a un servidor de dispositivos móviles con MDM de iOS:

1. En el árbol de consola, seleccione la carpeta **Administración de dispositivos móviles**.
2. Seleccione un Servidor de dispositivos móviles con MDM de iOS.
3. Seleccione **Propiedades** en el menú contextual del servidor de dispositivos móviles con MDM de iOS.

   Se abre la ventana de propiedades del servidor de dispositivos móviles con MDM de iOS.
4. En la ventana de propiedades del servidor de dispositivos móviles con MDM de iOS, seleccione la sección **Aplicaciones administradas**.
5. Haga clic en el botón **Agregar** en la sección **Aplicaciones administradas**.

   Se abre la ventana **Agregar una aplicación**.
6. En la ventana **Agregar una aplicación**, en el campo **Nombre de la aplicación**, especifique el nombre de la aplicación que desea agregar.
7. En el campo **ID. de Apple o vínculo a la aplicación** especifique la ID de Apple de la aplicación que se agregará o un enlace al archivo de manifiesto que se pueda utilizar para descargarla.
8. Si desea eliminar una aplicación administrada del dispositivo móvil del usuario junto al perfil de MDM de iOS cuando elimine este, seleccione la casilla **Eliminar junto con el perfil MDM de iOS**.
9. Si desea bloquear la copia de seguridad de datos de la aplicación a través de iTunes, seleccione la casilla **Bloquear copia de seguridad de datos**.
10. Haga clic en **Aceptar**.

La aplicación agregada se muestra en la sección **Aplicaciones administradas** de la ventana de propiedades del servidor de dispositivos móviles con MDM de iOS.

INSTALAR UNA APLICACIÓN EN UN DISPOSITIVO

Para instalar una aplicación en un dispositivo móvil:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos con MDM de iOS haciendo clic en el enlace**MDM de iOS**.
3. Seleccione el dispositivo en el que desea instalar una aplicación.

   Puede seleccionar múltiples dispositivos móviles para instalar la aplicación simultáneamente.

4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.
5. En la ventana **Comandos para la administración de dispositivos móviles** vaya a la sección **Instalar aplicación** y haga clic en el botón **Enviar comando**.

   También puede enviar los comandos al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo y después **Instalar aplicación**.

   Como resultado, se abre la ventana **Seleccionar aplicaciones** que muestra una lista de los perfiles. Seleccione de la lista la aplicación que necesita instalar en el dispositivo móvil. Puede seleccionar múltiples aplicaciones para instalarlas simultáneamente. Para seleccionar un rango de aplicaciones, use la tecla **SHIFT**. Para combinar aplicaciones en un grupo, use la tecla **CTRL**.
6. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, la aplicación seleccionada se instalará en el dispositivo móvil del usuario. Si el comando se ejecuta exitosamente, el estado actual de este, en el registro de comandos, se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo, con los estados de ejecución respectivos. Puede hacer clic en el botón **Actualizar** para actualizar la lista de comandos.
7. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para administración de dispositivos móviles**.

El perfil que haya instalado se puede ver (consulte la sección "Visualización de la información acerca de un dispositivo iOS MDM " en la página 130) y eliminar, de ser necesario (consulte la sección "Eliminación de un perfil de aprovisionamiento de un dispositivo" en la página 129).

ELIMINAR UNA APLICACIÓN DE UN DISPOSITIVO

Para eliminar una aplicación de un dispositivo móvil:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos con MDM de iOS haciendo clic en el enlace**MDM de iOS**.
3. Seleccione el dispositivo móvil del usuario del que necesita eliminar la aplicación.

   Puede seleccionar múltiples dispositivos móviles para eliminar la aplicación simultáneamente.
4. En el menú contextual del dispositivo móvil, seleccione **Mostrar registro de comandos**.
5. En la ventana **Comandos para la administración de dispositivos móviles** vaya a la sección **Eliminar aplicación** y haga clic en el botón **Enviar comando**.

   También puede enviar los comandos al dispositivo móvil seleccionando **Todos los comandos** del menú contextual del dispositivo, después seleccionando **Eliminar aplicación**.

   Como resultado, se abre la ventana **Eliminar aplicaciones** que muestra una lista de las aplicaciones.
6. Seleccione de la lista la aplicación que necesita eliminar del dispositivo móvil. Puede seleccionar múltiples aplicaciones para eliminarlas simultáneamente. Para seleccionar un rango de aplicaciones, use la tecla **SHIFT**. Para combinar aplicaciones en un grupo, use la tecla **CTRL**.
7. Haga clic en el botón **Aceptar** para enviar el comando al dispositivo móvil.

   Cuando el comando se ejecute, la aplicación seleccionada se eliminará del dispositivo móvil del usuario. Si el comando se ejecuta exitosamente, el estado actual de este se mostrará como *Completado*.

   Puede hacer clic en el botón **Reenviar** para enviar nuevamente el comando al dispositivo móvil del usuario.

   Puede hacer clic en el botón **Eliminar de la cola** para cancelar la ejecución de un comando enviado si este aún no se ha ejecutado.

   La sección **Registro de comandos** muestra los comandos que se han enviado al dispositivo, con los estados de ejecución respectivos. Puede hacer clic en el botón **Actualizar** para actualizar la lista de comandos.
8. Haga clic en el botón **Aceptar** para cerrar la ventana **Comandos para administración de dispositivos móviles**.

VER LA INFORMACIÓN ACERCA DE UN DISPOSITIVO CON MDM DE IOS

Para ver información acerca de un dispositivo con MDM de iOS:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos con MDM de iOS haciendo clic en el enlace**MDM de iOS**.
3. Seleccione el dispositivo móvil sobre el que necesita ver la información.
4. En el menú contextual del dispositivo móvil, seleccione **Propiedades**.

   Como resultado, se abre la ventana de propiedades del dispositivo con MDM de iOS.

La ventana de propiedades del dispositivo móvil muestra información acerca del dispositivo con MDM de iOS conectado.

DESCONECTAR DE LA ADMINISTRACIÓN UN DISPOSITIVO CON MDM DE IOS

Para desconectar un dispositivo con MDM de iOS del Servidor de dispositivos móviles con MDM de iOS:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos con MDM de iOS haciendo clic en el enlace**MDM de iOS**.
3. Seleccione el dispositivo móvil que necesita desconectar.
4. En el menú contextual del dispositivo móvil, seleccione **Eliminar**.

Como resultado el dispositivo con MDM de iOS se marcará en la lista para ser eliminado. El dispositivo se eliminará automáticamente de la lista de dispositivos administrados después de que el antiguo sea eliminado de la base de datos del Servidor de dispositivos móviles con MDM de iOS. La eliminación de un dispositivo de la base de datos del Servidor de dispositivos móviles con MDM de iOS toma hasta un minuto.

Después de que el dispositivo con iOS MDM está desconectado de la administración, todos los perfiles de configuración instalados, el perfil iOS MDM, y las aplicaciones para las que se ha instalado la casilla **Eliminar junto con el perfil iOS MDM**, se eliminarán del dispositivo (consulte la sección "**Agregar una aplicación administrada**" en la página 128).

ADMINISTRACIÓN DE DISPOSITIVOS KES

Kaspersky Security Center admite las siguientes funciones para administración de dispositivos móviles KES:

- Administrar los dispositivos móviles KES en modo centralizado mediante comandos (consulte la sección "Comandos para la administración de dispositivos móviles" en la página 116)
- Ver la información acerca de la configuración para la administración de dispositivos KES (consulte la sección "Visualización de la información acerca de un dispositivo KES" en la página 131)
- Instalar aplicaciones mediante paquetes de aplicaciones móviles (consulte la sección "Creación de un paquete de aplicación móvil para los dispositivos KES" en la página 130)
- Desconectar los dispositivos KES de la administración (consulte la sección "Desconexión de un dispositivo KES de la administración" en la página 131).

Para obtener información detallada acerca de cómo manejar dispositivos KES y conectarlos al Servidor de administración consulte la *Guía de Implementación de Kaspersky Security Center 10*.

CREAR UN PAQUETE DE APLICACIÓN MÓVIL PARA DISPOSITIVOS KES

Para crear un paquete de aplicación móvil para dispositivos KES se requiere una licencia de Kaspersky Endpoint Security 10 para Dispositivos móviles.

Para crear un paquete de aplicaciones móviles:

1. En la carpeta **Instalación remota** del árbol de consola, seleccione la subcarpeta **Paquetes de instalación**.
2. En el espacio de trabajo de la carpeta **Paquetes de instalación**, haga clic en el enlace **Administrar paquetes de aplicaciones móviles** para abrir la ventana **Administración de paquetes de aplicaciones móviles**.
3. En la ventana **Administración de paquetes de aplicaciones móviles**, haga clic en el botón **Nuevo**.
4. Se inicia el Asistente para la creación de paquetes de aplicaciones móviles. Siga las instrucciones del asistente.
5. Si desea colocar una aplicación en un contenedor, en la ventana **Configuración** del Asistente, seleccione la casilla de verificación **Crear contenedor con aplicación seleccionada**.

El paquete de aplicaciones móviles recientemente creado se muestra en la ventana **Administración de paquetes de aplicaciones móviles**.

Los contenedores se usan para controlar las actividades de las aplicaciones que se ejecutan en el dispositivo móvil del usuario. Se pueden aplicar reglas de directiva de seguridad a las aplicaciones empaquetadas en un contenedor. Puede configurar reglas para las aplicaciones en la ventana de propiedades de la directiva de Kaspersky Endpoint Security 10 para Dispositivos móviles, en la sección **Contenedores**. Para conocer más detalles sobre contenedores y cómo administrarlos, consulte la documentación adjunta con Kaspersky Endpoint Security 10 para Dispositivos móviles.

Puede colocar una aplicación de terceros en un contenedor. No puede colocar el paquete de instalación de Kaspersky Endpoint Security 10 para Dispositivos móviles en un contenedor.

VER LA INFORMACIÓN ACERCA DE UN DISPOSITIVO KES

Para ver información acerca de un dispositivo KES:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos KES haciendo clic en el enlace **Kaspersky Endpoint Security (KES)**.
3. Seleccione el dispositivo móvil sobre el que necesita ver la información.
4. En el menú contextual del dispositivo móvil, seleccione **Propiedades**.

Se abre la ventana de propiedades del dispositivo KES.

La ventana de propiedades del dispositivo móvil muestra información acerca del dispositivo KES conectado.

DESCONECTAR DE LA ADMINISTRACIÓN UN DISPOSITIVO KES

Para desconectar de la administración un dispositivo KES, el usuario tiene que eliminar del dispositivo el Agente de red. Una vez que el usuario ha eliminado el Agente de red, la información de dispositivo se elimina de la base de datos del Servidor de administración, y el administrador puede eliminarlo de la lista de dispositivos administrados.

Para eliminar un dispositivo KES de la lista de dispositivos administrados:

1. En la carpeta **Administración de dispositivos móviles** del árbol de consola, seleccione la subcarpeta **Dispositivos móviles**.

   El espacio de trabajo de la carpeta muestra una lista de dispositivos móviles administrados.
2. En el campo de trabajo, filtre los dispositivos KES haciendo clic en el enlace **Kaspersky Endpoint Security (KES)**.
3. Seleccione el dispositivo móvil que necesita desconectar de la administración.
4. En el menú contextual del dispositivo móvil, seleccione **Eliminar**.

Como resultado, el dispositivo se elimina de la lista de dispositivos administrados.

Si Kaspersky Endpoint Security para Android no se ha eliminado del dispositivo, este reaparecerá en la lista de dispositivos administrados después de la sincronización con el Servidor de administración.

SELF SERVICE PORTAL

Esta sección contiene información acerca del Self Service Portal. La sección proporciona a los usuarios instrucciones para iniciar sesión en el Self Service Portal, así como instrucciones para crear cuentas en el Self Service Portal y agregar dispositivos móviles en el Self Service Portal.

EN ESTA SECCIÓN:

Acerca del Portal de autoservicio 132

Agregar un dispositivo 133

Crear una cuenta para acceder al Portal de autoservicio 133

ACERCA DEL PORTAL DE AUTOSERVICIO

El Self Service Portal es un portal web que permite al administrador delegar algunas de las funciones de Administración de dispositivos móviles a los usuarios. Un usuario de un dispositivo móvil que ha ingresado en Self Service Portal puede agregar un dispositivo al Self Service Portal. Luego de que el dispositivo es agregado, se instalará en este el Agente de red y se aplicarán las directivas corporativas al dispositivo (consulte la sección "Agregar un dispositivo" en la página 133). Después de esto el dispositivo se convierte en un dispositivo administrado.

El Self Service Portal admite la autorización automática de usuario usando Kerberos Constrained Delegation y autorización de dominio.

Self Service Portal admite dispositivos móviles con los sistemas operativos iOS y Android.

Si es necesario (por ejemplo, cuando el dispositivo del usuario se perdió o ha sido robado), el usuario puede ingresar al Self Service Portal y enviar comandos al dispositivo administrado. Un conjunto propietario de comandos es admitido para cada tipo de dispositivo (ver la tabla a continuación).

Tabla 11. Lista de comandos admitidos

TIPO DE DISPOSITIVO MÓVIL	COMANDOS	RESULTADO DE LA EJECUCIÓN DEL COMANDO
Dispositivo con MDM de iOS	Bloqueo	Dispositivo bloqueado.
	Eliminar datos	Se han eliminado todos los datos del dispositivo, las configuraciones se han revertido a los valores predeterminados, y el dispositivo ya no se administra.
	Eliminar datos corporativos	Se han eliminado los datos corporativos, el perfil MDM de iOS, y el Agente de red y el dispositivo ya no se administra.
Dispositivo KES	Bloqueo	Dispositivo bloqueado.
	Eliminar datos	Se han eliminado todos los datos del dispositivo, las configuraciones se han revertido a los valores predeterminados, y el dispositivo ya no se administra.
	Eliminar datos corporativos	Se han eliminado los datos corporativos, el perfil MDM de iOS, y el Agente de red y el dispositivo ya no se administra.
	Localizar	Dispositivo bloqueado. Dispositivos localizado y mostrado en Google Maps™. El operador de servicios móviles aplica un cargo por enviar el mensaje de texto y por proporcionar la conexión a Internet.
	Alarma	Dispositivo bloqueado. El dispositivo emite una señal sonora.
	Foto policial	Dispositivo bloqueado. Se ha tomado la foto mediante la cámara frontal del dispositivo y se ha guardado en el Servidor de administración. Las fotos pueden visualizarse en el Self Service Portal. El operador de servicios móviles aplica un cargo por enviar el mensaje de texto y por proporcionar la conexión a Internet.

El Self Service Portal usa la lista global de usuarios de Kaspersky Security Center. La lista se expande automáticamente al importar usuarios desde Active Directory (consulte la sección "Visualización y modificación de las propiedades del grupo de Active Directory" en la página 96) o en forma manual (consulte la sección "Agregar una cuenta de usuario" en la página 83).

Si la autorización de dominio en Self Service Portal está prohibida por el administrador, los usuarios pueden usar cuentas con alias para la autorización. La creación de sobrenombres para la autenticación en Self Service Portal está disponible en las propiedades de la cuenta del usuario (consulte la sección "Creación de una cuenta del Self Service Portal" en la página 133).

El administrador puede conceder a los usuarios los siguientes permisos de uso en Self Service Portal:

- Lectura
- Cambio
- Conectar nuevos dispositivos
- Enviar solo comandos de información.

  Foto policial y **Localizar** son comandos de información.
- Enviar comandos a dispositivos móviles

AGREGAR UN DISPOSITIVO

Antes de añadir un dispositivo en el Self Service Portal, el usuario debe aceptar el Contrato de licencia para el usuario final del Self Service Portal e ingresar en este.

