

The Kaspersky logo is displayed in a bold, lowercase, sans-serif font. It is positioned within a white, rounded rectangular area that is set against a background of teal and green abstract shapes.

kaspersky

Kaspersky Managed Detection and Response

© 2026 AO Kaspersky Lab

Contenido

[Ayuda de Kaspersky Managed Detection and Response](#)

[Novedades](#)

[Acerca de Kaspersky Managed Detection And Response](#)

[Principio de funcionamiento de Kaspersky Managed Detection And Response](#)

[Áreas de responsabilidad](#)

[Requisitos de hardware y software](#)

[Componentes de Kaspersky Managed Detection and Response](#)

[Activar e implementar Kaspersky Managed Detection and Response](#)

[Componentes necesarios para el funcionamiento de MDR](#)

[Integración con las aplicaciones y soluciones de Kaspersky](#)

[Configurar el complemento de MDR](#)

[Activación e implementación de MDR al utilizar versiones actualizadas de las aplicaciones y un solo inquilino](#)

[Activación e implementación de MDR al utilizar versiones actualizadas de las aplicaciones y multiinquilinato](#)

[Activación e implementación de MDR al utilizar versiones heredadas de las aplicaciones](#)

[Implementar un archivo de configuración de KPSN](#)

[Implementar un archivo de configuración de MDR \(BLOB\)](#)

[Despliegue con la captura y copia de la imagen de un dispositivo](#)

[Activar la solución MDR en las aplicaciones de Kaspersky](#)

[Activar la solución MDR en aplicaciones de Kaspersky. Licencias de complementos de Kaspersky MDR](#)

[Activar la solución MDR en aplicaciones de Kaspersky. Licencias de Kaspersky MDR](#)

[Activar la solución MDR en aplicaciones de Kaspersky. Licencias de Kaspersky Symphony MDR, Kaspersky Next Complete Security, Kaspersky Optimum Security y Kaspersky Next MXDR Optimum](#)

[Activar la solución MDR en aplicaciones de Kaspersky. Licencia del complemento para Kaspersky Managed Detection and Response for Industrial CyberSecurity](#)

[Licencias](#)

[Comparación de los niveles de licencias comerciales](#)

[Sobre el código de activación](#)

[Provisión de un nuevo código de activación](#)

[Administrar licencias en Kaspersky Security Center](#)

[Solución de problemas de licencias](#)

[Acerca del Contrato de MDR](#)

[Provisión de datos](#)

[Regiones donde se realiza el procesamiento de datos](#)

[Acerca del Contrato de procesamiento de datos](#)

[Interfaces de Kaspersky Managed Detection And Response](#)

[Sección MDR en Kaspersky Security Center](#)

[Configuración del complemento de MDR en Kaspersky Security Center](#)

[Configurar los derechos de acceso en Kaspersky Security Center](#)

[Ver y editar la configuración de MDR en Kaspersky Security Center](#)

[Usar funciones del complemento MDR en un Servidor de administración virtual](#)

[Usar funciones de MDR en Kaspersky Security Center mediante un servidor proxy](#)

[Cambiar los certificados para usar las funciones de MDR en Kaspersky Security Center con un servidor proxy o software antivirus](#)

[Ocultar y mostrar las funciones de MDR en Kaspersky Security Center](#)

[MDR Web Console](#)

[Cambiar el idioma de la interfaz en Kaspersky Security Center](#)

[Cambiar el idioma de las notificaciones y los informes en Kaspersky Security Center](#)

[Cambiar el idioma de la interfaz en MDR Web Console](#)

[Acerca del archivo de configuración de MDR](#)

[Acerca de Kaspersky Security Network](#)

[Actualización periódica de los archivos de configuración de KPSN](#)

[Hacer que la solución MDR pase a funcionar sin archivos de configuración de KPSN](#)

[Supervisar paneles en MDR Web Console](#)

[Recepción de información resumida](#)

[Recibir un resumen de todos los activos en formato CSV \(MDR Web Console\)](#)

[Recibir información del incidente en un documento PDF \(MDR Web Console\)](#)

[Configurar envío regular de informes en MDR Web Console](#)

[Recepción de notificaciones](#)

[Configurar notificaciones en MDR Web Console](#)

[Notificaciones sobre el estado de los activos](#)

[Recibir notificaciones ampliadas](#)

[Habilitar notificaciones ampliadas en MDR Web Console](#)

[Administrar usuarios](#)

[Invitar a nuevos usuarios en MDR Web Console](#)

[Cambiar las funciones de usuario en MDR Web Console](#)

[Editar métodos de notificación de usuario en MDR Web Console](#)

[Editar el acceso de los usuarios a los inquilinos en MDR Web Console](#)

[Eliminar cuentas de usuario](#)

[Administrar activos](#)

[Ver y buscar activos en MDR Web Console](#)

[Filtrar activos en MDR Web Console](#)

[Ver información detallada sobre activos en MDR Web Console](#)

[Estados de los activos](#)

[Verificar el estado de los activos en Kaspersky Security Center](#)

[Cómo evitar la pérdida de datos de telemetría de los activos](#)

[Administración de incidentes](#)

[Sobre los incidentes](#)

[Ver y buscar incidentes en MDR Web Console](#)

[Filtrar incidentes en MDR Web Console](#)

[Crear incidentes personalizados en MDR Web Console](#)

[Ver información detallada sobre incidentes en MDR Web Console](#)

[Procesar respuestas a incidentes en MDR Web Console](#)

[Tipos de respuesta](#)

[Aceptación automática de respuestas en MDR Web Console](#)

[Aceptación automática de respuestas en Kaspersky Security Center](#)

[Cerrar incidentes en MDR Web Console](#)

[Enviar un incidente al equipo de respuesta a incidentes para una investigación adicional](#)

[Integración de Kaspersky Unified Monitoring and Analysis](#)

[Creación de incidentes de Managed Detection and Response a partir de incidentes de XDR](#)

[Integración de Kaspersky Digital Footprint Intelligence para MDR](#)

[Uso de las funciones de Kaspersky Endpoint Detection and Response Expert](#)

[Respuestas](#)

[Administración de inquilinos](#)

[Gestionar inquilinos en Kaspersky Security Center](#)

[Ver inquilinos en Kaspersky Security Center](#)

[Ver la configuración de inquilinos en Kaspersky Security Center](#)

[Editar la configuración de inquilinos en Kaspersky Security Center](#)

[Añadir nuevos inquilinos en Kaspersky Security Center](#)

[Eliminar inquilinos en Kaspersky Security Center](#)

[Traslado de activos entre inquilinos](#)

[Administrar inquilinos en MDR Web Console](#)

[Ver inquilinos en MDR Web Console](#)

[Ver la configuración de inquilinos en MDR Web Console](#)

[Editar la configuración de inquilinos en MDR Web Console](#)

[Añadir nuevos inquilinos en MDR Web Console](#)

[Eliminar inquilinos en MDR Web Console](#)

[Administrar la solución a través de la API de REST](#)

[Escenario: realizar una autorización basada en token](#)

[Crear una conexión API en Kaspersky Security Center](#)

[Crear una conexión API en MDR Web Console](#)

[Editar una conexión API en Kaspersky Security Center](#)

[Editar una conexión API en MDR Web Console](#)

[Crear un token de acceso en Kaspersky Security Center](#)

[Crear un token de acceso en MDR Web Console](#)

[Trabajar con la API de REST](#)

[Revocar un token de actualización en Kaspersky Security Center](#)

[Eliminar una conexión API en Kaspersky Security Center](#)

[Eliminar una conexión API en MDR Web Console](#)

[Desactivar Kaspersky Managed Detection and Response](#)

[Finalizar el uso de Kaspersky Managed Detection and Response](#)

[Suspender temporalmente el uso de Kaspersky Managed Detection and Response](#)

[Revocar su consentimiento con los términos de uso de la solución MDR](#)

[Problemas conocidos](#)