El algoritmo para añadir el dispositivo de un usuario al Self Service Portal incluye los siguientes pasos:

1. El usuario abre la página principal del portal.
2. Self Service Portal crea un paquete de instalación y luego muestra un enlace único para la descarga del paquete de instalación y un código QR en el que está cifrado el enlace. La pantalla muestra el intervalo de tiempo durante el cual estará disponible un enlace para descargar el paquete de instalación. Se envía al correo electrónico del usuario un mensaje con un enlace para descargar el paquete de instalación.

   Es necesario el paquete de instalación para instalar el Agente de Red en el dispositivo y aplicar las directivas corporativas.

   > Un nuevo paquete de instalación solo puede crearse después de que el paquete de instalación creado previamente haya sido eliminado del Servidor de administración.
3. Al hacer clic en el enlace **Crear paquete para instalar en un dispositivo nuevo** se dirige al usuario a la página de descarga del paquete de instalación en el dispositivo móvil a añadirse al Self Service Portal.
4. Self Service Portal determina el sistema operativo del dispositivo del usuario.

   Si el sistema operativo del dispositivo pudo determinarse automáticamente, se abre la página de descarga del paquete de instalación. Si el sistema operativo del dispositivo no pudo determinarse automáticamente, se abre una ventana que permite al usuario elegir manualmente un sistema operativo.
5. El usuario descarga el paquete de instalación e instala el Agente de red en el dispositivo móvil.
6. Luego de que se ha instalado el Agente de Red, el dispositivo se conecta al Servidor de Administración.

Como resultado, el dispositivo se agregará a la lista de dispositivos administrados y se le aplicarán las directivas corporativas. Se envía un enlace a la información sobre la conexión al Servidor de Administración al correo electrónico del usuario.

CREAR UNA CUENTA PARA ACCEDER AL PORTAL DE AUTOSERVICIO

Si el uso de la autorización de dominio de usuarios en Self Service Portal está prohibido, puede crear cuentas con alias para los usuarios en la Consola de administración. Los usuarios pueden iniciar sesión en Self Service Portal usando las cuentas con alias.

- *Para proporcionar una cuenta del Self Service Portal (cuenta con alias) a un usuario:*

  1. En el árbol de consola, en la carpeta **Cuentas de usuario**, seleccione una cuenta de usuario.
  2. En el menú contextual de la cuenta de usuario, seleccione **Proporcionar cuenta para acceder al Portal de autoservicio**.
  3. En la ventana de propiedades de la cuenta de usuario, en la sección **Cuentas del Self Service Portal**, haga clic en el botón **Agregar**.

     Puede hacer clic en el botón **Agregar** para crear varias cuentas con alias en Self Service Portal.
  4. En la **Nueva cuenta del Self Service Portal**, especifique los datos de inicio de sesión y el método de notificación al usuario, y luego haga clic en **OK**.

     Automáticamente, se genera una contraseña para la cuenta del Portal de autoservicio. Se enviará una notificación de la creación de la cuenta al correo electrónico o al dispositivo móvil del usuario, con los datos de inicio de sesión y la contraseña.

  Como resultado, se creará la cuenta del Portal de autoservicio. Puede crear una cantidad ilimitada de cuentas del Portal de autoservicio para un único usuario. Después que se haya creado una cuenta en Self Service Portal, no puede modificarse. Sin embargo, puede eliminar una cuenta seleccionada al hacer clic en el botón con una cruz roja a la derecha de la lista de cuentas de Self Service Portal.

- *Para modificar una cuenta del Portal de autoservicio:*

  1. En la ventana de propiedades de la cuenta de un usuario, en la sección **Cuentas del Self Service Portal**, seleccione una cuenta del Self Service Portal y haga clic en el botón **Establecer contraseña nueva**.
  2. En la ventana Generar nueva contraseña para la cuenta del Portal de autoservicio, especifique un método de notificación al usuario y haga clic en el botón **Aceptar**.

  Como resultado, se cambiará la contraseña. Se enviará una notificación del cambio de contraseña al correo electrónico o al dispositivo móvil del usuario.

  Puede hacer clic en el botón **Establecer contraseña nueva** para generar una nueva contraseña de una cuenta de Self Service Portal seleccionada. Se creará automáticamente la contraseña. La nueva contraseña para el Self Service Portal se enviará al correo electrónico o teléfono móvil del usuario.

CARPETA CIFRADO Y PROTECCIÓN DE DATOS

El cifrado reduce el riesgo de fuga de datos accidental en el caso de que le roben o pierda su equipo portátil, medios extraíbles o unidad de disco duro, o tras el acceso de usuarios y aplicaciones no autorizados.

Kaspersky Endpoint Security 10 para Windows proporciona funcionalidad de cifrado. Kaspersky Endpoint Security 10 para Windows le permite cifrar archivos almacenados en unidades locales de un equipo y unidades extraíbles, así como medios de almacenamiento extraíbles y unidades de disco duro en su totalidad.

Las reglas de cifrado se configuran mediante directivas en Kaspersky Security Center. Al aplicar una directiva, se realiza el cifrado y el descifrado de acuerdo con las reglas existentes.

La disponibilidad de la función de administración de cifrado se determina mediante la configuración de la interfaz de usuario (ver la sección “Configuración de la interfaz” en la página 31).

El administrador puede realizar las siguientes acciones:

- Configurar y cifrar y descifrar archivos en unidades locales del equipo
- Configurar y cifrar archivos en medios extraíbles
- Crear reglas de acceso de la aplicación a archivos cifrados
- Crear y entregar al usuario el archivo de clave para acceder a archivos cifrados si se restringe el cifrado de archivos en el equipo del usuario
- Configurar y realizar el cifrado de unidades de disco duro
- Administrar el acceso de usuarios a unidades de disco duro y unidades extraíbles cifradas (administrar cuentas del agente de autenticación, crear y entregar a los usuarios información según pedido para la restauración de nombres de cuenta y contraseñas, además de claves de acceso para dispositivos cifrados)
- Ver estados de cifrado e informes de cifrado de archivos.

Estas operaciones se realizan mediante el uso de herramientas integradas a Kaspersky Endpoint Security 10 para Windows. Para conocer instrucciones detalladas sobre cómo realizar operaciones, además de una descripción de las funciones de cifrado, consulte la *Guía del administrador de Kaspersky Endpoint Security 10 para Windows*.

EN ESTA SECCIÓN:

Ver la lista de dispositivos cifrados 135

Ver la lista de eventos de cifrado 136

Exportar la lista de eventos de cifrado en un archivo de texto 136

Crear y ver informes de cifrado 137

VER LA LISTA DE DISPOSITIVOS CIFRADOS

Para ver la lista de dispositivos cifrados que almacenan información cifrada, realice lo siguiente:

1. Seleccione la carpeta **Cifrado y protección de datos** en el árbol de consola del Servidor de administración.
2. Abra la lista de dispositivos cifrados mediante uno de los siguientes métodos:
   - Haciendo clic en el vínculo **Ir a la lista de dispositivos cifrados** en la sección **Administrar dispositivos cifrados**.
   - En el árbol de consola, seleccione la carpeta **Dispositivos cifrados**.

El espacio de trabajo mostrará información acerca de los dispositivos de la red que almacenan archivos cifrados y acerca de los dispositivos cifrados a nivel de unidad. Después de descifrar la información de un dispositivo, este dispositivo se elimina automáticamente de la lista.

Puede ordenar la información en la lista de dispositivos, tanto en orden ascendente como descendente, en cualquier columna.

La presencia o ausencia de la carpeta **Cifrado y protección de datos** en el árbol de consola se determina mediante la configuración de la interfaz de usuario (ver la sección "Configuración de la interfaz" en la página 31).

VER LA LISTA DE EVENTOS DE CIFRADO

Cuando se ejecutan tareas de cifrado y descifrado de datos en equipos cliente, Kaspersky Endpoint Security 10 para Windows envía a Kaspersky Security Center información acerca de los siguientes tipos de eventos:

- No se puede cifrar o descifrar un archivo, ni crear un archivo de almacenamiento cifrado debido a la falta de espacio libre en disco
- No se puede cifrar o descifrar un archivo, ni crear un archivo de almacenamiento cifrado debido a problemas con la licencia
- No se puede cifrar o descifrar un archivo, ni crear un archivo de almacenamiento cifrado debido a que faltan derechos de acceso
- Se prohibió el acceso de la aplicación a un archivo cifrado
- Errores desconocidos.

Para ver una lista de los eventos que tuvieron lugar durante el cifrado de datos en equipos cliente, realice lo siguiente:

1. Seleccione la carpeta **Cifrado y protección de datos** en el árbol de consola del Servidor de administración.
2. Vaya a la lista de eventos que tuvieron lugar durante el cifrado de datos, mediante uno de los siguientes métodos:
   - Haga clic en el enlace **Ir a la lista de errores** en la sección de control **Errores de cifrado de datos**.
   - En el árbol de consola, seleccione la carpeta **Eventos de cifrado**.

El espacio de trabajo mostrará información acerca de los problemas que se produjeron durante el cifrado de datos en equipos cliente.

Puede realizar las siguientes acciones en la lista de eventos de cifrado:

- Ordenar los registros de datos en orden ascendente o descendente, en cualquier columna
- Realizar la búsqueda rápida de registros (por coincidencia de texto con una subcadena en cualquiera de los campos de la lista)
- Exportar la lista de eventos a un archivo de texto.

La presencia o ausencia de la carpeta **Cifrado y protección de datos** en el árbol de consola se determina mediante la configuración de la interfaz de usuario (ver la sección "Configuración de la interfaz" en la página 31).

EXPORTAR LA LISTA DE EVENTOS DE CIFRADO EN UN ARCHIVO DE TEXTO

Para exportar la lista de eventos de cifrado a un archivo de texto:

1. Cree una lista de eventos de cifrado (ver la sección "Visualización de la lista de eventos de cifrado" en la página 136).
2. En el menú contextual de la lista de eventos, seleccione **Exportar lista**.

   Se abre la ventana **Exportar lista**.
3. En la ventana **Exportar lista**, especifique el nombre del archivo de texto con la lista de eventos, seleccione una carpeta para guardarlo y haga clic en el botón **Guardar**.

   La lista de eventos de cifrado se guardará en el archivo especificado.

CREAR Y VER INFORMES DE CIFRADO

El administrador puede generar los siguientes informes:

- Informe de cifrado de dispositivos con información acerca del estado de cifrado de dispositivos para todos los grupos de equipos
- Informe de derechos de acceso a los dispositivos cifrados con información acerca del estado de las cuentas de usuarios que cuentan con permisos de acceso a dispositivos cifrados
- Informe de errores de cifrado con información acerca de los errores que se produjeron durante la ejecución de las tareas de cifrado y descifrado de datos en equipos cliente
- Informe del estado de cifrado del equipo con información que indica si el estado de cifrado del equipo cumple o no con la directiva de cifrado
- Informe del bloqueo de acceso a archivos con información acerca del bloqueo del acceso de aplicaciones a archivos cifrados.

Para ver el informe de cifrado de dispositivos, realice lo siguiente:

1. En el árbol de consola, seleccione la carpeta **Cifrado y protección de datos**.
2. Realice una de las siguientes acciones:
   - Haga clic en el enlace **Ver informe de cifrado de dispositivos** para ejecutar el Asistente para nueva plantilla de informe.
   - Seleccione la subcarpeta **Dispositivos cifrados** y luego haga clic en el enlace **Ver informe de cifrado de dispositivos** para ejecutar el Asistente para nueva plantilla de informe.
3. Siga las instrucciones del Asistente para nueva plantilla de informe.

En la carpeta **Informes y notificaciones** del árbol de consola aparece un nuevo informe. Se inicia el proceso de generación de informe. El informe se muestra en el espacio de trabajo de la consola.

Para ver el informe de derechos de acceso a los dispositivos cifrados, realice lo siguiente:

1. En el árbol de consola, seleccione la carpeta **Cifrado y protección de datos**.
2. Realice una de las siguientes acciones:
   - Haga clic en el enlace **Ver informe sobre los derechos de acceso a los dispositivos cifrados** en la sección **Administrar dispositivos cifrados** para ejecutar el Asistente para nueva plantilla de informe.
   - Seleccione la subcarpeta **Dispositivos cifrados** y luego haga clic en el enlace **Ver informe sobre los derechos de acceso a los dispositivos cifrados** para ejecutar el Asistente para nueva plantilla de informe.
3. Siga las instrucciones del Asistente para nueva plantilla de informe.

En la carpeta **Informes y notificaciones** del árbol de consola aparece un nuevo informe. Se inicia el proceso de generación de informe. El informe se muestra en el espacio de trabajo de la consola.

Para ver el informe sobre errores de cifrado, realice lo siguiente:

1. En el árbol de consola, seleccione la carpeta **Cifrado y protección de datos**.
2. Realice una de las siguientes acciones:
   - Haga clic en el enlace **Ver informe sobre errores de cifrado** en la sección de control **Errores de cifrado de datos** para ejecutar el Asistente para nueva plantilla de informe.
   - Seleccione la subcarpeta **Eventos de cifrado** y luego haga clic en el enlace **Ver informe sobre errores de cifrado** para ejecutar el Asistente para nueva plantilla de informe.
3. Siga las instrucciones del Asistente para nueva plantilla de informe.

En la carpeta **Informes y notificaciones** del árbol de consola aparece un nuevo informe. Se inicia el proceso de generación de informe. El informe se muestra en el espacio de trabajo de la consola.

Para ver el informe sobre el estado de cifrado del equipo, realice lo siguiente:

1. En el árbol de consola, seleccione la carpeta **Informes y notificaciones**.
2. Realice una de las siguientes acciones:
   - Haga clic con el botón derecho del mouse para activar el menú contextual de la carpeta **Informes y notificaciones**, seleccione **Crear** → **Plantilla de informe** y ejecute el Asistente para nueva plantilla de informe.
   - Haga clic en el enlace **Crear una plantilla de informe** para ejecutar el Asistente para nueva plantilla de informe.
3. Siga las instrucciones del Asistente para nueva plantilla de informe. En la ventana **Selección del tipo de plantilla de informe**, en la sección **Otros**, seleccione **Informe de estado del cifrado del equipo**.

   Cuando finaliza el Asistente para nueva plantilla de informe, aparece una nueva plantilla de informe en la carpeta **Informes y notificaciones** del árbol de consola.
4. En la carpeta **Informes y notificaciones**, seleccione la plantilla de informe creada en los pasos anteriores.

Se inicia el proceso de generación de informe. El informe aparece en el espacio de trabajo de la Consola de administración.

Para obtener información sobre si los estados de cifrado de los equipos y medios extraíbles cumplen con la directiva de cifrado, vea los paneles de información en la pestaña **Estadísticas** de la carpeta **Informes y notificaciones** (ver la sección "**Trabajo con la información estadística**" en la página 89).

Para ver el informe sobre el bloqueo de acceso a archivos, realice lo siguiente:

1. En el árbol de consola, seleccione la carpeta **Informes y notificaciones**.
2. Realice una de las siguientes acciones:
   - Haga clic con el botón derecho del mouse para activar el menú contextual de la carpeta **Informes y notificaciones**, seleccione **Crear** → **Plantilla de informe** y ejecute el Asistente para nueva plantilla de informe.
   - Haga clic en el enlace **Crear una plantilla de informe** para ejecutar el Asistente para nueva plantilla de informe.
3. Siga las instrucciones del Asistente para nueva plantilla de informe. En la ventana **Selección del tipo de plantilla de informe**, en la sección **Otros**, seleccione **Informe sobre el bloqueo de acceso a los archivos**.

   Cuando finaliza el Asistente para nueva plantilla de informe, aparece una nueva plantilla de informe en la carpeta **Informes y notificaciones** del árbol de consola.
4. En la carpeta **Informes y notificaciones**, seleccione la plantilla de informe creada en los pasos anteriores.

Se inicia el proceso de generación de informe. El informe aparece en el espacio de trabajo de la Consola de administración.

ADMINISTRACIÓN DEL ACCESO DE LOS DISPOSITIVOS A LA RED DE UNA ORGANIZACIÓN (CONTROL DE ACCESO A LA RED, NAC)

Kaspersky Security Center permite controlar el acceso de los dispositivos a la red de una organización mediante reglas de restricción de acceso y una lista blanca de dispositivos. Los agentes NAC se usan para administrar el acceso de los dispositivos a la red de una organización. Se instala un agente NAC en los equipos cliente junto con el Agente de red

Se utilizan dos agentes NAC en cada uno de los segmentos de difusión de una red: principal y redundante. El agente NAC principal está disponible para el uso regular de las directivas de acceso de la red. Cuando se apaga el equipo que aloja el agente NAC principal, el agente NAC redundante asume sus funciones, lo que garantiza un funcionamiento continuo de NAC en la red de la organización. Los roles de los agentes NAC pueden implementarse y distribuirse manual o automáticamente.

Antes de crear reglas de restricción de acceso a la red para dispositivos y una lista blanca de dispositivos, el administrador debe crear elementos de red. *Elemento de red* es un grupo de dispositivos creados según criterios definidos por el administrador.

El administrador puede especificar los siguientes criterios para agregar dispositivos a un elemento de red:

- Atributos de red (dirección IP, dirección MAC)
- Fabricante de dispositivo
- Membresía de un dominio del dispositivo
- Estado de protección del dispositivo
- Presencia de actualizaciones críticas de la aplicación y de seguridad no instaladas en el dispositivo

Cuando se crea un elemento de red, el administrador puede crear reglas de restricción de acceso para este elemento o agregarlo a una lista blanca.

El administrador puede crear las siguientes reglas de restricción de acceso a la red:

- Una regla que bloquea el acceso a la red para todos los dispositivos incluidos en el elemento de red.
- Una regla que redirige al portal de autorización las solicitudes de acceso a la red generadas por cualquier dispositivo incluido en el elemento de red. *El portal de autorización* es un servicio web que brinda a dispositivos invitados acceso a la red. El administrador crea cuentas y las asigna a los usuarios de dispositivos invitados.
- Una regla que permita a los dispositivos incluidos en el elemento de red acceder únicamente a las direcciones de red especificadas.

El administrador puede seleccionar un elemento de red y agregarlo a la lista blanca. Los dispositivos incluidos en la lista blanca tienen acceso completo a la red de la organización.

EN ESTA SECCIÓN:

Cambio a la configuración de NAC en las propiedades del Agente de red 140

Selección de un modo de operación para el agente NAC 140

Creación de elementos de red 140

Creación de reglas de restricción de acceso a la red 141

Creación de una lista blanca 142

Creación de una lista de direcciones de red permitidas 142

Creación de cuentas para usar en el portal de autorización 142

Configuración de la interfaz de la página de autorización 143

Configuración de NAC en una directiva del Agente de red 143

CAMBIO A LA CONFIGURACIÓN DE NAC EN LAS PROPIEDADES DEL AGENTE DE RED

Para cambiar a la configuración del Control de acceso a la red en las propiedades del Agente de red, realice las siguientes acciones:

1. En el árbol de consola, seleccione la carpeta **Equipos administrados**.
2. En la carpeta **Equipos administrados**, en la pestaña **Equipos**, seleccione el equipo cliente donde se ha instalado el Agente de red.
3. En el menú contextual del equipo cliente, seleccione **Propiedades**.

   Se abre la ventana de las propiedades del equipo cliente.
4. En la ventana de propiedades del equipo cliente, seleccione la sección **Aplicaciones**.
5. En la sección **Aplicaciones**, seleccione Agente de red y haga clic en el botón **Propiedades**.

   Se abre la ventana **Configuración del Agente de red de Kaspersky Security Center**.
6. En la ventana **Configuración del Agente de red de Kaspersky Security Center**, seleccione la sección **Control de acceso a la red (NAC)** y ajuste la configuración de NAC.

SELECCIÓN DE UN MODO DE OPERACIÓN PARA EL AGENTE NAC

Para seleccionar un modo de operación para el agente NAC:

1. En la ventana **Configuración del Agente de red de Kaspersky Security Center** (ver la sección "**Cambio a la configuración NAC de las propiedades del Agente de red**" en la página 140), seleccione la sección **Administración del acceso a la red (NAC)**.
2. En la subsección **Configuración**, en el bloque de configuración **Modo de operación del agente NAC**, seleccione un modo de operación para el agente NAC:
   - **Deshabilitado**. Seleccione esta opción para deshabilitar el agente NAC.
   - **Principal**. Seleccione esta opción para usar el agente NAC como el principal. El agente NAC principal es responsable del uso continuo de las reglas de restricción de acceso en el segmento de red.
   - **En espera**. Seleccione esta opción para usar el agente NAC como el de espera. Si el agente NAC principal está inactivo, se habilita el de espera.
3. En el bloque de configuración **Modo de operación de NAC**, seleccione un modo de operación para NAC:
   - **Deshabilitado**. Seleccione esta opción si no desea aplicar las reglas de restricción de acceso en el segmento de red en el que opera el agente NAC.
   - **Estándar**. Seleccione esta opción si desea que las reglas de restricción de acceso creadas se apliquen inmediatamente en el segmento de red en el que opera el agente NAC.
   - **Emulación**. Seleccione esta opción si desea que las reglas de restricción de acceso creadas se apliquen en modo de prueba. En este caso, las reglas no se aplican, pero se registran los eventos de aplicación de reglas.

CREACIÓN DE ELEMENTOS DE RED

Para crear un elemento de red:

1. En la ventana **Configuración del Agente de red de Kaspersky Security Center** (ver la sección "**Cambio a la configuración NAC en las propiedades del Agente de red**" en la página 140), en la sección **Administración del acceso a la red (NAC)**, seleccione la subsección **Elementos de red**.
2. En la lista desplegable **Agregar** seleccione el tipo de dispositivos que desea agregar al elemento de red (por ejemplo, equipos).

   Se abre la ventana **Creación de elemento de red**.

3. En la ventana **Creación de elemento de red** escriba un nombre para el elemento de red que creará.

   En la lista desplegable **Agregar** seleccione los criterios que deben definir si un dispositivo de red se incluirá en el elemento de red que está creando:

   - **Por atributos de red**. Si selecciona esta opción, puede agregar un equipo o varios equipos al elemento de red por dirección IP, dirección MAC, intervalo IP o máscara de subred.
   - **Por fabricante**. Si selecciona esta opción, puede agregar equipos al elemento de red por fabricante.
   - **Por membresía de dominio**. Si selecciona esta opción, puede agregar equipos al elemento de red según sus membresías de un dominio. La membresía de dominio puede usarse como criterio que permita el acceso a la red de la organización.
   - **Por estado del equipo**. Si selecciona esta opción, puede especificar un estado del equipo: por ejemplo, “Crítico”. Puede crear reglas que restrinjan el acceso a la red a los equipos que tengan ese estado.
   - **Por software**. Si selecciona esta opción, puede agregar equipos al elemento de red según el tipo de sistema operativo, el estado de firewall y la disponibilidad de actualizaciones.

   Los criterios agregados se muestran el campo **Criterios** de modo que los objetos de la red deben cumplirlos.

4. Haga clic en **Aceptar**.

Los elementos de red creados se muestran en la ventana de propiedades de la directiva del Agente de red de Kaspersky Security Center, en la subsección **Elementos de red**.

CREACIÓN DE REGLAS DE RESTRICCIÓN DE ACCESO A LA RED

Para crear una regla de restricción de acceso a la red:

1. En la ventana **Configuración del Agente de red de Kaspersky Security Center** (ver la sección “**Cambio a la configuración NAC en las propiedades del Agente de red**” en la página 140), en la sección **Administración del acceso a la red (NAC)**, seleccione la subsección **Reglas de acceso**.
2. En la sección **Reglas de acceso** seleccione la subsección **Restricciones de acceso** y haga clic en el botón **Agregar**.

   Se abre la ventana **Propiedades de la regla de restricción de acceso**.
3. En la ventana **Propiedades de la regla de restricción de acceso** escriba un nombre para la regla que creará.
4. En la ventana **Propiedades de la regla de restricción de acceso** haga clic en el botón **Agregar** para seleccionar un elemento de red al cual se aplicará la regla. Puede agregar varios elementos de red a la misma regla.

   Se abre la ventana **Incorporación de elementos de red**.
5. En la ventana **Incorporación de elementos de red** seleccione un elemento de red y haga clic en el botón **Aceptar**.

   El elemento de red seleccionado se muestra en la ventana **Propiedades de la regla de restricción de acceso**.
6. En la ventana **Propiedades de la regla de restricción de acceso**, en el bloque de configuración **Restringir acceso a la red**, seleccione una de las siguientes opciones:

   - **Bloquear acceso a la red**. Si selecciona esta opción, todos los dispositivos del elemento de red tienen prohibido el acceso a la red.
   - **Redirigir al portal de autorización**. Si selecciona esta opción, las solicitudes de los dispositivos del elemento de red serán redirigidas al servidor de autorización.
   - **Permitir solo las direcciones especificadas**. Si selecciona esta opción, en el campo **Direcciones disponibles** especifique las direcciones a las que los dispositivos incluidos en el elemento de red pueden tener acceso.
7. Haga clic en **Aceptar**.

La regla creada se muestra en la subsección **Restricciones de acceso**.

CREACIÓN DE UNA LISTA BLANCA

Para crear una lista blanca de dispositivos IP:

1. En la ventana **Configuración del Agente de red de Kaspersky Security Center** (ver la sección "**Cambio a la configuración NAC en las propiedades del Agente de red**" en la página 140), en la sección **Administración del acceso a la red (NAC)**, seleccione la subsección **Reglas de acceso**.
2. En la sección **Reglas de acceso** seleccione la subsección **Lista blanca** y haga clic en el botón **Agregar**.

   Se abre la ventana **Incorporación de elementos de red**.
3. En la ventana **Incorporación de elementos de red** seleccione el elemento de red que desee agregar a la lista blanca.
4. Haga clic en **Aceptar**.

Los elementos de red agregados a la lista blanca se muestran en la subsección **Lista blanca**. Los dispositivos agregados a la lista blanca tienen acceso completo a la red de la organización.

CREACIÓN DE UNA LISTA DE DIRECCIONES DE RED PERMITIDAS

Para crear una lista de direcciones de red habilitadas:

1. En la ventana **Configuración del Agente de red de Kaspersky Security Center** (ver la sección "**Cambio a la configuración NAC en las propiedades del Agente de red**" en la página 140), en la sección **Administración del acceso a la red (NAC)**, seleccione la subsección **Direcciones de los servicios de red**.
2. En la sección **Direcciones de servicios de red**, en la lista desplegable situada a la derecha del botón **Agregar**, seleccione un tipo de dirección de red:
   - **Direcciones de red permitidas**. Seleccione esta opción para agregar direcciones habilitadas para dispositivos invitados.

     Se abre la ventana **Direcciones de red permitidas**, en la cual puede agregar las direcciones de los servicios de red por dirección IP, dirección MAC, intervalo IP y máscara de subred.
   - **Portal de autorización**. Seleccione esta opción para agregar la dirección del portal de autorización al cual se redirigirán las solicitudes de los dispositivos invitados.

     Se abre la ventana **Portal de autorización**, en la cual puede especificar la dirección del servidor al que se redirigirán las solicitudes de los dispositivos de red.

Las direcciones agregadas se muestran en la sección **Direcciones de servicios de red**.

CREACIÓN DE CUENTAS PARA USAR EN EL PORTAL DE AUTORIZACIÓN

Para crear una cuenta y utilizarla en el portal de autorización:

1. En la ventana **Configuración del Agente de red de Kaspersky Security Center** (ver la sección "**Cambio a la configuración NAC en las propiedades del Agente de red**" en la página 140), en la sección **Control de acceso a la red (NAC)**, seleccione la subsección **Página de autorización**.
2. En la sección **Página de autorización** seleccione la subsección **Cuentas**.
3. Haga clic en el botón **Agregar** de la sección **Cuentas**.

   Se abre la ventana **Inclusión de cuenta**.
4. En la ventana **Inclusión de cuenta** ajuste la configuración de la cuenta.
5. Si desea bloquear el acceso a red para esta cuenta, seleccione la casilla **Bloquear cuenta**.
6. Haga clic en **Aceptar**.

Las cuentas creadas se muestran en la subsección **Cuentas**, que pertenece a la sección **Página de autorización**.

CONFIGURACIÓN DE LA INTERFAZ DE LA PÁGINA DE AUTORIZACIÓN

Para configurar la interfaz de la página de autorización:

1. En la ventana **Configuración del Agente de red de Kaspersky Security Center** (ver la sección "**Cambio a la configuración NAC en las propiedades del Agente de red**" en la página 140), en la sección **Administración del acceso a la red (NAC)**, seleccione la subsección **Página de autorización**.
2. En la sección **Página de autorización** seleccione la subsección **Interfaz**.
3. En el bloque de configuración **Logotipo** seleccione un logotipo para usar en la página de autorización:
   - **Predeterminado**. Seleccione esta opción si desea utilizar el logotipo de Kaspersky Lab en la página de autorización.
   - **Personalizar**. Seleccione esta opción si desea usar un logotipo personalizado. Haga clic en el botón **Seleccionar** si desea especificar la ruta a un archivo de logotipo. El nuevo logotipo debe tener la misma configuración que el predeterminado.
4. En el bloque de configuración **Página de autorización**, seleccione la página de autorización a la que se redirigirán las solicitudes de acceso a la red.
   - **Predeterminado**. Seleccione esta opción si desea utilizar la página predeterminada en el portal de autorización. Para editar la página predeterminada, haga clic en el botón **Guardar en archivo** y guarde la página de autorización como un archivo para editarlo más tarde.
   - **Personalizar**. Seleccione esta opción si desea utilizar una versión editada de la página Kaspersky Lab o su propia versión. Haga clic en el botón **Seleccionar** y especifique la ruta a un archivo de página de autorización.
5. Haga clic en **Aceptar**.

CONFIGURACIÓN DE NAC EN UNA DIRECTIVA DEL AGENTE DE RED

Para configurar NAC en una directiva del Agente de red:

1. En la carpeta **Equipos administrados** del árbol de consola, diríjase a la pestaña **Directivas**.
2. Inicie la configuración de NAC mediante uno de los siguientes métodos:
   - Haga clic en el enlace **Cambiar configuración de directiva** del menú **Acciones** para abrir la ventana de propiedades del Agente de red de Kaspersky Security Center y seleccione la sección **Control de acceso a la red (NAC)**.
   - Use los enlaces del grupo de configuraciones de **Control de acceso a la red (NAC)** en el menú **Acciones**.

INVENTARIO DE LOS EQUIPOS DETECTADOS EN LA RED

Kaspersky Security Center recupera información acerca de los equipos detectados durante el sondeo de red. El inventario abarca todos los equipos conectados a la red de la organización. La información sobre el equipo se actualiza después de cada nuevo sondeo de la red. La lista de equipos detectados puede contener los siguientes tipo de dispositivos:

- Equipos
- Dispositivos móviles
- Dispositivos de red
- Dispositivos virtuales
- Componentes OEM
- Periféricos de equipos
- Dispositivos conectados
- Teléfonos de VoIP
- Almacenamientos de red

Los equipos detectados durante un sondeo de red se muestran en la subcarpeta **Repositorios** de la carpeta **Hardware** del árbol de consola.

El administrador puede agregar manualmente nuevos dispositivos a la lista de equipos o editar información acerca del equipo ya existente en la red En las propiedades de un dispositivo puede ver y editar información detallada acerca de ese dispositivo.