[Ponerse en contacto con el Soporte técnico](#)

[Cómo obtener soporte técnico](#)

[Soporte técnico a través de Kaspersky CompanyAccount](#)

[Fuentes de información sobre la solución](#)

[Glosario](#)

[Activo](#)

[Aplicación de EPP](#)

[Incidente](#)

[Inquilino](#)

[IOC](#)

[Plataforma de protección de extremos \(EPP\)](#)

[Respuesta](#)

[Táctica MITRE](#)

[Técnica MITRE](#)

[Telemetría](#)

[Información sobre el código de terceros](#)

[Avisos de marcas comerciales](#)

Ayuda de Kaspersky Managed Detection and Response



Funciones nuevas

- [Novedades de la última versión de la solución](#)



Requisitos de hardware y software

- [Compruebe qué sistemas operativos y aplicaciones EPP son compatibles](#)



Comparación de funciones

- [Comparación de soluciones con licencias comerciales: MDR Optimum, MDR Expert, MDR Basic, MDR Advanced y MDR Prime](#)



Primeros pasos

- Implementación local
- Implementación basada en la nube
- [Activación de Kaspersky Managed Detection And Response](#)



Monitoreo y generación de informes

- [Recepción de notificaciones](#)
- [Recibir notificaciones ampliadas](#)
- [Recepción de información resumida](#)
- [Tableros de supervisión](#)



Suministro de datos / Protección de datos personales

- [Provisión de datos](#)
- [Kaspersky Security Network](#)

Novedades

Kaspersky Managed Detection and Response presenta numerosas nuevas funciones y mejoras.

Agosto de 2026

Se lanza el complemento MDR versión 3.1.1 para Open Single Management Platform versión 2.2.

Julio de 2026

- Notificaciones sobre el estado de los activos

MDR ahora admite [el envío automático de notificaciones cuando el estado de sus activos protegidos requiere atención](#). Configure los valores de umbral para los estados de los activos OK, Warning, Critical y Offline, y reciba notificaciones por correo electrónico o Telegram cuando se cumplan las condiciones configuradas. Esto le ayuda a detectar rápidamente problemas de recopilación de telemetría o conectividad sin supervisar continuamente la página Assets.

Junio de 2026

- Integración de Kaspersky DFI para MDR

Nuestro servicio MDR ahora aprovecha la inteligencia de credenciales comprometidas del servicio Kaspersky DFI para mejorar los flujos de trabajo de detección, investigación y búsqueda de amenazas. Mediante la correlación de las credenciales filtradas con los eventos de seguridad y la incorporación de esta inteligencia en las actividades de búsqueda proactiva de amenazas, MDR puede identificar antes posibles compromisos de cuentas, mejorar la priorización de incidentes y ayudar a reducir el riesgo de acceso no autorizado.

Capacidades clave:

- Enriquecimiento de alertas con contexto de credenciales filtradas
 - Correlación de credenciales filtradas con eventos de seguridad
 - Búsqueda de amenazas y detección de compromisos basadas en credenciales
 - Matriz actualizada de compatibilidad de aplicaciones de MDR
- Se ha actualizado la tabla de aplicaciones y soluciones compatibles de Kaspersky. Algunas versiones de productos heredados se han trasladado a la categoría Compatibilidad limitada con MDR (es posible que algunas capacidades de MDR no estén disponibles), mientras que se ha dejado de ofrecer soporte para Kaspersky Endpoint Agent.

Para obtener más información, consulte el [artículo actualizado de la Ayuda en línea](#).

Mayo de 2026

- Se lanza el complemento MDR versión 3.0.2 para Open Single Management Platform versión 2.1.
- Los usuarios ahora pueden dejar comentarios directamente al cerrar un incidente en la Consola de MDR. Esto ayuda a mejorar la calidad del servicio y captar la satisfacción del cliente de manera más eficiente.
- Los administradores de MDR ahora pueden [definir el límite de activos esperado para cada inquilino](#) en la consola de MDR.

Si el número de activos conectados supera el límite configurado, se mostrará una notificación tanto en la lista de inquilinos como en la página de propiedades del inquilino. Esto ayuda a los administradores a supervisar de forma proactiva el alcance de la incorporación y las expectativas de licencias.

Esta funcionalidad se añadirá al complemento MDR en una versión posterior.

- El formato de las notificaciones entregadas por correo electrónico y Telegram se ha mejorado para brindar una mejor legibilidad y un acceso más rápido a la información importante.

La actualización afecta a las notificaciones relacionadas con lo siguiente:

- Incidentes
- Comentarios en comunicación con analistas de MDR
- Acciones de respuesta
- Actualizaciones del estado de la clave de licencia

Marzo de 2026

Se ha añadido compatibilidad con Kaspersky Embedded Systems Security para Linux versión 4.0 o posterior. Ahora puede [activar la solución MDR](#) en Kaspersky Embedded Systems Security para Linux con una licencia de Kaspersky MDR.

Diciembre de 2025

- Se ha añadido compatibilidad con las siguientes aplicaciones EPP:
 - Kaspersky Embedded Systems Security for Windows versión 4.0 o posteriores
 - Kaspersky Industrial CyberSecurity for Nodes Windows, versión 4.5
- Ahora puede configurar [notificaciones ampliadas de Telegram](#) en el complemento MDR, además de en Web Console MDR.
- Puede [enviar incidentes al equipo de respuesta a incidentes para una investigación adicional](#) mediante la interfaz de la consola web de MDR.

- Se ha añadido compatibilidad con las siguientes soluciones de Kaspersky:
 - Integración con Kaspersky Endpoint Detection and Response versión 8.0 o posterior que habilita la siguiente función:
 - [La capacidad de crear incidentes de MDR a partir de incidentes de XDR.](#)
 - Get artefacts [Obtener artefactos.](#)
 - Integración con Kaspersky Anti Targeted Attack versión 8.0 o posterior que añade el [tipo de respuesta](#) Get artefacts.

Consulte el siguiente artículo: [Integración con aplicaciones y soluciones de Kaspersky](#)

Octubre de 2025

Ahora puede configurar [notificaciones ampliadas de Telegram](#) en Web Console MDR.

Julio de 2025

- Se ha añadido la capacidad de usar códigos de activación para activar la solución MDR en las siguientes aplicaciones:
 - Kaspersky Endpoint Security for Linux 12.3
 - Kaspersky Endpoint Security for Linux version 12.3 en modo Light Agent
 - Kaspersky Endpoint Security para Windows versión 12.6 o posteriores
 - Kaspersky Endpoint Security para Windows versión 12.8 o posterior en modo Light Agent
 - Kaspersky Endpoint Security for Mac 12.2

Consulte el siguiente artículo para obtener más detalles: [Activación de la solución MDR en aplicaciones de Kaspersky.](#)
- La solución MDR ahora puede funcionar sin el archivo de configuración de KPSN con las siguientes aplicaciones:
 - Kaspersky Endpoint Security for Linux 12.3
 - Kaspersky Endpoint Security for Linux version 12.3 en modo Light Agent
 - Kaspersky Endpoint Security para Windows versión 12.6 o posteriores
 - Kaspersky Endpoint Security para Windows versión 12.8 o posterior en modo Light Agent
 - Kaspersky Endpoint Security for Mac 12.2

Consulte el siguiente artículo para obtener más detalles: [Hacer que la solución MDR pase a funcionar sin archivos de configuración de KPSN.](#)

- La solución MDR ahora es compatible con [Kaspersky Endpoint Security para Windows versión 12.8 o posterior en modo Light Agent](#) ².
- La versión 2.5.1 del complemento MDR ahora admite el funcionamiento de MDR sin el archivo de configuración de KPSN.
- Kaspersky Endpoint Security for Linux versión 12.3 ahora admite las siguientes acciones de respuesta:
 - Aislar
 - Desactivar el aislamiento
 - Poner en cuarentena el archivo
 - Restaurar archivo almacenado en cuarentena
 - Terminar proceso
 - Ejecutar proceso

Mayo de 2025

- En la sección [Licencias](#) del complemento MDR para Kaspersky Security Center:
 - Para cada licencia MDR, ahora se muestra el nombre del cliente al que se emite la licencia.
 - Ya está disponible la matriz de utilización de licencias específicas en los inquilinos.
- En la sección [Inquilinos](#) del complemento MDR para Kaspersky Security Center:
 - Al crear un archivo de configuración MDR para una licencia específica, ahora se muestra el nombre del cliente para el cual se emite la licencia.
 - La lista de inquilinos ahora muestra el inquilino raíz, que se crea de forma predeterminada después de activar el cliente. Puede descargar archivos de configuración para todas las licencias vigentes del inquilino raíz.