El administrador puede asignar el atributo de “Equipo de empresa” a los dispositivos detectados. Esta atributo puede asignarse manualmente en las propiedades de un dispositivo o el administrador puede especificar los criterios para que los atributos se asignen automáticamente. En este caso, el atributo de “Equipo de empresa” se asigna por tipo de dispositivo. Puede permitir o prohibir la conexión del equipo a la red por medio del atributo de “Equipo de empresa”.

Kaspersky Security Center permite cancelar equipos. Para hacer esto, seleccione la casilla **El dispositivo está cancelado** en las propiedades del dispositivo. Ese dispositivo no se muestra en la lista de equipos.

EN ESTA SECCIÓN:

Agregar información sobre los dispositivos nuevos 144

Configurar criterios usados para los dispositivos de empresa 145

AGREGAR INFORMACIÓN SOBRE LOS DISPOSITIVOS NUEVOS

Para agregar información acerca de nuevos dispositivos en la red:

1. En la carpeta **Repositorios** del árbol de consola, seleccione la subcarpeta **Hardware**.
2. En el espacio de trabajo de la carpeta **Hardware** haga clic en el enlace **Agregar dispositivo** para abrir la ventana **Nuevo dispositivo**.

   Se abre la ventana **Nuevo dispositivo**.
3. En la ventana **Nuevo dispositivo**, en la lista desplegable **Tipo**, seleccione un tipo de dispositivo que desee agregar.
4. Haga clic en **Aceptar**.

   La ventana de Propiedades del dispositivo se abre en la sección **General**.

5. En la sección **General** complete los campos de entrada con datos del dispositivo. La sección **General** detalla la siguiente configuración:
   - **Dispositivo corporativo**. Seleccione esta casilla si desea asignarle el atributo "Empresa" al dispositivo. Mediante este atributo, puede buscar dispositivos en la carpeta **Hardware**.
   - **El dispositivo está cancelado**. Seleccione esta casilla si no desea que el dispositivo figure en la lista de dispositivos de la carpeta **Hardware**.
6. Haga clic en **Aplicar**.

El nuevo dispositivo se mostrará en el espacio de trabajo de la carpeta **Hardware**.

CONFIGURAR CRITERIOS USADOS PARA LOS DISPOSITIVOS DE EMPRESA

Para configurar los criterios de detección para los dispositivos de empresa:

1. En la carpeta **Repositorios** del árbol de consola, seleccione la subcarpeta **Hardware**.
2. En el espacio de trabajo de la carpeta **Hardware**, haga clic en el enlace **Configurar criterios para los dispositivos corporativos** para abrir la ventana de propiedades de hardware.
3. En la ventana Propiedades de hardware, en la sección **Dispositivos de empresa**, seleccione un modo de asignación del atributo de "Empresa" al dispositivo:
   - **Establecer el atributo de "Empresa" de forma manual**. El atributo de "Equipo de empresa" se asigna manualmente al dispositivo en la ventana de propiedades del dispositivo, en la sección **General**.
   - **Establecer el atributo de "Empresa" de forma automática**. En el bloque de configuración **Por tipo de dispositivo**, especifique los tipos de dispositivos a los que la aplicación asignará automáticamente el atributo de "Empresa".
4. Haga clic en **Aplicar**.

ACTUALIZACIÓN DE BASES DE DATOS Y MÓDULOS DE SOFTWARE

Esta sección describe cómo descargar y distribuir las actualizaciones de las bases de datos y los módulos de software con Kaspersky Security Center.

Para mantener la confiabilidad del sistema de protección, debe actualizar oportunamente las bases de datos y los módulos de la aplicación Kaspersky Lab, administrados a través de Kaspersky Security Center.

Para actualizar las bases de datos y módulos de la aplicación Kaspersky Lab administrados a través de Kaspersky Security Center, se utiliza la tarea **Descargar actualizaciones en el repositorio** del Servidor de administración. Como resultado, las bases de datos y los módulos de la aplicación se descargan desde el origen de actualizaciones.

La tarea **Descargar actualizaciones en el repositorio** no está disponible en los Servidores de administración virtuales. El repositorio del Servidor de administración virtual muestra las actualizaciones descargadas al Servidor de administración maestro.

Puede configurar la comprobación de rendimiento y errores en las actualizaciones antes de que se distribuyan a los equipos cliente.

EN ESTA SECCIÓN:

Creación de la tarea de descarga de actualizaciones en el repositorio 146

Configurar la tarea de descarga de actualizaciones al repositorio 147

Comprobación de actualizaciones descargadas 147

Configurar las directivas de prueba y tareas auxiliares 148

Ver actualizaciones descargadas 149

Distribución automática de las actualizaciones 149

Revertir las actualizaciones instaladas 152

CREACIÓN DE LA TAREA DE DESCARGA DE ACTUALIZACIONES EN EL REPOSITORIO

La tarea Descargar actualizaciones en el repositorio es creada automáticamente por el Asistente de inicio rápido de Kaspersky Security Center. Puede crear únicamente una tarea de descarga de actualizaciones en el repositorio. Por ello, puede crear una tarea de descarga de actualizaciones en el repositorio únicamente si dicha tarea se eliminó de la lista de tareas del Servidor de administración.

Para crear una tarea de descarga de actualizaciones en el repositorio:

1. En el árbol de consola, seleccione la carpeta **Tareas del Servidor de administración**.
2. Comience a crear la tarea en una de las siguientes formas:
   - En el árbol de consola, en el menú contextual de la carpeta **Tareas del Servidor de administración**, seleccione **Nuevo** → **Tarea**.
   - Haga clic en el enlace **Crear una tarea** en el espacio de trabajo.

   Se iniciará el Asistente para nueva tarea. Siga las instrucciones del asistente. En la ventana del asistente **Tipo de tarea**, seleccione **Descargar actualizaciones en el repositorio**.

Una vez finalizado el Asistente, se creará la tarea **Descargar actualizaciones en el repositorio** en la lista de tareas del Servidor de administración.

Cuando un Servidor de administración realiza la tarea de **Descargar actualizaciones en el repositorio**, las actualizaciones de las bases de datos y los módulos del programa se descargan del origen de actualizaciones y se almacenan en la carpeta compartida.

Las actualizaciones se distribuyen a los equipos cliente y a los Servidores de administración secundarios desde la carpeta compartida.

Los siguientes recursos pueden utilizarse como una fuente de actualizaciones para el Servidor de administración:

- Servidores de actualización de Kaspersky Lab: servidores de Kaspersky Lab en los que se cargan las bases de datos antivirus y los módulos de aplicación.
- Servidor de administración maestro.
- Servidor FTP/HTTP o carpeta de actualizaciones de red: servidor FTP, servidor HTTP o carpeta local o de red agregada por el usuario que contiene las actualizaciones más recientes. Al seleccionar una carpeta local, se debe especificar una carpeta de un equipo que tenga instalado el Servidor de administración.

  Para actualizar el Servidor de administración desde un servidor FTP/HTTP o una carpeta de red, se debe copiar en estos recursos la estructura de carpetas correcta con las actualizaciones, que debe ser idéntica a la que se creó mediante los servidores de actualización de Kaspersky Lab.

La selección de la fuente depende de los parámetros de tarea. De forma predeterminada, la actualización se lleva a cabo a través de Internet desde los servidores de actualización de Kaspersky Lab.

CONFIGURAR LA TAREA DE DESCARGA DE ACTUALIZACIONES AL REPOSITORIO

Para configurar la tarea para descargar actualizaciones al repositorio:

1. En el espacio de trabajo de la carpeta **Tareas del Servidor de administración**, seleccione la tarea **Descargar actualizaciones en el repositorio** en la lista de tareas.
2. Abra la ventana de propiedades de la tarea en una de las siguientes formas:
   - En el menú contextual de la tarea, seleccione **Propiedades**.
   - Mediante un clic en el enlace **Cambiar configuración de tarea** en el espacio de trabajo de la tarea seleccionada.

Se abrirá la ventana de propiedades de la tarea **Descargar actualizaciones en el repositorio**. En esta ventana puede configurar cómo se descargarán las actualizaciones al repositorio del Servidor de administración.

COMPROBACIÓN DE ACTUALIZACIONES DESCARGADAS

Para que Kaspersky Security Center verifique las actualizaciones descargadas antes de distribuirlas a los equipos cliente:

1. En el espacio de trabajo de la carpeta **Tareas del Servidor de administración**, seleccione la tarea **Descargar actualizaciones en el repositorio** en la lista de tareas.
2. Abra la ventana de propiedades de la tarea en una de las siguientes formas:
   - En el menú contextual de la tarea, seleccione **Propiedades**.
   - Mediante un clic en el enlace **Cambiar configuración de tarea** en el espacio de trabajo de la tarea seleccionada.
3. En la ventana de propiedades de tarea que se abre, en la sección **Verificación de actualizaciones**, marque la casilla **Verificar actualizaciones antes de distribuirlas** y seleccione la tarea de verificación de actualizaciones de una de las siguientes maneras:
   - Haga clic en **Seleccionar** para seleccionar una tarea de verificación de actualizaciones existente.
   - Haga clic en el botón **Crear** para crear una tarea de verificación de actualizaciones.

     Esto inicia el Asistente para la tarea de verificación de actualizaciones. Siga las instrucciones del asistente.

     Mientras crea la tarea de verificación de actualizaciones, debe seleccionar un grupo de administración que contenga los equipos en los cuales se ejecutará la tarea. Los equipos incluidos en este grupo se denominan *equipos de prueba*.

Se recomienda utilizar equipos con la protección más fiable y la configuración más popular de la aplicación en la red. Este enfoque incrementa la calidad de los análisis y minimiza el riesgo de falsas alarmas y la probabilidad de detección de virus durante el escaneo. Si se detectan virus en los equipos de prueba, se considerará que la tarea de verificación de actualizaciones ha fallado.

4. Haga clic en **Aceptar** para cerrar la ventana de propiedades de la tarea descargar actualizaciones en el repositorio.

Como resultado, la tarea de verificación de actualizaciones se lleva a cabo con la tarea descargar actualizaciones en el repositorio. El Servidor de administración descargará actualizaciones desde el origen, las guardará en un repositorio temporal y ejecutará la tarea de verificación de actualizaciones. Si la tarea se completa correctamente, las actualizaciones se copiarán del repositorio de temporal a la carpeta compartida del Servidor de administración (<Carpeta de instalación de Kaspersky Security Center>\Compartir\Actualizaciones) y se distribuirán a todos los equipos cliente en los que el Servidor de administración es la fuente de actualización.

Si los resultados de la tarea de verificación de actualizaciones muestran que las actualizaciones ubicadas en el repositorio temporal son incorrectas o si la tarea de verificación de actualizaciones se completa con errores, las actualizaciones de este tipo no se copiarán a la carpeta compartida y el Servidor de administración guardará el conjunto de actualizaciones anterior. Las tareas que utilizan el tipo de programación **Al descargar nuevas actualizaciones al repositorio** no se inician tampoco. Estas operaciones se llevarán a cabo con el siguiente inicio de la tarea de descarga de actualizaciones del Servidor de administración si el escaneo de las actualizaciones nuevas finaliza correctamente.

El conjunto de actualizaciones se considera como incorrecto si una de las condiciones siguiente se cumple al menos en un equipo de prueba:

- Se ha producido un error de la tarea de actualización
- El estado de la protección en tiempo real de la aplicación antivirus ha cambiado después de la aplicación de actualizaciones
- Se detectó un objeto infectado mientras se ejecutaba la tarea de escaneo
- Se ha producido un error funcional de la aplicación Kaspersky Lab.

Si ninguna de las condiciones enumeradas es válida para todos los equipos de prueba, el conjunto de actualizaciones se considera como correcto y la tarea de la verificación de datos se completa correctamente.

CONFIGURAR LAS DIRECTIVAS DE PRUEBA Y TAREAS AUXILIARES

Cuando se crea una tarea de verificación de actualizaciones, el Servidor de administración genera directivas de prueba, tareas de actualización de grupo auxiliares y tareas de análisis a pedido.

Las tareas de actualización de grupo auxiliares y tareas de análisis a pedido llevan tiempo. Estas tareas se llevan a cabo cuando se ejecuta la tarea de verificación de actualizaciones. La tarea de verificación de actualizaciones se lleva a cabo cuando las actualizaciones se descargan en el repositorio. La duración de la tarea Descargar actualizaciones en el repositorio incluye la actualización del grupo auxiliar y las tareas de análisis a pedido.

Puede cambiar la configuración de las directivas de prueba y las tareas auxiliares.

Para cambiar la configuración de una directiva de prueba o tarea auxiliar:

1. En el árbol de consola, seleccione un grupo para el que se crea la tarea de verificación de actualizaciones.
2. En el espacio de trabajo del grupo, seleccione una de las siguientes pestañas:
   - **Directivas**, si desea editar la configuración de directivas de prueba
   - **Tareas**, si desea cambiar la configuración de tarea auxiliar.
3. En la pestaña de espacio de trabajo, seleccione una directiva o tarea, a la que desee cambiarle la configuración.
4. Abra la ventana de propiedades de la directiva (tarea) en una de las siguientes formas:
   - En el menú contextual de la directiva (tarea), seleccione **Propiedades**.
   - Haciendo clic en el enlace **Cambiar configuración de directiva** (**Cambiar configuración de tarea**) en el espacio de trabajo de la directiva (tarea) seleccionada.

Para verificar correctamente las actualizaciones, se deben imponer las siguientes restricciones en la modificación de las directivas de prueba y tareas auxiliares:

- En la configuración de tarea auxiliar:
  - Guarde todas las tareas con los niveles de gravedad **Evento crítico** y **Fallo operativo** en el Servidor de administración. Usando los eventos de estos tipos, el Servidor de administración analiza la operación de aplicaciones.
  - Usar el Servidor de administración como el origen de actualizaciones.
  - Especificar tipo de programación de tarea: **Manualmente**
- En la configuración de las directivas de prueba:
  - Deshabilitar los algoritmos de aceleración de escaneo iChecker, iSwift y iStream.
  - Seleccionar acción para realizar en objetos infectados: **No solicitar**/**Omitir**/**Escribir información en un informe**.
- En la configuración de las directivas de prueba y tareas auxiliares:

  Si después de la instalación de actualizaciones para módulos de software se requiere el reinicio del equipo, es necesario que lo reinicie inmediatamente. Si no se reinicia un equipo, es imposible probar este tipo de actualizaciones. Para algunas aplicaciones, la instalación de actualizaciones que requieren el reinicio puede ser prohibida o configurada para solicitar al usuario la confirmación primero. Estas restricciones deben deshabilitarse en la configuración de las directivas de prueba y tareas auxiliares.

VER ACTUALIZACIONES DESCARGADAS

➧ *Para ver la lista de actualizaciones descargadas,*

en el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Actualizaciones**.

El espacio de trabajo de la carpeta **Actualizaciones** muestra la lista de actualizaciones guardadas en el Servidor de administración.

DISTRIBUCIÓN AUTOMÁTICA DE LAS ACTUALIZACIONES

Kaspersky Security Center permite distribuir e instalar automáticamente actualizaciones en equipos cliente y Servidores de administración secundarios.

EN ESTA SECCIÓN:

Distribución automática de actualizaciones a equipos cliente 149
Distribución automática de actualizaciones a Servidores de administración secundarios 150
Instalación automática de módulos de programa para Servidores y Agentes de red 150
Creación y configuración de la lista de Agentes de actualización 151
Descarga de actualizaciones a través de Agentes de actualización 151

DISTRIBUCIÓN AUTOMÁTICA DE ACTUALIZACIONES A EQUIPOS CLIENTE

➧ *Para distribuir las actualizaciones de la aplicación seleccionada a equipos cliente inmediatamente después de la descarga de las actualizaciones en el repositorio del Servidor de administración:*

1. Conéctese al Servidor de administración que administra los equipos cliente.
2. Crear una tarea de distribución de actualizaciones para los equipos cliente seleccionados en una de las siguientes formas:
   - Si desea distribuir actualizaciones a equipos cliente que pertenecen al grupo de administración seleccionado, cree una tarea para el grupo seleccionado (consulte la sección “Crear una tarea de grupo” en la página 65).