Febrero de 2025

- Web Console MDR ahora incluye la sección **Licensing**. La siguiente funcionalidad está disponible:
 - Ver las licencias MDR vigentes, no usadas y caducadas.
 - Ver el número total de activos y su límite para cada licencia.
 - Descargar un archivo de configuración de MDR para el inquilino root:
 Utilice la [sección Inquilinos](#) para crear y descargar archivos de configuración MDR para otros inquilinos.

- Introducir un nuevo código de activación de licencia.
Si su organización tiene varias licencias, sólo puede administrarlas en el complemento de MDR para Kaspersky Security Center. La sección **Licensing** en Web Console MDR pasa a ser de solo lectura.
- Kaspersky Security Center ahora permite usar el complemento MDR para [aplicar múltiples licencias](#) en su organización. La siguiente funcionalidad está disponible:
 - Ver las licencias MDR vigentes, no usadas y caducadas.
 - Eliminar una licencia de MDR vigente.
 - Introducir un nuevo código de activación.
 - Descargar el archivo de configuración de MDR para una licencia.
 - Elegir una licencia para un archivo de configuración MDR al crear o editar un inquilino en la [sección Inquilinos](#).

Diciembre de 2024

- Se ha simplificado la activación de Kaspersky Managed Detection and Response en dispositivos Kaspersky Endpoint Security for Windows (a partir de la versión 12.4). Todo lo que necesita es una licencia estándar para la solución Kaspersky MDR.
Tenga en cuenta que aún necesitará utilizar el archivo de configuración MDR (BLOB) en cualquiera de los siguientes casos:
 - Si tiene más de un inquilino.
 - Si está utilizando la solución MDR junto con Kaspersky Endpoint Detection and Response Optimum.
- Ahora se puede administrar la solución MDR en Kaspersky Security Center Linux (a partir de la versión 15.1).
- Se ha añadido a la Ayuda [información detallada sobre los requisitos del canal de comunicación](#).

Octubre de 2024

Se ha lanzado la versión 2.4.1 del complemento de MDR para Kaspersky Security Center. Contiene las siguientes mejoras:

- Se ha añadido la capacidad de configurar la aceptación automática de acciones de respuesta en el complemento MDR para Kaspersky Security Center.
- Se ha mejorado la funcionalidad e interfaz de usuario de la [sección que proporciona la lista de activos inactivos](#). Dichos activos se han añadido a Kaspersky Security Center, tienen el componente MDR instalado, pero nunca se han enviado telemetría a Kaspersky Managed Detection and Response. Puede filtrar los activos por estado MDR, ver la información detallada sobre cada activo y exportar la lista de activos a un archivo CSV.

Esta función funciona correctamente en Kaspersky Security Center 15.1 Windows o versiones posteriores, Kaspersky Security Center 15.1 Linux o versiones posteriores, y Kaspersky Next Expert View.

- Solo en MDR Web Console: ahora se puede crear [una tarea para la entrega regular de un informe sobre incidentes abiertos](#). Esta función se ha eliminado de la sección MDR en Kaspersky Security Center.

Julio de 2024

MDR Web Console ahora le permite configurar la aceptación automática de acciones de respuesta para los inquilinos seleccionados.

Junio de 2024

- Ahora están disponibles nuevas [acciones de respuesta](#):
 - Poner archivo en cuarentena
 - Restaurar archivo almacenado en cuarentena
 - Ejecutar un script en un activo
- [Documentación de la API REST](#) actualizada, se incluyen nuevos ejemplos de scripts.
- Hemos introducido grandes cambios en el diseño de los [informes](#):
 - Mapeo MITRE ATT&CK para realizar análisis de amenazas en profundidad.
 - Listado de los ordenadores atacados con mayor frecuencia, para ayudar a los clientes a enfocarse en los riesgos críticos.

- Soporte para multiinquilinos:
 - Genere informes y [configure un cronograma de informes resumidos](#) para inquilinos específicos.
 - Cambie, sin ningún inconveniente, de widgets a estadísticas específicas del inquilino en el [panel de monitoreo](#).
 - Configure la confirmación automática de la ejecución de la tarea de respuesta para inquilinos específicos.
 - API mejorada de MDR para la gestión de inquilinos.

Diciembre de 2023

- MDR Web Console ahora contiene el panel **Telemetry statistics**, que muestra la cantidad de eventos, alertas e incidentes de telemetría.
- Kaspersky Managed Detection and Response ahora es compatible con Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent (EDR Agent) (con [limitaciones](#)).

Noviembre de 2023

- Visualización mejorada de los estados de los activos en MDR Web Console y en el complemento de MDR para Kaspersky Security Center: el [estado del activo](#) ahora muestra la operatividad de los componentes de la aplicación EPP del activo, el estado de actualización de la base de datos antivirus del activo y el estado de transmisión de telemetría.
- El estado de los activos ahora muestra la presencia de pérdidas de telemetría de los activos, lo que le permite identificar los activos con problemas de entrega de telemetría. Esta función está activada de forma predeterminada para los nuevos clientes y se irá activando de manera gradual para los clientes existentes.

Octubre de 2023

Se ha añadido una nueva región de residencia del cliente: **Arabia Saudí**, para los clientes que almacenan datos de telemetría en el Reino de Arabia Saudí.

Septiembre de 2023

Se ha lanzado la versión 2.3.1 del complemento de MDR para Kaspersky Security Center. En esta versión, las funciones de administración de incidentes se han eliminado de la sección MDR en Kaspersky Security Center. Puede gestionar incidentes en [MDR Web Console](#).

Julio de 2023

Se ha lanzado la versión 2.3.0 del complemento de MDR para Kaspersky Security Center. Contiene las siguientes mejoras:

- Ahora puede configurar notificaciones ampliadas en el complemento de MDR.
- Ahora puede usar las funciones de MDR en Kaspersky Security Center con el complemento de MDR mediante un servidor proxy.
- Ahora puede cambiar los certificados para usar las funciones de MDR en Kaspersky Security Center con un servidor proxy o con software antivirus.

Julio de 2022

Se ha lanzado la versión 2.1.17 del complemento de MDR. Esta versión del complemento es compatible con la versión 14 o posterior de Kaspersky Security Center.

Mayo de 2022

Mejoras generales:

- Se ha añadido una nueva región de residencia del cliente: **EE. UU./Canadá**. Los datos de telemetría de los clientes de esta región se almacenan en el norte de Europa.
- Se ha modificado la descripción del proceso de implementación de MDR en la ayuda.

Mejoras en el complemento de MDR:

- En la sección **Configuración** ahora se puede cambiar el idioma de las notificaciones en Telegram y correo electrónico, y de la comunicación en el chat de incidencias.
- Se ha mejorado la interfaz para trabajar con imágenes y tablas en las tarjetas de incidentes.
- MDR Expert. En la sección **Uso del servicio** se puede comprobar cuántas incidencias se pueden crear según el SLA.

Corrección de errores y otras mejoras:

- La búsqueda en las listas de incidentes y activos ahora se realiza mediante si la subcadena buscada aparece completa en cualquier parte de la cadena.
- En Kaspersky Endpoint Security for Mac versión 11.2 o posterior, después de introducir el código de activación de MDR y añadir el archivo de configuración de KPSN, ya no necesita reiniciar su dispositivo Mac para iniciar la transferencia de telemetría.
- Al calcular las licencias para máquinas virtuales con Kaspersky Security for Virtualization Light Agent versión 5.2 o posterior, no se incluyen los activos que no han transferido telemetría durante más de 24 horas.

Marzo de 2022

Los usuarios de [MDR Optimum](#) ahora pueden charlar con los analistas de Kaspersky SOC sobre un incidente (con la siguiente limitación: las solicitudes se procesan solo en relación con un incidente en particular y no se aplica ningún SLA).

Octubre de 2021

- El complemento Kaspersky Managed Detection and Response para Kaspersky Security Center Web Console y Kaspersky Next Expert View se ha actualizado con la [función mejorada de estados de activos de MDR](#):
 - Interfaz mejorada de estados de activos de MDR.
 - La lista de activos muestra todos los activos de todos los estados, que anteriormente solo estaban disponibles en MDR Web Console.
 - Se han añadido opciones de filtrado y ordenación para trabajar con la lista de activos.

Julio de 2021

- Compatibilidad con Kaspersky Managed Detection and Response en Kaspersky Next Expert View, que permite administrar la solución en la consola de administración única de Kaspersky Security Center. Las siguientes funciones están disponibles con la solución Kaspersky Managed Detection and Response:

- [Trabajar con incidentes:](#)

- Ver, crear y comentar incidentes
- Ponerse en contacto con Kaspersky Security Operation Center sobre un incidente, aceptar o rechazar las respuestas sugeridas por los analistas de SOC

- [Responder a un incidente mediante Kaspersky Endpoint Detection and Response](#)

Las siguientes funciones están disponibles:

- Aplicar aislamiento de la red de los dispositivos
- Crear reglas de bloqueo por hash
- Crear tareas para eliminar, poner en cuarentena, finalizar el proceso y buscar por indicadores de compromiso (IOC) relacionados con un incidente
- [Supervisar los eventos de Kaspersky Managed Detection and Response en los tableros](#) de la consola de supervisión de Kaspersky Security Center Web Console
- [Configurar notificaciones](#) sobre eventos de Kaspersky Managed Detection and Response por correo electrónico y Telegram
- [Configurar la programación del resumen del rendimiento del MDR](#) enviado por correo electrónico
- [Visualizar dispositivos en los que hay problemas](#) en el rendimiento de MDR
- [Nuevo asistente de activación](#), que permite conectar el MDR en Kaspersky Security Center Web Console
- [Configuración automática de KPSN](#), que ya no requiere la descarga y carga manual del archivo de configuración en la configuración de Kaspersky Security Center
- [Gestionar conexiones a la API MDR pública](#): visualizar, crear, editar y eliminar tokens
- [Gestionar los inquilinos de la organización, incluida su creación](#)
- Obtener información sobre el número de incidentes que puede registrar un usuario. Estos incidentes se manejan según los términos del acuerdo de nivel de servicio (SLA).

Estas funciones también están disponibles en Kaspersky Security Center Web Console.

- Se ha añadido a MDR Web Console la administración de varias cuentas de administrador de MDR: ahora puede crear cuentas y administrar privilegios

- Las nuevas versiones de las aplicaciones compatibles ya no requieren la instalación adicional de Kaspersky Endpoint Agent. La funcionalidad integrada de Kaspersky Managed Detection and Response es compatible con las siguientes aplicaciones de EPP:
 - Kaspersky Endpoint Security para Windows versión 11.6 o posterior
 - Kaspersky Endpoint Security para Mac 11.2
 - Kaspersky Endpoint Security para Linux 11.2
 - Kaspersky Security para Virtualization 5.2 Light Agent

Para obtener detalles sobre diferentes situaciones de implementación, consulte [Implementación de Kaspersky Managed Detection and Response](#).

- Se agregó el filtrado por tipo de evento para Kaspersky Endpoint Security para Windows y para Linux con la funcionalidad incorporada de Kaspersky Managed Detection and Response, que permite disminuir la carga en los canales y reducir el consumo de tráfico al enviar datos por telemetría.
- Se encuentran disponibles los siguientes tipos de respuesta: [obtener el archivo del dispositivo, aislar el dispositivo, deshabilitar el aislamiento del dispositivo, eliminar la clave de registro](#), finalizar el proceso.
Es posible realizar estas acciones con la confirmación del usuario que tiene la función de administrador de MDR.
- Compatibilidad con las siguientes nuevas localizaciones en el complemento web para Kaspersky Security Center Web Console y Kaspersky Next Expert View: francés, alemán, italiano y español.

Marzo de 2021

El nuevo complemento web para Kaspersky Security Center Web Console permite utilizar las siguientes funciones de Kaspersky Managed Detection and Response:

- Ver incidentes
- Creación de incidentes
- Añadir comentarios a los incidentes
- Ponerse en contacto con Kaspersky Security Operation Center sobre un incidente
- Aceptación o rechazo de respuestas sugeridas por analistas de SOC
- Posibilidad de dar una respuesta independiente a un incidente:
 - Aislar los activos de la red
 - Crear reglas de bloqueo por hash
 - Crear tareas para la eliminación, puesta en cuarentena, finalización del proceso y búsqueda por indicadores de compromiso (IOC) relacionados con un incidente
- Supervisar los eventos de Kaspersky Managed Detection and Response en los tableros de la consola de supervisión de Kaspersky Security Center Web Console

- Configuración de notificaciones de correo electrónico y Telegram sobre eventos de Kaspersky Managed Detection and Response
- Configurar la programación de envío de resúmenes de incidentes por correo electrónico

Acerca de Kaspersky Managed Detection And Response

Kaspersky Managed Detection and Response es una solución que detecta y analiza automáticamente los incidentes de seguridad en su infraestructura mediante el uso de telemetría y tecnologías avanzadas de aprendizaje automático, y después transfiere información sobre el incidente a los expertos de Kaspersky. Luego, los expertos pueden procesar el incidente o dar recomendaciones sobre cómo procesarlo.

Kaspersky Managed Detection and Response (también denominado MDR) ofrece protección las 24 horas contra el creciente volumen de amenazas que eluden las barreras de seguridad automatizadas de las organizaciones que no tienen la suficiente experiencia y personal, o para aquellas cuyos recursos internos son limitados. La solución ayuda a mejorar la resiliencia de su empresa a las ciberamenazas, al tiempo que libera sus recursos existentes para que centren su atención en otras tareas.

A diferencia de ofertas similares en el mercado, este servicio tiene un historial comprobado de investigación de ataques selectivos, que aprovecha para garantizar una defensa constante, incluso contra las amenazas más complejas.

La solución Kaspersky Managed Detection and Response (MDR) no está disponible en los Estados Unidos ni para ciudadanos estadounidenses. El uso de la solución MDR en el territorio especificado o por parte de ciudadanos estadounidenses es una violación de los [términos de uso de la solución MDR](#). Para no infringir los términos de uso de la solución MDR, es necesario [finalizar el uso de MDR de forma permanente](#) en todos los activos ubicados en el territorio especificado, o en aquellos utilizados por ciudadanos estadounidenses. Los ciudadanos no estadounidenses que se encuentren temporalmente en los Estados Unidos, deben [suspender el uso de MDR](#) en sus activos.

Principio de funcionamiento de Kaspersky Managed Detection And Response

Kaspersky Managed Detection and Response analiza los datos de telemetría de las aplicaciones EPP y genera eventos de seguridad que la tecnología de detección puede clasificar como incidentes generales.

Kaspersky Managed Detection and Response recibe datos de las aplicaciones EPP que admiten MDR, procesa los datos para después enviarlos a través de [Kaspersky Security Network](#) a Kaspersky Managed Detection and Response. Para obtener la lista de datos que se procesan, consulte [Provisión de datos](#). Las aplicaciones de EPP se instalan en dispositivos de extremos dentro de la infraestructura de TI de una organización (por ejemplo, dispositivos móviles, ordenadores o portátiles). Ejemplo de una aplicación EPP es Kaspersky Endpoint Security para Windows.