- Si desea distribuir actualizaciones a equipos cliente que pertenecen a diferentes grupos de administración o no pertenecen a ninguno, cree una tarea para equipos específicos (consulte la sección “Creación de una tarea para equipos específicos” en la página 66).

Se iniciará el Asistente para nueva tarea. Siga las instrucciones y realice las siguientes acciones:

a. En la ventana del asistente **Tipo de tarea**, en el nodo de la aplicación requerida seleccione la tarea de distribución de actualizaciones.

> El nombre de la tarea de distribución de actualizaciones que se muestra en la ventana **Tipo de tarea** depende de la aplicación para la cual creó esta tarea. Para obtener información detallada sobre los nombres de tareas de actualización para la aplicación de Kaspersky Lab seleccionada, consulte las guías correspondientes.

b. En la ventana del asistente **Programación**, en el campo **Inicio programado**, seleccione **Al descargar nuevas actualizaciones al repositorio**.

Como resultado, la tarea de distribución de actualizaciones creada se iniciará para los equipos seleccionados cada vez que se descargan actualizaciones en el repositorio del Servidor de administración.

Si una tarea de distribución de actualizaciones para la aplicación requerida se crea para los equipos seleccionados, para distribuir automáticamente actualizaciones a equipos cliente, en la ventana de propiedades de la tarea en la sección **Programación**, seleccione la opción **Al descargar nuevas actualizaciones al repositorio** en el campo **Inicio programado**.

DISTRIBUCIÓN AUTOMÁTICA DE ACTUALIZACIONES A SERVIDORES DE ADMINISTRACIÓN SECUNDARIOS

Para distribuir las actualizaciones de la aplicación seleccionada en los Servidores de administración secundarios inmediatamente después de la descarga de las actualizaciones en el repositorio del Servidores de administración:

1. En el árbol de consola, en el nodo del Servidor de administración maestro, seleccione la carpeta **Tareas del Servidor de administración**.
2. En la lista de tareas del espacio de trabajo, seleccione la tarea de descarga de actualizaciones en el repositorio del Servidor de Administración.
3. Abra la sección **Configuración** de la tarea seleccionada en una de las siguientes formas:
   - En el menú contextual de la tarea, seleccione **Propiedades**.
   - Mediante un clic en el enlace **Modificar configuración** en el espacio de trabajo de la tarea seleccionada.
4. En la sección **Configuración** de la ventana de propiedades de la tarea, seleccione la subsección **Otras configuraciones** y haga clic en el enlace **Configurar**. Se abre la ventana **Otras configuraciones**.
5. En la ventana **Otras configuraciones** que se abre, seleccione la casilla **Forzar actualización en los servidores secundarios**.

En la configuración de la tarea de descarga de actualizaciones mediante el Servidor de administración, en la pestaña **Configuración** de la ventana de propiedades de la tarea, seleccione la casilla **Forzar actualización en los servidores secundarios**.

Como resultado, una vez que el Servidor de administración maestro recupera las actualizaciones, las tareas de descarga de actualizaciones se inician automáticamente en los Servidores de administración secundarios sin importar su programación.

INSTALACIÓN AUTOMÁTICA DE MÓDULOS DE PROGRAMA PARA SERVIDORES Y AGENTES DE RED

Para instalar las actualizaciones para los módulos del Servidor de administración y el Agente de red automáticamente luego de que se cargan en el repositorio del Servidor de administración:

1. En el árbol de consola, en el nodo del Servidor de administración maestro, seleccione la carpeta **Tareas del Servidor de administración**.
2. En la lista de tareas del espacio de trabajo, seleccione la tarea de descarga de actualizaciones en el repositorio del Servidor de Administración.

3. Abra la sección **Configuración** de la tarea seleccionada en una de las siguientes formas:
   - En el menú contextual de la tarea, seleccione **Propiedades**.
   - Mediante un clic en el enlace **Modificar configuración** en el espacio de trabajo de la tarea seleccionada.
4. En la sección **Configuración** de la ventana de propiedades de la tarea, seleccione la subsección **Otras configuraciones** y haga clic en el enlace **Configurar**. Se abre la ventana **Otras configuraciones**.
5. En la ventana **Otras configuraciones** que se abre, seleccione las siguientes casillas:
   - **Actualizar módulos del Servidor de administración**. Si se selecciona esta casilla, las actualizaciones de los módulos del Servidor de administración se instalarán inmediatamente después de que finalice la tarea de descarga de actualizaciones que realiza el Servidor de administración. Si esta casilla está desactivada, podrá instalar las actualizaciones sólo manualmente. Esta casilla se activa de forma predeterminada.
   - **Actualizar módulos del Agente de red**. Si esta casilla de verificación está seleccionada, las actualizaciones de los módulos del Agente de red se instalarán después de completar la tarea de descarga de actualizaciones realizada por el Servidor de administración, siempre que se recuperen las actualizaciones de los módulos del Agente de red. Si esta casilla está desactivada, podrá instalar las actualizaciones sólo manualmente. Esta casilla se activa de forma predeterminada.

Como resultado, una vez que el Servidor de administración maestro recupera actualizaciones, todos los módulos del programa seleccionados se instalarán automáticamente.

CREACIÓN Y CONFIGURACIÓN DE LA LISTA DE AGENTES DE ACTUALIZACIÓN

Para crear una lista de Agentes de actualización y configurarlos para la distribución de actualizaciones a equipos cliente dentro de un grupo de administración:

1. Abra la carpeta **Equipos administrados** en el árbol de consola.
2. En la carpeta **Equipos administrados** seleccione un grupo de administración para el cual desea crear la lista de Agentes de actualización.

   Si desea crear una lista de Agentes de actualización para el grupo **Equipos administrados**, puede omitir este paso.
3. Abra la ventana de propiedades del grupo en una de las siguientes formas:
   - En el menú contextual del grupo, seleccione **Propiedades**.
   - Mediante un clic en el enlace **Configurar Agentes de actualización para el grupo**.
4. En la ventana de propiedades de grupo, en la sección **Agentes de actualización**, cree la lista de equipos que actuarán como Agentes de actualización en los grupos de administración, mediante el uso de los botones **Agregar** y **Eliminar**.
5. Para cada Agente de actualización de la lista, puede hacer clic en **Propiedades** para abrir la ventana de propiedades y personalizar la configuración.

DESCARGA DE ACTUALIZACIONES A TRAVÉS DE AGENTES DE ACTUALIZACIÓN

Kaspersky Security Center permite distribuir actualizaciones a equipos cliente incluidos en los grupos de administración no solo a través del Servidor de administración, sino también a través de los Agentes de actualización de estos grupos.

Para configurar la recuperación de actualizaciones para un grupo a través de los Agentes de actualización:

1. Abra la carpeta **Equipos administrados** en el árbol de consola.
2. En la carpeta **Equipos administrados** seleccione el grupo requerido.

   Puede omitir este paso si ya ha seleccionado el grupo **Equipos administrados**.
3. Abra la ventana de propiedades del grupo en una de las siguientes formas:
   - En el menú contextual del grupo, seleccione **Propiedades**.
   - Mediante un clic en el enlace **Configurar Agentes de actualización para el grupo**.

4. En la sección **Agentes de actualización**, en la ventana de propiedades del grupo, seleccione un equipo que actuará como Agente de actualización para equipos cliente incluidos en el grupo.
5. Haga clic en el botón **Propiedades** para abrir las propiedades de este Agente de actualización y seleccione la sección **Origen de actualizaciones**.
6. Seleccione la casilla **Utilizar la tarea de descarga de actualizaciones** y seleccione una tarea de descarga de actualizaciones de alguna de las siguientes maneras:
   - Haga clic en **Seleccionar** para elegir una tarea de descarga de actualizaciones existente.
   - Haga clic en el botón **Nueva tarea** para crear la tarea de descarga de actualizaciones para el Agente de actualización.

La tarea de descarga de actualizaciones a través del Agente de actualización es una tarea del Agente de red; el tipo de tarea es **Descargar actualizaciones en el repositorio**. La tarea para descargar actualizaciones a través del Agente de actualización es una tarea local: debe crearse individualmente para cada equipo que actúa como Agente de actualización.

REVERTIR LAS ACTUALIZACIONES INSTALADAS

Para revertir las actualizaciones que se han instalado:

1. En la carpeta **Administración de aplicaciones** del árbol de consola, seleccione la subcarpeta **Actualizaciones de software**.
2. En el espacio de trabajo de la carpeta **Actualizaciones de software**, seleccione la actualización que desea revertir.
3. En el menú contextual de la actualización, seleccione **Eliminar archivos de actualización**.
4. Ejecute la tarea de actualizar (consulte la sección "Instalación automática de actualizaciones en los equipos cliente" en la página 107).

Cuando esta tarea se ha completado, la actualización instalada en el equipo cliente se revierte y su estado cambia a **Sin instalar**.

TRABAJAR CON CLAVES DE APLICACIÓN

Esta sección describe las características de Kaspersky Security Center relacionadas con el manejo de claves de las aplicaciones administradas de Kaspersky Lab.

Kaspersky Security Center permite realizar una distribución centralizada de las claves de las aplicaciones de Kaspersky Lab en equipos cliente, supervisar su uso y renovar las licencias.

Al agregar una clave mediante Kaspersky Security Center, las propiedades de la clave se guardan en el Servidor de administración. En función de esta información, la aplicación genera un informe sobre el uso de claves y notifica al administrador sobre la caducidad de las licencias y sobre el exceso de restricciones especificado por la configuración de las claves. Puede configurar notificaciones sobre el uso de claves dentro de la configuración del Servidor de administración.

EN ESTA SECCIÓN:

Visualización de información sobre las claves en uso 153

Agregar una clave al repositorio del Servidor de administración 154

Eliminación de una clave del Servidor de administración 154

Distribución de una clave en equipos cliente 154

Distribución automática de una clave 155

Crear y ver un informe de uso de claves 155

VISUALIZACIÓN DE INFORMACIÓN SOBRE LAS CLAVES EN USO

Para ver información sobre las claves en uso,

en el árbol de consola, en la carpeta **Administración de aplicaciones**, seleccione la subcarpeta **Licencias de Kaspersky Lab**.

El espacio de trabajo mostrará una lista de las claves usadas en los equipos cliente.

Junto a cada una de las claves se muestra un icono que corresponde al tipo de uso:

-  - La información sobre la clave se recibe desde un equipo cliente conectado al Servidor de administración. El archivo de esta clave se almacena afuera del Servidor de administración.
-  - El archivo de clave se almacena en el repositorio del Servidor de administración. La distribución automática se deshabilita para esta clave.
-  - El archivo de clave se almacena en el repositorio del Servidor de administración. La distribución automática se habilita para esta clave.

Puede ver información sobre las claves que corresponden a las aplicaciones de un equipo cliente abriendo la ventana de propiedades de la aplicación desde la sección **Aplicaciones** de la ventana de propiedades del equipo cliente.

AGREGAR UNA CLAVE AL REPOSITORIO DEL SERVIDOR DE ADMINISTRACIÓN

Para agregar una clave al repositorio del Servidor de administración:

1. En el árbol de consola, en la carpeta **Administración de aplicaciones**, seleccione la subcarpeta **Licencias de Kaspersky Lab**.
2. Comience la tarea de incorporación de claves mediante uno de los siguientes métodos:
   - desde el menú contextual de la lista de claves, seleccione **Agregar clave**;
   - haga clic en el enlace **Agregar clave** del espacio de trabajo de la lista de claves.

Esto iniciará el Asistente para agregar claves. Siga las instrucciones del asistente.

ELIMINACIÓN DE UNA CLAVE DEL SERVIDOR DE ADMINISTRACIÓN

Para eliminar una clave del Servidor de administración:

1. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
2. En la ventana de propiedades del Servidor de administración que se abre, seleccione la sección **Claves**.
3. Elimine la clave activa o de reserva haciendo clic en el botón **Eliminar**.

Al hacer esto, se elimina la clave.

> Si se ha agregado una llave de reserva, después de eliminar la llave activa, la llave de reserva automáticamente se convierte en la llave activa.

Luego de que se elimine la clave activa, características tales como **Administración del Sistema** (consulte la sección "**Opciones de licencias de Kaspersky Security Center**" en la página 34) y **Administración de dispositivos móviles** (consulte la sección "**Opciones de licencias de Kaspersky Security Center**" en la página 34) se deshabilitan para el Servidor de Administración. Puede agregar (consulte la sección "Agregar una clave al repositorio del Servidor de Administración" en la página 154) una clave que ya ha eliminado; o agregar una clave diferente.

DISTRIBUCIÓN DE UNA CLAVE EN EQUIPOS CLIENTE

Kaspersky Security Center permite distribuir la clave en los equipos cliente mediante la tarea de distribución de claves.

Para distribuir una clave en los equipos cliente:

1. En el árbol de consola, en la carpeta **Administración de aplicaciones**, seleccione la subcarpeta **Licencias de Kaspersky Lab**.
2. Ejecute la tarea de distribución de claves mediante uno de los siguientes métodos:
   - desde el menú contextual de la lista de claves, seleccione **Distribuir una clave**;
   - haga clic en el enlace **Distribuir una clave a equipos administrados** en el espacio de trabajo de la lista de claves.

Esto iniciará el Asistente de creación de tareas de distribución de claves. Siga las instrucciones del asistente.

Las tareas creadas con el Asistente de creación de tareas de distribución de claves son tareas para equipos individuales almacenadas en la carpeta **Tareas para equipos específicos** del árbol de consola.

También puede crear una tarea de distribución de claves local o de grupo mediante el Asistente de creación de tareas para un grupo de administración y para un equipo cliente.

DISTRIBUCIÓN AUTOMÁTICA DE UNA CLAVE

Kaspersky Security Center permite la distribución automática de claves a equipos cliente si están ubicadas en el repositorio de claves del Servidor de administración.

Para distribuir automáticamente una clave a los equipos cliente:

1. En el árbol de consola, en la carpeta **Administración de aplicaciones**, seleccione la subcarpeta **Licencias de Kaspersky Lab**.
2. Seleccione la clave que desea distribuir.
3. Abra la ventana de propiedades de la clave seleccionada mediante uno de los siguientes métodos:
   - en el menú contextual de la clave, seleccione **Propiedades**;
   - haga clic en el enlace **Mostrar ventana de propiedades de clave** en el espacio de trabajo de la clave seleccionada.
4. En la ventana de propiedades de clave que se abre, seleccione la casilla de verificación **Clave implementada automáticamente**. Cierre la ventana de propiedades de clave.

La clave se distribuirá automáticamente a los equipos cliente en los que se haya instalado la aplicación sin una clave activa.

La distribución de la clave se realiza mediante el Agente de red. No se crea ninguna tarea de distribución de clave adicional para la aplicación. La clave se agrega como activa.

Cuando se distribuye una clave, también se tiene en cuenta el límite de licencia especificado en su configuración. Si se alcanza el límite, la clave no se distribuirá en ningún equipo cliente.

CREAR Y VER UN INFORME DE USO DE CLAVES

Para crear un informe sobre el uso de claves en equipos cliente,

en el árbol de consola, en la carpeta **Informes y notificaciones**, seleccione la plantilla de informe denominada **Informe de uso de claves** o cree una plantilla de informe nueva del mismo tipo.

El espacio de trabajo del informe sobre el uso de claves mostrará información sobre las claves activas y adicionales usadas en los equipos cliente. El informe también contiene información sobre los equipos en los que se usan las claves, y sobre las restricciones especificadas en la configuración de las claves.

ALMACENAMIENTOS DE DATOS

Esta sección proporciona información sobre los datos almacenados en el Servidor de administración que se usan para hacer un seguimiento del estado de los equipos cliente y para darles mantenimiento.

Los datos utilizados para realizar un seguimiento del estado de los equipos cliente se muestran en la carpeta **Repositorios** del árbol de consola.

La carpeta **Repositorios** contiene los siguientes objetos:

- las actualizaciones descargadas por el Servidor de administración distribuidas a los equipos cliente (consulte la sección “Ver actualizaciones descargadas” en la página 149);
- lista de elementos de hardware detectados en la red;
- claves detectadas en los equipos cliente (consulte la sección “Trabajar con claves de aplicación” en la página 153);
- archivos puestos en cuarentena en los equipos cliente por aplicaciones antivirus;
- archivos colocados en los repositorios de equipos cliente;
- archivos asignados para escanear más tarde por aplicaciones antivirus.

EN ESTA SECCIÓN:

Exportar una lista de objetos de repositorio a un archivo de texto 156

Paquetes de instalación 156

Cuarentena y Copia de seguridad 157

Archivos no procesados 159

EXPORTAR UNA LISTA DE OBJETOS DE REPOSITORIO A UN ARCHIVO DE TEXTO

Puede exportar la lista de objetos del repositorio a un archivo de texto.

Para exportar la lista de objetos del repositorio a un archivo de texto:

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta necesaria.
2. En la subcarpeta del repositorio, seleccione **Exportar lista**.

   Esto abre la ventana **Exportar lista**, en la que se puede especificar el nombre de archivo de texto y la ruta de la carpeta en la que se colocó.

PAQUETES DE INSTALACIÓN

Kaspersky Security Center coloca paquetes de instalación de aplicaciones por Kaspersky Lab y otros proveedores en áreas de almacenamiento de datos.

Un *paquete de instalación* es un conjunto de archivos requeridos para instalar una aplicación. Un paquete de instalación contiene la configuración de instalación y la configuración inicial de la aplicación que se está instalando.

Si desea instalar una aplicación en un equipo cliente, debe crear un paquete de instalación para esa aplicación (ver la sección “Creación de paquetes de instalación de aplicaciones” en la página 114) o utilice uno existente. La lista de los paquetes de instalación disponibles se almacena en la carpeta **Instalación remota** del árbol de consola, en la subcarpeta **Paquetes de instalación**.

Para obtener información detallada de los paquetes de instalación, consulte la *Guía de implementación de Kaspersky Security Center*.

CUARENTENA Y COPIA DE SEGURIDAD

Las aplicaciones antivirus Kaspersky Lab instaladas en equipos cliente pueden poner objetos en cuarentena o ubicarlos en copia de seguridad durante el escaneo del equipo.

Cuarentena es un área especial donde se almacenan archivos probablemente infectados con virus o archivos que no se pueden desinfectar al momento de su detección.

Almacenamiento de copia de seguridad está diseñado para almacenar copias de seguridad de los archivos que se han eliminado o modificado durante el proceso de desinfección.

Kaspersky Security Center genera una lista de archivos puestos en Cuarentena o Copia de seguridad por la aplicación Kaspersky Lab en equipos cliente. Los Agentes de red en equipos cliente transfieren la información sobre los archivos en Cuarentena y Copia de seguridad al Servidor de administración. Puede usar la Consola de administración para ver las propiedades de los archivos en los repositorios de equipos cliente, ejecutar el escaneo antivirus de estos repositorios y eliminar los archivos almacenados.

Las operaciones con Cuarentena y Copia de seguridad son compatibles con las versiones 6.0 o superior de Kaspersky Anti-Virus para Windows Workstations y Kaspersky Anti-Virus para Windows Servers, y también Kaspersky Endpoint Security 10 para Windows.

Kaspersky Security Center no copia archivos desde repositorios del Servidor de administración. Todos los archivos se almacenan en repositorios de equipos cliente. Puede restaurar archivos solo en un equipo donde esté instalada la aplicación antivirus que colocó el archivo en el repositorio.

EN ESTA SECCIÓN:

Habilitar la administración remota para archivos en repositorios 157
Visualizar propiedades de un archivo colocado en repositorio 158
Eliminar archivos desde los repositorios 158
Restaurar archivos desde los repositorios 158
Guardar un archivo desde los repositorios al disco 158
Escaneo de archivos en Cuarentena 159

HABILITAR LA ADMINISTRACIÓN REMOTA PARA ARCHIVOS EN REPOSITORIOS

De forma predeterminada, no es posible administrar los archivos ubicados en los repositorios de los equipos cliente.

Para habilitar la administración remota de los archivos en los repositorios de los equipos cliente:

1. En el árbol de consola, seleccione un grupo de administración, para el cual desee habilitar la administración remota de los archivos del repositorio.
2. En el espacio de trabajo del grupo, abra la pestaña **Directivas**.
3. En la pestaña **Directivas**, seleccione la directiva de una aplicación de antivirus que coloque los archivos en los repositorios de equipos cliente.
4. En la ventana de configuraciones de directiva del grupo de configuraciones **Informar al Servidor de administración**, seleccione las casillas correspondientes a los repositorios para los cuales desea habilitar la administración remota.

   La ubicación del grupo de configuraciones **Informar al Servidor de administración** de la ventana de propiedades de directivas y los nombres de las casillas dependen de la aplicación antivirus seleccionada.

VISUALIZAR PROPIEDADES DE UN ARCHIVO COLOCADO EN REPOSITORIO

Para ver las propiedades de un archivo en Cuarentena o Copia de seguridad:

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**), seleccione un archivo cuyas propiedades desea ver.
3. Abra la ventana de propiedades de archivo en una de las siguientes formas:
   - En el menú contextual del archivo, seleccione **Propiedades**.
   - Haga clic en el enlace **Mostrar ventana de propiedades de objeto** en el espacio de trabajo del archivo seleccionado.

ELIMINAR ARCHIVOS DESDE LOS REPOSITORIOS

Para eliminar un archivo desde Cuarentena o Copia de seguridad:

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**) seleccione los archivos que desea eliminar mediante las teclas **Mayús** y **Ctrl**.
3. Elimine los archivos en una de las siguientes formas:
   - En el menú contextual de los archivos, seleccione **Eliminar**.
   - Haga clic en **Eliminar objetos** (**Eliminar objeto** si desea eliminar un archivo) en el espacio de trabajo de los archivos seleccionados.

Como resultado, las aplicaciones antivirus que colocaron los archivos en repositorios de equipos cliente eliminarán los archivos desde estos repositorios.

RESTAURAR ARCHIVOS DESDE LOS REPOSITORIOS

Para restaurar un archivo desde Cuarentena o Copia de seguridad:

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**) seleccione los archivos que desea restaurar mediante las teclas **Mayús** y **Ctrl**.
3. Inicie la restauración de archivos en una de las siguientes formas:
   - En el menú contextual de los archivos, seleccione **Restaurar**.
   - Mediante un clic en el enlace **Restaurar** en el espacio de trabajo de los archivos seleccionados.

Como resultado, las aplicaciones antivirus que colocaron los archivos en repositorios de equipos cliente restaurarán los archivos a sus carpetas iniciales.

GUARDAR UN ARCHIVO DESDE LOS REPOSITORIOS AL DISCO

Kaspersky Security Center permite guardar en el disco copias de archivos que fueron colocados por una aplicación antivirus en Cuarentena o Copia de seguridad en un equipo cliente. Los archivos se copian al equipo donde se instaló Kaspersky Security Center, a la carpeta especificada.

Para guardar una copia de archivo desde Cuarentena o Copia de seguridad al disco duro:

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Cuarentena** o **Copia de seguridad**.
2. En el espacio de trabajo de la carpeta **Cuarentena** (**Copia de seguridad**), seleccione un archivo que desea copiar al disco duro.

3. Comience a copiar los archivos en una de las siguientes formas:
   - En el menú contextual del archivo, seleccione el elemento **Guardar en disco**.
   - Haga clic en el enlace **Guardar en disco** en el espacio de trabajo del archivo seleccionado.

Como resultado, la aplicación antivirus que colocó el archivo en Cuarentena en el equipo cliente, guardará una copia del archivo en el disco duro.

ESCANEO DE ARCHIVOS EN CUARENTENA

Para escanear archivos en cuarentena:

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Cuarentena**.
2. En el espacio de trabajo de la carpeta **Cuarentena** seleccione los archivos que desea escanear mediante las teclas **Mayús** y **Ctrl**.
3. Inicie el proceso de escaneo de archivos de una de las siguientes formas:
   - Seleccione **Escanear archivos en cuarentena** en el menú contextual del archivo.
   - Mediante un clic en el enlace **Análisis** en el espacio de trabajo de los archivos seleccionados.

   Como resultado, la aplicación ejecuta la tarea de escaneo a petición para aplicaciones antivirus que colocaron archivos en cuarentena en los equipos donde se almacenan los archivos seleccionados.

ARCHIVOS NO PROCESADOS

La información sobre archivos no procesados detectada en equipos cliente se almacena en la carpeta **Repositorios**, en la subcarpeta **Archivos no procesados**.

El procesamiento y desinfección aplazada por parte de una aplicación antivirus se ejecutan a petición o después de un evento específico. Puede configurar el procesamiento aplazado.

DESINFECCIÓN DE ARCHIVO APLAZADA

Para iniciar una desinfección de archivo aplazada:

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Archivos no procesados**.
2. En el espacio de trabajo de la carpeta **Archivos no procesados**, seleccione el archivo que desea desinfectar.
3. Comience a desinfectar el archivo en una de las siguientes formas:
   - En el menú contextual del archivo, seleccione **Desinfectar**.
   - Mediante un clic en el enlace **Desinfectar** en el espacio de trabajo del archivo seleccionado.

   A continuación, se ejecuta el intento de desinfectar este archivo.

Si un archivo se desinfectó, la aplicación antivirus instalada en el equipo cliente lo restaura a su ubicación inicial. El registro sobre el archivo será eliminado de la lista en la carpeta **Archivos no procesados**. Si no es posible la desinfección del archivo, la aplicación antivirus instalada en el equipo cliente elimina el archivo del equipo. El registro sobre el archivo será eliminado de la lista en la carpeta **Archivos no procesados**.

GUARDAR UN ARCHIVO NO PROCESADO EN DISCO

Kaspersky Security Center permite guardar en el disco copias de archivos no procesados detectados en equipos cliente. Los archivos se copian al equipo donde se instaló Kaspersky Security Center, a la carpeta especificada.

Para guardar una copia de archivo no procesado en el disco:

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Archivos no procesados**.
2. En el espacio de trabajo de la carpeta **Archivos no procesados**, seleccione los archivos que desea copiar al disco duro.

3. Comience a copiar los archivos en una de las siguientes formas:
   - En el menú contextual del archivo, seleccione el elemento **Guardar en disco**.
   - Haga clic en el enlace **Guardar en disco** en el espacio de trabajo del archivo seleccionado.

Como resultado, la aplicación antivirus instalada en un equipo cliente en que se detectó un archivo no procesado guardará una copia del archivo en la carpeta especificada.

ELIMINAR ARCHIVOS DESDE LA CARPETA ARCHIVOS NO PROCESADOS

*Para eliminar un archivo desde la carpeta **Archivos no procesados**:*

1. En el árbol de consola, seleccione la carpeta **Repositorios** y la subcarpeta **Archivos no procesados**.
2. En el espacio de trabajo de la carpeta **Archivos no procesados** seleccione los archivos que desea eliminar mediante las teclas **Mayús** y **Ctrl**.
3. Elimine los archivos en una de las siguientes formas:
   - En el menú contextual de los archivos, seleccione **Eliminar**.
   - Haga clic en **Eliminar objetos** (**Eliminar objeto** si desea eliminar un archivo) en el espacio de trabajo de los archivos seleccionados.

Como resultado, las aplicaciones antivirus que colocaron los archivos en repositorios de equipos cliente eliminarán los archivos desde estos repositorios. Los registros sobre archivos se eliminan de la lista en la carpeta **Archivos no procesados**.

KASPERSKY SECURITY NETWORK (KSN)

Esta sección describe cómo usar la infraestructura de servicios en línea llamada Kaspersky Security Network (KSN). La sección provee detalles sobre KSN, así como instrucciones sobre cómo habilitar KSN, configurar el acceso a KSN y ver las estadísticas de uso del servidor proxy de KSN.

ACERCA DE KSN

Kaspersky Security Network (KSN) es una infraestructura de servicios en línea que brinda acceso a la base de conocimientos en línea de Kaspersky Lab, que contiene información sobre la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza una respuesta más rápida de las aplicaciones de Kaspersky Lab ante las amenazas desconocidas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos. KSN permite el uso de las bases de datos de reputación de Kaspersky Lab para recuperar información acerca de aplicaciones instaladas en los equipos cliente.

Al participar en KSN, acuerda enviar en modo automático a Kaspersky Lab información acerca de la operación de las aplicaciones de Kaspersky Lab (consulte la sección "Acerca de la provisión de datos" en la página 161) instaladas en equipos cliente administrados por Kaspersky Security Center, de acuerdo con la Declaración de KSN. La información se transfiere conforme a la actual configuración de acceso a KSN (consulte la sección "Establecer el acceso a KSN" en la página 162).

La aplicación le solicita que se una a KSN al instalar la aplicación y cuando ejecuta el Asistente de Inicio Rápido (consulte la sección "Asistente de Inicio Rápido de Kaspersky Security Center" en la página 38). Puede iniciar o detener el uso de KSN en cualquier momento que use la aplicación (consulte la sección "Habilitar y Deshabilitar KSN" en la página 163).

Los equipos cliente administrados por el Servidor de administración interactúan con KSN a través del servicio de proxy de KSN. El uso del servicio proxy de KSN le proporciona las siguientes opciones:

- Los equipos cliente pueden enviar solicitudes a KSN y transferir información a KSN, incluso si no se tiene acceso directo a Internet.
- El proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga de trabajo en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un equipo cliente.

Puede configurar el Proxy de KSN en la sección **Servidor Proxy de KSN** de la ventana de propiedades del Servidor de Administración (consulte la sección "Configuración del acceso a KSN" en la página 162).

ACERCA DEL APROVISIONAMIENTO DE DATOS

Al aceptar los términos del Contrato de licencia y participar en el programa Kaspersky Security Network, usted acepta enviar a Kaspersky Lab de manera automática información sobre el funcionamiento de las aplicaciones de Kaspersky Lab instaladas en los equipos cliente administrados por Kaspersky Security Center. Los especialistas de Kaspersky Lab usan la información obtenida de equipos cliente para solucionar los problemas de las aplicaciones de Kaspersky Lab o para modificar algunas de sus características.

Si participa en el programa Kaspersky Security Network, acepta enviar a Kaspersky Lab de manera automática la siguiente información de su equipo obtenida por Kaspersky Security Center:

- Nombre, versión e idioma del producto de software para el cual se instalará la actualización.
- Versión de la base de datos de actualización que usa el software durante la instalación.
- El resultado de la instalación de la actualización.
- Identificación del equipo y versión del Agente de red que utiliza.
- La configuración de software usada cuando instala actualizaciones, como las identificaciones de las operaciones ejecutadas y los códigos de los resultados de esas operaciones.

Si cancela su participación en el programa Kaspersky Security Network, los detalles mencionados anteriormente no se enviarán a Kaspersky Lab.

Kaspersky Lab protege la información obtenida en virtud de los requisitos de la legislación actual y las reglas existentes de Kaspersky Lab. Kaspersky Lab usa la información obtenida únicamente de forma no personalizada y con el fin de confeccionar estadísticas generales. Los datos de estadísticas generales se generan de manera automática de acuerdo con la información obtenida originalmente y no contienen detalles personales ni otra información confidencial. La información obtenida originalmente se almacena de manera cifrada y se borra a medida que se acumula (dos veces al año). El período de almacenamiento de los datos de estadísticas generales es ilimitado.