MDR Web Console se utiliza para procesar incidentes. Como alternativa, puede integrar Kaspersky Managed Detection and Response con una solución de terceros, como se describe en el artículo [Administración de la solución a través de la API de REST](#).

Kaspersky Managed Detection and Response puede resolver un incidente de forma automática o solicitar la intervención del usuario ante una posible amenaza de seguridad. Consulte el artículo [Tipos de respuesta](#) para obtener más detalles. Para garantizar una respuesta rápida a posibles amenazas de seguridad, la solución Kaspersky Managed Detection and Response puede solicitarle una aclaración sobre un evento sospechoso. Debe procesar dichas solicitudes a tiempo.

La investigación detallada de incidentes (como la identificación de los eventos previos, las circunstancias y el mecanismo del ataque) está a cargo del componente Kaspersky Incident Response, que no forma parte de Kaspersky Managed Detection and Response y requiere comprarlo por separado

El uso de Kaspersky Managed Detection and Response implica que los usuarios procesen los incidentes con la ayuda de los expertos de Kaspersky. Para obtener más información, consulte el artículo: [Áreas de responsabilidad](#).

Áreas de responsabilidad

El uso de Kaspersky Managed Detection and Response implica que los usuarios procesen los incidentes con el apoyo de la solución MDR. Además, el soporte técnico de Kaspersky se encarga de los problemas relacionados con el producto.

La siguiente tabla muestra las áreas de responsabilidad de los usuarios, la solución MDR y el soporte técnico de Kaspersky.

Tarea	La solución MDR	Soporte técnico de Kaspersky	Usuarios de MDR
Activar MDR, desplegar MDR, administrar activos, configurar notificaciones, administrar usuarios, finalizar el uso de MDR	–	Responder a consultas	Realizar la tarea
Usar la consola web para gestionar incidentes	–	Responder a consultas	Realizar la tarea
Detectar, investigar y emitir recomendaciones de respuesta ante incidentes basados en datos de telemetría .	Realizar la tarea	–	Recibir información
Aclarar detalles durante la investigación y responder preguntas de la solución MDR para ofrecer mejores recomendaciones de respuesta	Recibir información	–	Realizar la tarea
Crear solicitudes para utilizar las herramientas y capacidades de MDR para gestionar incidentes.	Realizar la tarea	–	Recibir información
Coordinar solicitudes para utilizar las herramientas y capacidades de MDR para gestionar incidentes.	Recibir información	–	Realizar la tarea
Realizar tareas que estén fuera de las capacidades funcionales del MDR	Responder a consultas	–	Realizar la tarea
Creación manual de un incidente (es importante elegir un activo MDR y describir el incidente en detalle)	Recibir información	–	Realizar la tarea
Gestionar problemas de los componentes de infraestructura de Kaspersky que afectan a MDR	Recibir información	Responder a consultas	Realizar la tarea
Administrar reglas de detección	Realizar la tarea	–	–

Requisitos de hardware y software

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Aplicaciones de EPP requeridas y configuraciones compatibles

Para utilizar Kaspersky Managed Detection and Response, se debe implementar al menos una de las siguientes aplicaciones de EPP en su infraestructura:

- Portátiles, equipos de escritorio, tabletas y servidores
 - [Kaspersky Endpoint Security para Windows](#) [↗]
 - [Kaspersky Endpoint Security para Linux](#) [↗]
 - [Kaspersky Endpoint Security para Mac](#) [↗]
- Endpoints industriales
 - [Kaspersky Industrial CyberSecurity for Nodes Windows](#) [↗]
- Sistemas virtuales
 - [Kaspersky Security para Virtualization Light Agent](#) [↗]
- Sistemas integrados
 - [Kaspersky Embedded Systems Security para Windows](#) [↗]
 - [Kaspersky Embedded Systems Security para Linux](#) [↗]
- Supervisión de eventos de red
 - [Plataforma Kaspersky Anti Targeted Attack](#) [↗]

Sistemas operativos

Kaspersky Managed Detection and Response es compatible con los mismos sistemas operativos que las aplicaciones de EPP enumeradas a continuación. Para obtener más información, consulte la sección *Requisitos de hardware y software* en la documentación de las aplicaciones EPP compatibles enumeradas en la siguiente tabla.

Aplicaciones y soluciones de Kaspersky compatibles

Kaspersky Managed Detection and Response es compatible con las versiones de las aplicaciones de Kaspersky enumeradas en la siguiente tabla.

Aplicación de Kaspersky	Versiones recomendadas y su periodo de soporte	Compatibilidad limitada con MDR *	Notas
Kaspersky Endpoint Security para Windows	12.10 o posteriores 	12.6–12.9 	Kaspersky Endpoint Security para Windows versión 12.6–12.9 admite la activación de la solución MDR con un código de activación. Kaspersky Endpoint Security para Windows versión 12.10 o posterior también admite la activación de la solución MDR con un archivo de clave.
Kaspersky Endpoint Security para Windows en modo Light Agent	12.9 o posteriores 	12.8 	Kaspersky Endpoint Security para Windows versión 12.6–12.9 en el modo Light Agent admite la activación de la solución MDR con un código de activación. Kaspersky Endpoint Security para Windows versión 12.10 o posterior en el modo Light Agent también admite la activación de la solución MDR con un archivo de clave.
Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent (EDR Agent) A partir de la versión 12.3 de Kaspersky Endpoint Security para Windows, la aplicación incluye la configuración de Endpoint Detection and Response Agent (EDR Agent). Endpoint Detection and Response Agent es una aplicación que se instala en estaciones de trabajo individuales y servidores en la infraestructura de TI de la organización para ofrecer soporte a las soluciones Kaspersky Managed Detection and Response y Kaspersky Anti Targeted Attack Platform (EDR). EDR Agent supervisa en todo momento los procesos que se ejecutan en estos equipos, las conexiones de red abiertas y los archivos que se modifican. Los componentes de protección y control no están disponibles para EDR Agent. EDR Agent es compatible con aplicaciones EPP de terceros  . Esto le permite usar herramientas de seguridad de infraestructura de terceros junto con Detection and Response de Kaspersky. Para obtener más detalles, consulte la Ayuda en línea de Kaspersky Endpoint Security para Windows  .	12.8 o posteriores 	12.6–12.7 	- Para los activos con Kaspersky Endpoint Security para Windows en la configuración de EDR Agent, los estados <i>Advertencia</i> y <i>Crítico</i> para los componentes de protección y control no se muestran. - No puede usar las funciones de Kaspersky Endpoint Detection and Response Optimum para los activos con Kaspersky Endpoint Security para Windows en la configuración de EDR Agent. - La lista de aplicaciones EPP de terceros que son compatibles con EDR Agent se proporciona en la ayuda en línea de Kaspersky Endpoint Security para Windows . Kaspersky Endpoint Security para Windows versión 12.6–12.9 en la configuración de Endpoint Detection and Response Agent (EDR Agent) admite la activación de la solución MDR con un código de activación. Kaspersky Endpoint Security para Windows versión 12.10 o posterior en la configuración de Endpoint Detection and Response Agent (EDR Agent) también admite la activación de la solución MDR con un archivo clave.
Kaspersky Endpoint Security for Linux	12.4 o posteriores 	12.1–12.3 	Si utiliza Kaspersky Endpoint Security para Linux y no tiene instalado el paquete Linux Audit Daemon (también conocido como auditd), los eventos de auditoría del sistema se registran en el registro del kernel (dmesg). Recomendamos instalar el paquete auditd, porque es conveniente para administrar la rotación de registros de Kaspersky Endpoint Security for Linux. Kaspersky Endpoint Security for Linux versión 12.3 o posterior admite la activación de la solución MDR con un archivo clave y un código de activación.

Aplicación de Kaspersky	Versiones recomendadas y su periodo de soporte	Compatibilidad limitada con MDR *	Notas
Kaspersky Endpoint Security for Linux en el modo Light Agent	12.4 o posteriores 	12.1-12.3 	Kaspersky Endpoint Security for Linux versión 12.3 o posterior en el modo Light Agent admite la activación de la solución MDR con un archivo clave y un código de activación.
Kaspersky Endpoint Security para Mac	12.2 o posteriores 	12-12.1 	Kaspersky Endpoint Security for Mac admite la activación de la solución MDR con un código de activación.
Kaspersky Security para Virtualization Light Agent	6.3 o posteriores 	5.2-6.2 	Consulte el siguiente artículo para obtener detalles: Versiones compatibles de aplicaciones en modo Light Agent .
Kaspersky Embedded Systems Security para Windows	4.0 o posteriores 	4.0 	Kaspersky Endpoint Security para Windows versión 12.3 o posterior admite la activación de la solución MDR mediante un archivo clave o un código de activación.
Kaspersky Embedded Systems Security para Linux	4.0 o posteriores 	4.0 	Kaspersky Embedded Systems Security for Linux admite la activación de la solución MDR mediante un archivo clave o un código de activación.
Kaspersky Industrial CyberSecurity for Nodes Windows	4.5 	4.5 	Use la versión 3.0.0 o posteriores del complemento MDR a fin de aplicar varios códigos de activación para la licencia de Kaspersky Industrial CyberSecurity for Nodes. Puede usar Web Console MDR si solo tiene un código de activación para la licencia de Kaspersky Industrial CyberSecurity for Nodes. La aplicación de nuevos códigos de activación para Kaspersky Industrial CyberSecurity for Nodes no está disponible en la región del Reino de Arabia Saudí, si tiene alguna de las siguientes licencias: • Kaspersky Managed Detection and Response Basic Add-on • Kaspersky Managed Detection and Response Advanced Add-on • Kaspersky Managed Detection and Response Prime Add-on
Kaspersky Endpoint Agent	-	4.0 o posteriores 	Le recomendamos que cambie a Kaspersky Endpoint Security para Windows. Kaspersky Endpoint Agent solo se usa si usted utiliza Kaspersky Security for Windows Server.

* La integración de MDR está disponible con ciertas limitaciones funcionales (por ejemplo, telemetría reducida o menos acciones de respuesta automatizadas).

Para obtener más información sobre las versiones compatibles de las aplicaciones y soluciones de Kaspersky, consulte la [página web Ciclo de vida del soporte técnico](#) .

Consulte el siguiente artículo para obtener detalles sobre la integración con otras soluciones de Kaspersky: [Integración con aplicaciones y soluciones de Kaspersky](#).

Kaspersky Security Center

La siguiente tabla enumera los componentes de Kaspersky Security Center compatibles con la solución MDR.

Componentes de Kaspersky Security Center	Versiones y su periodo de soporte	Notas
Kaspersky Security Center Windows	15.1 o posteriores 	Se utilizaron con el Complemento de MDR para Kaspersky Security Center .
Kaspersky Security Center Linux	15.1 o posteriores 	Se utilizaron con el Complemento de MDR para Kaspersky Security Center .
Kaspersky Next Expert View	Expert View	
Complemento de MDR para Kaspersky Security Center	Última versión	La versión 2.5.1 es la versión mínima admitida.

MDR Web Console

MDR Web Console tiene los siguientes requisitos de hardware y software:

- Monitor con resolución de pantalla de 1024 x 768 o superior
- Cualquiera de los siguientes navegadores:
 - Apple Safari 18.3 o versiones posteriores en macOS
 - Google Chrome 143.0.7499.40 o versiones posteriores (compilación oficial)
 - Microsoft Edge 143.0.3650.66 o versiones posteriores
 - Mozilla Firefox Extended Support Release 140.5.0.2342 o versiones posteriores

Canal de red

La siguiente tabla muestra la capacidad de transmisión del canal de red, calculado a partir de nuestros datos estadísticos.

Sistema operativo	Ancho de banda estimado para 1000 activos
Windows	4.3 Mbit/s
Servidor Windows	5,2 Mbit/s
Linux (promedio para hosts y servidores)	14,7 Mbit/s
macOS	8,5 Mbit/s

Estos valores de ancho de banda son aproximados, ya que el ancho de banda necesario depende en gran medida del tipo de carga del activo que genera eventos de telemetría. El rendimiento máximo puede ser mucho mayor. Deberá disponer de un mayor ancho de banda de red si su infraestructura opera a su máxima capacidad con frecuencia. Hay varias situaciones en las que la carga puede mayor. Por ejemplo:

- los desarrolladores están compilando código de software
- se está realizando un análisis completo del sistema

- en la red hay servidores de alta carga (por ejemplo, DNS y controladores de dominio)
- existen múltiples conexiones de red

Funciones de las versiones del complemento MDR y compatibilidad con Kaspersky Security Center y Open Single Management Platform

En la siguiente tabla se muestran las versiones de Kaspersky Security Center y Open Single Management Platform compatibles con las versiones del complemento MDR.

Funciones de las versiones del complemento MDR y compatibilidad con Kaspersky Security Center

Versión del complemento MDR	Versión compatible de Kaspersky Security Center	Funciones añadidas en la versión del complemento MDR
2.5.1	Kaspersky Security Center Windows, versión 15.1 o posterior Kaspersky Security Center Windows/Linux, versión 16.1 o posterior	Uso de varias claves de licencia. La capacidad de generar un archivo de configuración de MDR (BLOB) para una clave de licencia específica. Configuración de acciones de respuesta automática para inquilinos. Informes configurables específicos de inquilino.
2.5.2	Kaspersky Security Center Windows, versión 15.1 o posterior Kaspersky Security Center Windows/Linux, versión 16.1 o posterior	Funcionamiento sin archivos de configuración de KPSN.
3.0.0	Kaspersky Security Center Windows, versión 15.1 o posterior Kaspersky Security Center Windows/Linux, versión 16.1 o posterior	Compatibilidad con las siguientes aplicaciones EPP: • Kaspersky Industrial CyberSecurity for Nodes Windows versión 4.5 o posteriores • Kaspersky Embedded Systems Security for Windows versión 4.0 o posteriores
3.1.0	Kaspersky Security Center Windows, versión 15.1 o posterior Kaspersky Security Center Windows/Linux, versión 16.1 o posterior	Compatibilidad con las siguientes aplicaciones EPP: Kaspersky Embedded Systems Security for Linux versión 4.0 o posteriores La capacidad de especificar el límite de activos para inquilinos. A partir de la versión 3.1.0 del complemento MDR, las notificaciones ya no se pueden configurar en Kaspersky Security Center. Utilice la Web Console MDR para configurar las notificaciones.

Compatibilidad de versiones del complemento MDR con Open Single Management Platform

Versión del complemento MDR	Versión de Open Single Management Platform compatible	Funciones añadidas en la versión del complemento MDR
3.0.1	2.0	Integración con Kaspersky Endpoint Detection and Response Expert: • Creación de incidentes MDR a partir de incidentes EDR. • La acción de respuesta Get artefacts, que permite copiar archivos relacionados con alertas o incidentes de Kaspersky EDR a Kaspersky SOC. La compatibilidad con Open Single Management Platform versión 2.0 está limitada a la versión 3.0.1 del complemento MDR.
3.0.2	2.1	Integración de MDR con Open Single Management Platform versión 2.1.
3.1.0	2.1	Compatibilidad con las siguientes aplicaciones EPP: Kaspersky Embedded Systems Security for Linux versión 4.0 o posteriores La capacidad de especificar el límite de activos para inquilinos. A partir de la versión 3.1.0 del complemento MDR, las notificaciones ya no se pueden configurar en Open Single Management Platform. Utilice la Web Console MDR para configurar las notificaciones.
3.1.1	2.2	Integración de MDR con Open Single Management Platform versión 2.2.