El suministro de datos se acepta de manera voluntaria. La característica de provisión de datos se puede habilitar o desactivar en cualquier momento en la ventana de configuración de la aplicación (consulte la sección "Interacción del Servidor de Administración con el servicio Proxy KSN" en la página 53).

CONFIGURACIÓN DEL ACCESO A KSN

Para establecer el acceso del Servidor de administración a KSN:

1. En el árbol de consola, seleccione el Servidor de administración para el que necesita configurar el acceso a KSN.
2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
3. En la ventana de propiedades del Servidor de administración, en la sección **servidor proxy de KSN** seleccione la subsección **Configuración del servidor proxy para KSN**.
4. Seleccione la casilla **Usar Servidor de administración como servidor proxy** para habilitar el servicio de proxy de KSN.

   Los datos se envían desde los equipos cliente a KSN de acuerdo con la directiva de Kaspersky Endpoint Security activa en esos equipos. Si esta casilla está desactivada, no se enviarán datos a KSN desde el Servidor de administración y los equipos cliente, a través de Kaspersky Security Center. Sin embargo, los equipos cliente pueden enviar datos directamente a KSN de acuerdo con su configuración.

   Si esta casilla está desactivada, los equipos cliente envían los datos permitidos por la directiva de Kaspersky Endpoint Security para Windows.
5. Seleccione **Enviar estadísticas de Kaspersky Security Center a KSN**.

   Si se selecciona esta casilla, los equipos cliente enviarán los resultados de instalación de la revisión a Kaspersky Lab. Al seleccionar esta casilla, debe leer y aceptar los términos de la Declaración de KSN.

   Si está usando KSN Privada (la infraestructura de KSN no está localizada en los servidores de Kaspersky Lab, sino, por ejemplo, dentro de la red de proveedores de Internet), seleccione la casilla **Configurar KSN privada** y haga clic en el botón **Seleccionar archivo con los ajustes de KSN** para descargar la configuración de la KSN privada (archivos con las extensiones pkcs7, pem). Después de que se descarga la configuración, la interfaz muestra el nombre y contactos del proveedor, así como la fecha de creación del archivo con la configuración de la KSN privada.

   La KSN privada es compatible con Kaspersky Security Center 10 Service Pack 1 y Kaspersky Endpoint Security 10 Service Pack 1.
6. Configure la conexión del Servidor de administración al servicio de proxy de KSN:
   - En el campo de entrada **Puerto TCP** puede especificar el número del puerto TCP que se utilizará para establecer conexión con el proxy de KSN. El puerto predeterminado para conectarse al proxy de KSN es 13111.
   - Si desea que el Servidor de administración esté conectado al proxy de KSN a través de un puerto UDP, seleccione la casilla **Usar puerto UDP** y especifique el número de puerto en el campo **puerto UDP**. Esta casilla está desactivada de forma predeterminada y se utiliza el puerto UDP 15111 para conectarse al proxy de KSN.
7. Haga clic en **Aceptar**.

Como resultado, se guardará la configuración de acceso a KSN.

HABILITAR Y DESHABILITAR KSN

- *Para habilitar KSN:*

  1. En el árbol de consola seleccione el Servidor de administración para el que necesita habilitar KSN.
  2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
  3. En la ventana de propiedades del Servidor de administración, en la sección **servidor proxy de KSN** seleccione la subsección **Configuración del servidor proxy para KSN**.
  4. Seleccione **Usar Servidor de administración como servidor proxy**.

     Como resultado, se habilitará el servicio de proxy de KSN.
  5. Seleccione **Enviar estadísticas de Kaspersky Security Center a KSN**.

     Como resultado, se habilitará KSN.

     Si se selecciona esta casilla, los equipos cliente enviarán los resultados de instalación de la revisión a Kaspersky Lab. Al seleccionar esta casilla, debe leer y aceptar los términos de la Declaración de KSN.
  6. Haga clic en **Aceptar**.

- *Para deshabilitar KSN:*

  1. En el árbol de consola seleccione el Servidor de administración para el que necesita habilitar KSN.
  2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
  3. En la ventana de propiedades del Servidor de administración, en la sección **servidor proxy de KSN** seleccione la subsección **Configuración del servidor proxy para KSN**.
  4. Desactive la casilla **Usar Servidor de administración como servidor proxy** para deshabilitar el servicio de proxy de KSN, o desactive la casilla **Enviar estadísticas de Kaspersky Security Center a KSN**.

     Si esta casilla está desactivada, los equipos cliente no enviarán los resultados de instalación de la revisión a Kaspersky Lab.

     Si está usando la KSN privada, desactivar la casilla **Configurar KSN privada**.

     Como resultado, se deshabilitará KSN.
  5. Haga clic en **Aceptar**.

VER LAS ESTADÍSTICAS DEL SERVIDOR PROXY DE KSN

La aplicación permite ver la información estadística a cerca del servidor proxy de KSN.

- *Para ver las estadísticas del servidor proxy de KSN:*

  1. En el árbol de consola, seleccione el Servidor de administración para el que necesita ver las estadísticas de KSN.
  2. En el menú contextual del Servidor de administración, seleccione **Propiedades**.
  3. En la ventana de propiedades del Servidor de administración, en la sección **servidor proxy de KSN** seleccione la subsección **Estadísticas del servidor proxy de KSN**.

  Esta sección muestra las estadísticas de operación del servidor proxy de KSN. De ser necesario, actualice las estadísticas haciendo clic en el botón **Actualizar** y exporte los datos estadísticos a un archivo CSV haciendo clic en el botón **Exportar a archivo**.

CONTACTAR CON EL SERVICIO DE SOPORTE TÉCNICO

En esta sección se proporciona información sobre las formas y las condiciones para brindarle soporte técnico.

EN ESTA SECCIÓN:

Acerca del soporte técnico 164

Consultas por teléfono al Servicio de soporte técnico 164

Consultas mediante Kaspersky CompanyAccount al servicio de soporte técnico 164

ACERCA DEL SOPORTE TÉCNICO

Si no encuentra una solución a su problema en la documentación o en una de las fuentes de información acerca de la aplicación (ver la sección "Fuentes de información acerca de la aplicación" en la página 12), le recomendamos que se comunique con el Soporte técnico de Kaspersky Lab. Los especialistas responderán sus preguntas acerca de la instalación y el uso de la aplicación.

El soporte técnico solo está disponible para los usuarios que compraron la licencia comercial. Los usuarios que no han recibido una licencia de prueba no tienen derecho a recibir soporte técnico.

Antes de comunicarse con Soporte técnico, por favor lea las reglas de soporte técnico (http://support.kaspersky.com/sp/support/rules).

Puede comunicarse con el Servicio de soporte técnico de las siguientes maneras:

- Llamada al Soporte técnico de Kaspersky Lab.
- Envío de una solicitud al Soporte técnico mediante el servicio web Kaspersky CompanyAccount.

CONSULTAS POR TELÉFONO AL SERVICIO DE SOPORTE TÉCNICO

Si surge algún problema urgente, puede llamar por teléfono a los especialistas de Soporte técnico de Kaspersky Lab (http://support.kaspersky.com/mx/b2c).

Antes de comunicarse con Soporte técnico, se recomienda que lea las reglas de soporte técnico (http://support.kaspersky.com/support/rules). Estas reglas brindan información sobre los horarios de llamada al Soporte técnico de Kaspersky Lab, así como los datos que necesitará el especialista de soporte técnico para ayudarlo.

CONSULTAS MEDIANTE KASPERSKY COMPANYACCOUNT AL SERVICIO DE SOPORTE TÉCNICO

Kaspersky CompanyAccount (https://companyaccount.kaspersky.com) es un servicio web para las compañías que usan las aplicaciones de Kaspersky Lab. El servicio web Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los especialistas de Kaspersky Lab mediante solicitudes en línea. El servicio web Kaspersky CompanyAccount le permite monitorear el progreso del procesamiento de solicitudes electrónicas realizado por los especialistas de Kaspersky Lab y almacenar un historial de las solicitudes electrónicas.

Puede registrar a todos los empleados de su organización en una cuenta única en Kaspersky CompanyAccount. Una cuenta única le permite administrar de forma centralizada las solicitudes electrónicas enviadas por los empleados registrados a Kaspersky Lab y además administrar los privilegios de estos empleados a través de Kaspersky CompanyAccount.

El servicio web Kaspersky CompanyAccount está 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 de Soporte Técnico (http://support.kaspersky.com/faq/companyaccount_help).

GLOSARIO

A

ACTUALIZACIÓN DISPONIBLE

Un paquete de actualizaciones para los módulos de una aplicación de Kaspersky Lab incluso un conjunto de revisiones urgentes emitidas durante un cierto intervalo de tiempo y modificaciones de la arquitectura de la aplicación.

ADMINISTRADOR DE KASPERSKY SECURITY CENTER

Persona que administra las operaciones de la aplicación mediante el sistema de Kaspersky Security Center de administración remota centralizada.

AGENTE DE ACTUALIZACIÓN

Un equipo dentro de un grupo de administración que actúa como un nodo de comunicación intermediario entre los equipos del mismo grupo y el Servidor de administración.

Un Agente de actualización puede realizar las siguientes funciones:

Administrar las actualizaciones y los paquetes de instalación recibidos del Servidor de administración distribuyéndolos a los equipos cliente del grupo (incluido un método, como la multidifusión a través de UDP).

Esta función acelera la distribución de actualizaciones y permite la liberación de recursos del Servidor de administración.

Distribuir directivas y tareas de grupo mediante la multidifusión a través de UDP.

Actuar como una puerta de enlace de conexión al Servidor de administración para los equipos del grupo.

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

La disponibilidad de un Agente de actualización que funciona como la puerta de enlace de conexión no bloquea la opción de conexión directa entre los equipos administrados y el Servidor de administración. Si la puerta de enlace de conexión no está disponible, pero la conexión directa con el Servidor de administración es técnicamente posible, los equipos administrados se conectarán directamente al Servidor.

Sondear la red de equipos en la que está ubicado.

Realizar la instalación remota de la aplicación a través de las herramientas de Microsoft Windows, incluida la instalación en equipos cliente sin el Agente de red.

Esta función permite transferir en forma remota paquetes de instalación del Agente de red a equipos cliente ubicados en redes a las que el Servidor de administración no tiene acceso.

Podrá ver la lista completa de Agentes de actualización para los grupos de administración si crea un informe sobre la lista de Agentes de actualización.

El alcance de un Agente de actualización es el grupo de administración al que se ha asignado, así como sus subgrupos de todos los niveles de incrustación. Si se asignaron varios Agentes de actualización en la jerarquía de los grupos de administración, el Agente de red del equipo administrado se conecta al Agente de actualización más cercano en la jerarquía.

AGENTE DE AUTENTICACIÓN

Interfaz que permite pasar el procedimiento de autenticación para obtener acceso a los discos duros cifrados y reiniciar el sistema operativo después del cifrado del disco duro del sistema.

AGENTE DE RED

Un componente de Kaspersky Security Center que permite la interacción entre el Servidor de administración y las aplicaciones de Kaspersky Lab instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es el mismo para todos los productos para Windows de la empresa. Existen versiones distintas del Agente de red para los productos de Kaspersky Lab desarrollados para Novell®, Unix® y Mac.

B

BASES DE DATOS ANTIVIRUS

Bases de datos que contienen información sobre amenazas para la seguridad del equipo conocidas por Kaspersky Lab al momento de publicación de las bases de datos antivirus. Los registros que se encuentran en las bases de datos antivirus permiten detectar código malintencionado en los objetos analizados. Las bases de datos antivirus son generadas por especialistas de Kaspersky Lab y actualizadas cada una hora.

C

CERTIFICADO GENERAL

Un certificado está destinado a identificar al usuario de un dispositivo móvil.

CLAVE ACTIVA

Clave que se usa en el momento de trabajar con la aplicación.

CLAVE ADICIONAL

Clave que comprueba el uso de la aplicación, pero que no se usa en simultáneo con la activa.

CLIENTE DEL SERVIDOR DE ADMINISTRACIÓN (EQUIPO CLIENTE)

Equipo, servidor o estación de trabajo en los que están en ejecución el Agente de red y las aplicaciones de Kaspersky Lab administradas.

CONSOLA DE ADMINISTRACIÓN

Componente de Kaspersky Security Center que proporciona una interfaz de usuario para los servicios administrativos del Servidor de administración y el Agente de red.

D

DERECHOS DEL ADMINISTRADOR

El nivel de los derechos y privilegios del usuario requeridos para la administración de objetos Exchange dentro de una organización Exchange.

DIRECTIVA

Conjunto de parámetros de la aplicación en un grupo de administración gestionado a través de Kaspersky Security Center. La configuración de una aplicación puede diferir según el grupo. Se define una directiva específica para cada aplicación. Una directiva incluye las opciones para la configuración completa de todas las funciones de la aplicación.

DIRECTIVA MDM

Un conjunto de parámetros de la aplicación utilizados para administrar dispositivos móviles a través de Kaspersky Security Center. Se utilizan diferentes parámetros de la aplicación para administrar diferentes tipos de dispositivos móviles. Una directiva incluye las opciones para la configuración completa de todas las funciones de la aplicación.

DISPOSITIVO EAS

Dispositivo móvil conectado al Servidor de administración por medio del protocolo Exchange ActiveSync®. Dispositivos en sistemas operativos iOS, Android™ y Windows Phone® pueden conectarse y administrarse a través del protocolo Exchange ActiveSync.

DISPOSITIVO KES

Un dispositivo móvil conectado al Servidor de administración y administrado a través de Kaspersky Endpoint Security para Android.

DISPOSITIVO CON MDM DE IOS

Un dispositivo móvil que está conectado al Servidor de dispositivos móviles con MDM de iOS a través del protocolo MDM de iOS. Dispositivos que ejecutan el sistema operativo iOS que pueden conectarse y administrarse a través del protocolo MDM de iOS.

F

FOCO DE VIRUS

Serie de intentos deliberados de infectar el equipo con un virus.

G

GRUPO DE ADMINISTRACIÓN

Un conjunto de equipos agrupados, de acuerdo con las funciones realizadas y las aplicaciones Kaspersky Lab instaladas en dichos equipos. Los equipos se agrupan para facilitar su administración como una única entidad. Un grupo puede incluir otros grupos. Un grupo puede contener directivas de grupo para cada aplicación instalada en este y tareas de grupo apropiadas.

GRUPO DE APLICACIONES CON LICENCIA

Grupo de aplicaciones creado según criterios establecidos por el administrador (por ejemplo, por el proveedor), para el cual se mantienen las estadísticas de instalaciones en equipos cliente.

GRUPO DE ROLES

Grupo de usuarios de los dispositivos móviles de Exchange ActiveSync a los que se les otorga derechos del administrador idénticos (consulte la sección "derechos del Administrador" en la página 172).

K

KASPERSKY SECURITY NETWORK (KSN)

Una infraestructura de servicios en línea que brinda acceso a la base de conocimientos en línea de Kaspersky Lab, que contiene información sobre la reputación de los archivos, los recursos web y el software. El uso de los datos de Kaspersky Security Network garantiza una respuesta más rápida de las aplicaciones de Kaspersky Lab ante las amenazas desconocidas, mejora la eficacia de algunos componentes de protección y reduce el riesgo de falsos positivos.

P

PAQUETE DE INSTALACIÓN

Conjunto de archivos creado para la instalación remota de una aplicación de Kaspersky Lab mediante el sistema de administración remota de Kaspersky Security Center. El paquete de instalación contiene un rango de configuraciones necesarias para instalar la aplicación y ejecutarla inmediatamente después de su instalación. Los valores de los parámetros corresponden con aquellos predeterminados por la aplicación. El paquete de instalación se crea usando archivos con las extensiones .kpd y .kud que se incluyen en el kit de distribución.