Componentes de Kaspersky Managed Detection and Response

Descripción de Kaspersky Managed Detection And Response:

- Un [activo](#) es un dispositivo de una organización que está protegido por las soluciones de Kaspersky.
- Endpoint Protection Platform (EPP) es una aplicación de Kaspersky que protege los dispositivos y los datos almacenados en ellos frente al malware y otras amenazas.
- Kaspersky Endpoint Agent es un componente del programa que se instala en estaciones de trabajo y servidores de la infraestructura de TI corporativa. Kaspersky Endpoint Agent supervisa en todo momento los procesos que se ejecutan en esos equipos, las conexiones de red activas y los archivos que se modifican. En versiones recientes de aplicaciones de la EPP, fue reemplazado por la funcionalidad incorporada.
- Kaspersky Network Agent es un componente de Kaspersky Security Center que permite la interacción entre el servidor de administración y las aplicaciones de Kaspersky que están instaladas en un nodo de red específico (estación de trabajo o servidor). Este componente es común a todas las aplicaciones de la empresa para Microsoft Windows. Existen versiones del Agente de red para las aplicaciones de Kaspersky desarrolladas para sistemas operativos tipo Unix y macOS.
- Kaspersky Security Center es una aplicación para administradores de redes corporativas y empleados responsables de la protección de dispositivos en una amplia gama de organizaciones.
- Kaspersky Security Network es una infraestructura de servicios en la nube que brinda acceso a la base de conocimientos en línea de Kaspersky, que contiene información sobre la reputación de archivos, recursos web y software. El uso de datos de Kaspersky Security Network garantiza que las aplicaciones de Kaspersky den una respuesta más rápida a las amenazas, mejora el rendimiento de algunos componentes de protección y reduce la probabilidad de falsas alarmas.
- Kaspersky Managed Detection and Response (también conocido como MDR) es una solución que brinda protección administrada continua, lo que permite a las organizaciones buscar automáticamente las amenazas evasivas, al tiempo que libera a los equipos de seguridad de TI para que se concentren en las tareas críticas que requieren su participación.
- MDR Web Console proporciona una interfaz web para administrar y mantener el sistema de protección de la red de una organización cliente administrada por Kaspersky Managed Detection and Response. A las funciones de la MDR Web Console se suma el complemento web de Kaspersky Security Center, que le permite administrar Kaspersky Managed Detection and Response desde una sola consola de administración.
- El API de MDR es la interfaz de programación de aplicaciones para administrar y respaldar el sistema de protección de red de una organización cliente administrada por Kaspersky Managed Detection and Response.

Activar e implementar Kaspersky Managed Detection and Response

En esta sección se describe cómo activar e implementar Kaspersky Managed Detection and Response.

Para activar e implementar Kaspersky Managed Detection and Response, necesita una de las siguientes soluciones para la administración centralizada de la seguridad de la red:

- Local: [Kaspersky Security Center Web Console](#) ², [Open Single Management Platform](#) ².
- Basada en la nube: [Kaspersky Next Expert View](#) ².

Los pasos para implementar Kaspersky Managed Detection and Response dependen de las [aplicaciones EPP](#) ² específicas que estén instaladas en sus activos y del uso del [multiinquilinato](#).

Versiones actualizadas de las aplicaciones, un solo inquilino

[Active e implemente MDR utilizando solo aplicaciones actualizadas y un único inquilino](#) si se cumplen las siguientes condiciones:

- Hay versiones actualizadas de las aplicaciones instaladas en todos sus activos:
 - Kaspersky Endpoint Security para Windows versión 12.10 o posteriores
 - Kaspersky Endpoint Security for Linux versión 12.3 o posteriores
 - Kaspersky Endpoint Security for Mac versión 12.2 o posteriores
 - Kaspersky Industrial CyberSecurity for Nodes Windows versión 4.5 o posteriores
 - Kaspersky Embedded Systems Security for Windows versión 4.0 o posteriores
 - Kaspersky Embedded Systems Security for Linux versión 4.0 o posteriores
- No tiene previsto configurar el multiinquilinato inmediatamente después de la implementación. Puede configurar el multiinquilinato más adelante.
- Dispone de alguna de las siguientes licencias:
 - Kaspersky NEXT Complete Security
 - Kaspersky Optimum Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum

- Kaspersky MDR
- Kaspersky Managed Detection and Response

Versiones actualizadas de las aplicaciones, multiinquilinato

Active e implemente MDR utilizando únicamente aplicaciones actualizadas y multiinquilinato si se cumplen las siguientes condiciones:

- Hay versiones actualizadas de las aplicaciones instaladas en todos sus activos:
 - Kaspersky Endpoint Security para Windows versión 12.10 o posteriores
 - Kaspersky Endpoint Security for Linux versión 12.3 o posteriores
 - Kaspersky Endpoint Security for Mac versión 12.2 o posteriores
 - Kaspersky Industrial CyberSecurity for Nodes Windows versión 4.5 o posteriores
- Tiene previsto configurar el multiinquilinato inmediatamente después de la implementación.
- Dispone de alguna de las siguientes licencias:
 - Kaspersky NEXT Complete Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum
 - Kaspersky MDR
 - Kaspersky Managed Detection and Response
 - Kaspersky MDR Expert Add-on
 - Kaspersky MDR Optimum Add-on
 - Kaspersky Managed Detection and Response Basic Add-on
 - Kaspersky Managed Detection and Response Advanced Add-on
 - Kaspersky Managed Detection and Response Prime Add-on

Versiones heredadas de las aplicaciones

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Active e implemente MDR si su infraestructura incluye activos con versiones heredadas de aplicaciones:

- Kaspersky Endpoint Security para Windows 12.9 y versiones anteriores
- Kaspersky Endpoint Security para Linux versión 12.2 y anteriores
- Kaspersky Endpoint Security for Mac versión 12.1 y anteriores
- Kaspersky Security for Virtualization Light Agent versión 5.2
- Kaspersky Security for Windows Server con Kaspersky Endpoint Agent for Windows

Componentes necesarios para el funcionamiento de MDR

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

En la siguiente tabla se indican los componentes requeridos para el envío de telemetría desde los activos. Si alguno de estos componentes está desactivado o ausente, Kaspersky Managed Detection and Response deja de enviar telemetría desde el activo.

El modo Light Agent es compatible con las siguientes versiones:

- Kaspersky Endpoint Security para Windows versión 12.8 o posteriores
- Kaspersky Endpoint Security for Linux versión 12.1 o posteriores

Componente	Documentación
Detección de comportamiento	Kaspersky Endpoint Security para Windows  Kaspersky Endpoint Security for Linux  Kaspersky Embedded Systems Security para Windows  Kaspersky Embedded Systems Security para Linux  Kaspersky Industrial CyberSecurity for Nodes 
Protección frente a amenazas en archivos	Kaspersky Endpoint Security para Windows  Kaspersky Endpoint Security for Linux  Kaspersky Endpoint Security para Mac  Kaspersky Security para Virtualization Light Agent  Kaspersky Embedded Systems Security para Windows  Kaspersky Embedded Systems Security para Linux  Kaspersky Industrial CyberSecurity for Nodes 
System Watcher	Kaspersky Security para Virtualization Light Agent 

La siguiente tabla muestra los componentes que afectan la integridad de la telemetría enviada.