PERFIL

Un conjunto de opciones de configuración de dispositivos móviles Exchange ActiveSync que define su comportamiento cuando están conectados a un servidor Microsoft Exchange.

PERFIL DE MDM DE IOS

Conjunto de opciones de configuración para conectar los dispositivos móviles de iOS al Servidor de administración. El usuario instala un perfil de MDM de iOS en un dispositivo móvil, después de lo cual este dispositivo móvil se conecta al Servidor de administración.

PERFIL DE APROVISIONAMIENTO

Conjunto de opciones de configuración para el funcionamiento de aplicaciones en dispositivos móviles de iOS. Un perfil de aprovisionamiento contiene información sobre la licencia; está vinculado a una aplicación específica.

PERFIL DE CONFIGURACIÓN

Directiva que contiene un conjunto de opciones de configuración y restricciones para un dispositivo móvil con MDM de iOS.

R

RESTAURACIÓN

Reubicación del objeto original de la Cuarentena o Copia de seguridad a su carpeta original donde el objeto había sido almacenado antes de su puesta en cuarentena, desinfección o eliminación, o en una carpeta definida por un usuario.

RESTAURACIÓN DE LOS DATOS DEL SERVIDOR DE ADMINISTRACIÓN

Restauración de los datos del Servidor de administración a partir de la información guardada en la copia de seguridad mediante la utilidad de copia de seguridad. La utilidad puede restaurar:

- base de datos de información del Servidor de administración (directivas, tareas, parámetros de la aplicación, eventos guardados en el Servidor de administración);
- información de configuración de la estructura de los grupos de administración y los equipos cliente;
- el repositorio de los archivos de instalación para la instalación remota de aplicaciones (contenido de las carpetas Paquetes, Desinstalar actualizaciones);
- Certificado del Servidor de administración.

S

SERVICIOS DE ACTUALIZACIÓN DEL SERVIDOR DE WINDOWS (WSUS)

Aplicación que se utiliza para la distribución de actualizaciones de aplicaciones de Microsoft en equipos de usuarios de la red de una organización.

SERVIDOR DE ADMINISTRACIÓN VIRTUAL

Componente de Kaspersky Security Center diseñado para administrar el sistema de protección de la red de una organización cliente.

El Servidor de administración virtual es un caso particular de Servidor de administración secundario y posee las siguientes restricciones en comparación con el Servidor de administración físico:

- El Servidor de administración virtual puede crearse solamente en el Servidor de administración maestro.
- El Servidor de administración virtual usa bases de datos del Servidor de administración maestro en su funcionamiento: las tareas de copia de seguridad de los datos, las tareas de recuperación de datos, las tareas de actualización de verificación, y las tareas de descarga de actualizaciones no son compatibles con el Servidor virtual. Estas tareas existen únicamente en el Servidor de administración maestro.
- El Servidor virtual no admite la creación de Servidores de administración secundarios (incluidos Servidores virtuales).

SERVIDOR DE DISPOSITIVOS MÓVILES

Componente de Kaspersky Security Center que proporciona acceso a los dispositivos móviles y permite administrarlos por medio de la Consola de administración.

SERVIDOR DE DISPOSITIVOS MÓVILES EXCHANGE ACTIVESYNC

Componente de Kaspersky Security Center instalado en un equipo cliente que permite la conexión de dispositivos móviles Exchange ActiveSync al Servidor de administración.

SERVIDOR DE DISPOSITIVOS MÓVILES CON MDM DE IOS

Componente de Kaspersky Security Center instalado en un equipo cliente que permite la conexión de dispositivos móviles iOS al Servidor de administración y la administración de dispositivos móviles iOS por medio del servicio Apple Push Notifications (APNs).

SERVIDOR WEB DE KASPERSKY SECURITY CENTER

Un componente de Kaspersky Security Center que se instala junto con el Servidor de administración. El Servidor web está diseñado para la transferencia de paquetes de instalación independiente, perfiles MDM de iOS MDM, y archivos de la carpeta compartida a la red.

T

TAREA

Las funciones que realiza la aplicación de Kaspersky Lab se implementan como tareas, como por ejemplo: Protección en tiempo real, Escaneo completo, Actualización de la base de datos.

TAREA DE GRUPO

Una tarea definida por un grupo de administración y realizada en todos los equipos cliente de dicho grupo.

TAREA LOCAL

Una tarea definida y ejecutada en un solo equipo cliente.

TAREA PARA EQUIPOS ESPECÍFICOS

Tarea asignada a un conjunto de equipos cliente desde grupos de administración arbitrarios y realizada en dichos hosts.

U

USUARIOS INTERNOS

Las cuentas de usuarios internos se utilizan para trabajar con Servidores de administración virtuales. Con la cuenta de un usuario interno, el administrador de un Servidor de administración interno puede iniciar Kaspersky Security Center Web Console para comprobar el estado de seguridad antivirus de una red. Kaspersky Security Center otorga los permisos de usuarios reales a los usuarios internos de la aplicación.

Las cuentas de los usuarios internos se crean y utilizan solo para trabajar dentro de Kaspersky Security Center. No se transfiere ningún dato sobre usuarios internos al sistema operativo. Kaspersky Security Center autentica a los usuarios internos.

V

VULNERABILIDAD

Un error en un sistema operativo o una aplicación que puede ser explotado por los creadores de software malicioso para penetrar en el sistema operativo o en la aplicación y poner en riesgo su integridad. Numerosas vulnerabilidades en un sistema operativo lo hacen poco confiable, dado que los virus que han penetrado en el sistema operativo pueden provocar errores en el funcionamiento del sistema operativo y en las aplicaciones instaladas.

Z

ZONA DESMILITARIZADA (DMZ)

Una zona desmilitarizada es un segmento de una red local que contiene servidores que responden a solicitudes de la Web global. Para garantizar la seguridad de la red local de una organización, el acceso a LAN desde la zona desmilitarizada está protegido por un firewall.

KASPERSKY LAB ZAO

El software de Kaspersky Lab tiene fama internacional por su protección contra virus, software malicioso, correo no deseado, ataques de hackers e intrusiones y otras amenazas.

En el 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 fabricante de sistemas de protección de equipos preferido entre los usuarios domésticos de Rusia, según la encuesta "TGI-Russia 2009" de COMCON.

Kaspersky Lab se creó en Rusia en 1997. En la actualidad, es un grupo internacional de compañías con sede en Moscú y posee cinco divisiones regionales que administran la actividad de la compañía en Rusia, Europa Oriental y Occidental, Oriente Medio, África, América del Norte y del Sur, Japón, China y otros países de la región de Asia-Pacífico. La compañía emplea más de 2000 especialistas calificados.

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 antivirus para equipos de escritorio, equipos portátiles, equipos de bolsillo y también para teléfonos inteligentes y otros dispositivos móviles.

Kaspersky Lab ofrece aplicaciones y servicios para proteger estaciones de trabajo, servidores web y de archivos, gateways de correo y firewalls. Cuando se usan junto con el sistema de administración centralizada de Kaspersky Lab, estas soluciones garantizan la protección automatizada efectiva para las compañías y organizaciones contra las amenazas informáticas. Los productos de Kaspersky Lab están certificados por los principales laboratorios de pruebas, son compatibles con el software de muchos proveedores de aplicaciones para equipos y están optimizados para que puedan ejecutarse en varias plataformas de software.

Los analistas de virus de Kaspersky Lab trabajan en todo momento. Todos los días, ellos descubren cientos de amenazas informáticas nuevas, crean herramientas para detectarlas y desinfectarlas y las incorporan en las bases de datos que las aplicaciones de Kaspersky Lab usan. *La base de datos de antivirus de Kaspersky Lab se actualiza cada hora*, *base de datos Anti-spam – cada cinco minutos*.

TECNOLOGÍAS. Muchas tecnologías que ahora son parte integral de las herramientas antivirus modernas fueron desarrolladas por Kaspersky Lab. No es coincidencia que muchos otros desarrolladores utilicen el núcleo de Kaspersky Anti-Virus en sus productos, tales como: SafeNet (EE. UU.), Alt-N Technologies (EE. UU.), Blue Coat Systems (EE. UU.), Check Point Software Technologies (Israel), Clearswift (Reino Unido), CommuniGate Systems (EE. UU.), Openwave Messaging (Irlanda), D-Link (Taiwán), M86 Security (EE. UU.), GFI Software (Malta), IBM (EE. UU.), Juniper Networks (EE. UU.), LANDesk (EE. UU.), Microsoft (EE. UU.), Netasq+Arkoon (Francia), NETGEAR (EE. UU.), Parallels (EE. UU.), SonicWALL (EE. UU.), WatchGuard Technologies (EE. UU.) y ZyXEL Communications (Taiwán). Gran parte de las tecnologías innovadoras de la organización están patentadas.

LOGROS. Con el paso de los años, Kaspersky Lab ha obtenido cientos de premios por sus servicios para combatir las amenazas informáticas. Por ejemplo, en 2010, Kaspersky Anti-Virus recibió algunos de los mejores premios Advanced+ en una prueba realizada por AV-Comparatives, un famoso laboratorio austríaco de aplicaciones antivirus. 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 300 millones de usuarios, y sus clientes corporativos suman más de 200.000.

Sitio oficial de Kaspersky Lab:	http://latam.kaspersky.com
Enciclopedia de virus:	http://www.securelist.com
Laboratorio Antivirus:	newvirus@kaspersky.com (solamente para enviar archivos que probablemente estén infectados en formato de archivo comprimido)
Foro web de Kaspersky Lab	http://forum.kaspersky.com/index.php?showforum=80

INFORMACIÓN ACERCA DE CÓDIGO DE TERCEROS

La información acerca de código de terceros se incluye en un archivo denominado legal_notices.txt, que está almacenado en la carpeta de instalación de la aplicación.

ACERCA DE LA TECNOLOGÍA NAC/ARP ENFORCEMENT

La tecnología NAC Solution/ARP Enforcement es una tecnología lícita dedicada a garantizar la seguridad y reglamentar el acceso a una red corporativa al asegurar el cumplimiento de los dispositivos de las directivas de seguridad corporativa.

Comportamiento y obligaciones del usuario

El usuario acepta cumplir las leyes y reglamentaciones locales, estatales, nacionales, internacionales y supranacionales vigentes, además de las especificaciones mencionadas en la documentación o en los documentos de transferencia relacionados del distribuidor autorizado del que el usuario obtuvo el software y

- (a) no usar el software para fines ilícitos,
- (b) no transmitir ni almacenar material que infrinja los derechos de propiedad intelectual o cualquier otro derecho de terceros o que sea ilegal, no autorizado, difamatorio u ofensivo, o que invada la privacidad de terceros,
- (c) no transmitir ni almacenar datos de propiedad de terceros, sin obtener de manera anticipada el consentimiento estipulado por ley del propietario de los datos para la transmisión de datos,
- (d) no transmitir material que incluya virus de software u otros códigos, archivos o programas informáticos perjudiciales,
- (e) no llevar a cabo actos que interfieran o interrumpan el funcionamiento del servidor o las redes asociado al software,
- (f) no intentar obtener acceso no autorizado a sistemas informáticos o redes asociados al software.

El usuario tiene restringido el uso del software de la manera prevista y dentro de las condiciones del marco de trabajo legal específico en su país. Tenga en cuenta que el uso de este software de seguridad dentro de las redes puede afectar las disposiciones de las leyes de protección de datos en la UE o en los países miembros de la UE. Asimismo, en el uso operativo, es posible que se deban cumplir también las leyes de trabajo colectivo.

MEJOR PROTECCIÓN CON KASPERSKY SECURITY NETWORK

Kaspersky Lab ofrece un nivel adicional de protección a los usuarios a través de Kaspersky Security Network. Este método de protección está diseñado para combatir amenazas persistentes avanzadas y ataques desde el día cero. Las tecnologías de nube integradas y la experiencia de los analistas de virus de Kaspersky Lab hacen que Kaspersky Endpoint Security sea una opción inigualable contra las amenazas de red más sofisticadas.

Podrá encontrar detalles sobre la protección mejorada de Kaspersky Endpoint Security en el sitio web de Kaspersky Lab.

INFORMACIÓN SOBRE LA MARCA REGISTRADA

Las marcas registradas y marcas de servicio son propiedad de sus respectivos propietarios.

Active Directory, Data Access, Internet Explorer, Microsoft, SQL Server, Windows, Windows Server y Windows Vista son marcas comerciales de Microsoft Corporation registradas en los Estados Unidos y en otros países.

Apache y el logotipo de la pluma de Apache son marcas registradas de Apache Software Foundation.

Cisco es una marca comercial registrada o marca comercial de Cisco Systems, Inc. y sus afiliadas en los Estados Unidos y otros países.

Linux es una marca comercial de propiedad de Linus Torvalds y registrada en los Estados Unidos y en otros países.

Mac, Mac OS, Apple, iPhone, iTunes son marcas registradas de Apple Inc.

Novell es una marca comercial propiedad de Novell, Inc. y registrada en los Estados Unidos y en otros países.

UNIX es una marca comercial registrada en los Estados Unidos y en otros partes, cuya licencia se otorga exclusivamente a través de X/Open Company Limited.

ÍNDICE

A

Actualización de la aplicación 106

Actualizar
- distribución....149, 150, 151
- Escanear 147
- Recuperación....146
- Ver....149

Administración de la aplicación 58

Administrar
- Claves....153
- Configuración inicial....38
- Directivas....58
- Equipo cliente 78

Árbol de consola....22

Asistente de conversión de directivas y tareas 61, 68

C

Certificado
- correo 86, 119
- general....86, 119
- Instalar un certificado para un usuario....86, 119
- VPN 86, 119

Certificado del Servidor de administración 49

Cifrado....135

Clave 34, 153
- distribución....155
- Eliminar....154
- Informe 155
- Instalación 154

D

Directivas
- activación....59
- Copiado 60
- Crear....59
- Eliminación 60
- Exportar 61
- Importar 61

Dispositivo móvil con MDM de iOS 124

Dispositivo móvil Exchange ActiveSync 121

E

Eliminar
- Directiva....60
- Servidor de administración 50

Equipos cliente....42
- Conectarse al Servidor de administración 72
- Mensaje al usuario....78

Estadísticas....89

Exportar
- Directivas....61
- Tareas 68

G

Grupo de aplicaciones con licencia....103

Grupos
Estructura 56

I

Imagen 111
Importación
Directivas 61
Tareas 68
Informes
Claves 155
Creación 88
Envío 88
Ver 88

K

Kaspersky Lab ZAO 171

L

Límite de tráfico 52

M

Menú contextual 31

N

Notificaciones 89

P

Perfil de directiva 61, 62
Perfil de Directiva
Perfil de Directiva
Creación 63
Eliminar 64
Plantilla de informe
Creación 87

R

Rol de usuario
agregar 121
Roles de usuario
rol del usuario
agregar 84
Roles de usuarios 84
rol del usuario
asignar 85

S

Selecciones de eventos
configuración 90
Creación 91
Ver el registro 90
Servidor de administración virtual 40
Servidor de dispositivos móviles Exchange ActiveSync 121
Sondeo
Grupos de Active Directory 96
red de Windows 96
Subredes IP 96
Subredes IP
Cambio 96, 97
Creación 97

T

Tarea
Agregar clave....154
Tareas
Administración de equipos cliente....78
Cambio del Servidor de administración....77
Ejecución....69
Envío de informes....88
Exportar....68
Grupo....65
Importación....68
Local....66
Visualización de los resultados....69
Tareas de grupo
Filtro....70
Herencia....67

V

Vulnerabilidad....104