Componente	Documentación
Firewall	Kaspersky Endpoint Security para Windows Kaspersky Security para Virtualization Light Agent Kaspersky Embedded Systems Security para Windows Kaspersky Industrial CyberSecurity for Nodes
Protección frente a amenazas en la red	Kaspersky Endpoint Security para Windows Kaspersky Endpoint Security for Linux Kaspersky Endpoint Security para Mac Kaspersky Embedded Systems Security para Windows Kaspersky Embedded Systems Security para Linux Kaspersky Industrial CyberSecurity for Nodes
Protección frente a amenazas en el correo	Kaspersky Endpoint Security para Windows
Protección frente a amenazas web	Kaspersky Endpoint Security para Windows Kaspersky Endpoint Security for Linux Kaspersky Endpoint Security para Mac Kaspersky Embedded Systems Security para Linux Kaspersky Security para Virtualization Light Agent
Autodefensa	Kaspersky Endpoint Security para Windows Kaspersky Security para Virtualization Light Agent Kaspersky Embedded Systems Security para Windows Kaspersky Industrial CyberSecurity for Nodes

Integración con aplicaciones y soluciones de Kaspersky

La siguiente tabla describe cómo configurar la integración de Kaspersky Managed Detection and Response con otras aplicaciones y soluciones de Kaspersky.

Solución o aplicación	Versión	Configuración
Kaspersky Endpoint Security para Windows Kaspersky Endpoint Security for Linux Kaspersky Endpoint Security para Mac Kaspersky Security para Virtualization Light Agent Kaspersky Industrial CyberSecurity for Nodes Windows Kaspersky Embedded Systems Security Windows Kaspersky Security for Windows Server con Kaspersky Endpoint Agent for Windows		Consulte el siguiente artículo: Activación de la solución MDR en aplicaciones de Kaspersky .

Solución o aplicación	Versión	Configuración
Kaspersky Endpoint Detection and Response Expert (local)	8.0 o posterior integrado en la Open Single Management Platform con Kaspersky Next XDR 2.1 o posterior	Requiere claves de licencia activas para Kaspersky MDR Expert y Kaspersky EDR Expert. Se requiere la función de Administrador de MDR para configurar la integración. 1. Configure el complemento MDR en la Consola de Open Single Management Platform. 2. En la sección MDR de la interfaz de la Consola OSMP, haga clic en la pestaña Uso de MDR. 3. Expanda el bloque Archivo de configuración de KPSN para la integración con KEDR Expert. 4. Active la opción Aceptar acuerdo de KPSN y haga clic en Aplicar el archivo de configuración de KPSN para la integridad con KEDR Expert. La solución MDR ahora recibe telemetría que incluye alertas de KEDR para su análisis.
Kaspersky Unified Monitoring and Analysis Platform	4.0 o posteriores	Consulte el siguiente artículo: Integración de Kaspersky Managed Detection and Response .
Kaspersky Anti Targeted Attack Platform (KATA)	7.0–7.1	1. Descargue el archivo de configuración de MDR. 2. Active la integración de MDR. No disponible en la siguiente región: Reino de Arabia Saudí.
	8.0 o posteriores	Asegúrese de que el servidor en el que se realiza la configuración de integración con la solución MDR tenga acceso de red a las siguientes direcciones: • *uis.kaspersky.com:443 • mdr.kaspersky.com:443 Asegúrese de que los servidores KATA secundarios tengan acceso a la red mdr.kaspersky.com:443. Consulte el siguiente artículo: Configuración de la integración con Kaspersky Managed Detection and Response. No disponible en la siguiente región: Reino de Arabia Saudí.

Configurar el complemento de MDR

Para administrar Kaspersky Managed Detection and Response mediante la función del complemento de MDR, debe instalar el complemento de MDR en la solución de administración centralizada de la seguridad de la red que utilice:

- Kaspersky Security Center Web Console
- Kaspersky Next Expert View

El complemento de MDR está preinstalado en Kaspersky Next Expert View.

- Open Single Management Platform

Prerrequisitos

Asegúrese de tener acceso a Kaspersky Security Center Web Console, Kaspersky Next Expert View u Open Single Management Platform, con los siguientes derechos de acceso mínimos:

- Derecho de acceso de **lectura** para el área funcional [Funciones generales: Integración de aplicaciones](#) 
- **Permita** el derecho de acceso para el área funcional [Acceso a incidentes](#) de Kaspersky Managed Detection and Response.

Instalar el complemento de MDR en Kaspersky Security Center Web Console

Para instalar el complemento de MDR en Kaspersky Security Center Web Console:

1. En el menú principal de Kaspersky Security Center Web Console, vaya a **Configuración** → **Complementos web**.
2. En la ventana que se abre, haga clic en el botón **Añadir**.
Se muestra una lista de complementos disponibles.
3. En la lista de complementos disponibles, seleccione el complemento de MDR.
Se muestra la página de descripción del complemento.
4. En la página de descripción del complemento, haga clic en **Instalar complemento**.
5. Cuando la instalación se haya completado, haga clic en **Aceptar**.

El complemento de MDR se descarga con la configuración predeterminada y se muestra en la lista de complementos web de administración.

Instalar el complemento de MDR en Open Single Management Platform

Si Open Single Management Platform funciona en un entorno de red cerrado, debe especificar la configuración del proxy. Ejecute el siguiente comando en el host de Open Single Management Platform para añadir variables de entorno con la configuración del proxy:

```
kubectl set env deployment/plugin-mdr-proxy -n nwc \
  HTTP_PROXY=http://<proxy>:8080 \
  HTTPS_PROXY=http://<proxy>:8080 \
  NO_PROXY=localhost,127.0.0.1,.local,.cluster.local
```

Ejecute el siguiente comando para asegurarse de que se hayan configurado las variables de entorno:

```
kubectl rollout status deployment/plugin-mdr-proxy -n nwc
```

Para instalar el complemento de MDR en OSMP:

1. Transfiera el archivo del complemento web de administración al host del administrador donde se encuentra la utilidad KDT.
2. En el host del administrador con la utilidad KDT, ejecute el siguiente comando para instalar el complemento:

```
./kdt apply -k <ruta al archivo comprimido del complemento>
```

3. Recargue la interfaz de la Consola OSMP para mostrar el complemento agregado.

El complemento web de administración de MDR queda instalado y usted puede acceder a las funciones de MDR en la consola OSMP.

Puede usar la utilidad KDT para ver la lista de complementos web instalados y cerciorarse de que el complemento web de administración de MDR se haya instalado correctamente.

Para ver la lista de complementos web de administración y otros componentes relacionados con OSMP,

En el host del administrador donde se encuentra la utilidad KDT, ejecute el siguiente comando:

```
./kdt state
```

La lista de componentes integrados en OSMP se muestra en la ventana de línea de comandos. Usted puede revisar esta lista para cerciorarse de que el complemento web de administración de MDR está instalado.

Resultados

Una vez finalizado este escenario, el complemento de MDR queda configurado para funcionar con Kaspersky Managed Detection and Response.

Activación e implementación de MDR al utilizar versiones actualizadas de las aplicaciones y un solo inquilino

Las siguientes instrucciones para activar y desplegar la solución MDR son adecuadas si se cumplen las siguientes condiciones:

- Hay versiones actualizadas de las aplicaciones instaladas en todos sus activos:
 - Kaspersky Endpoint Security para Windows versión 12.10 o posteriores
 - Kaspersky Endpoint Security for Linux versión 12.3 o posteriores
 - Kaspersky Endpoint Security for Mac versión 12.2 o posteriores
 - Kaspersky Industrial CyberSecurity for Nodes Windows versión 4.5 o posteriores

- Kaspersky Embedded Systems Security for Windows versión 4.0 o posteriores
- Kaspersky Embedded Systems Security for Linux versión 4.0 o posteriores
- No tiene previsto utilizar el [multiinquilinato](#) inmediatamente después de la implementación.
Podrá configurar el multiinquilinato más adelante añadiendo archivos de configuración de MDR (BLOB) a las aplicaciones.
- Dispone de alguna de las siguientes licencias:
 - Kaspersky NEXT Complete Security
 - Kaspersky Optimum Security
 - Kaspersky Symphony MDR
 - Kaspersky NEXT MDR Optimum
 - Kaspersky MDR
 - Kaspersky Managed Detection and Response

Prerrequisitos

Asegúrese de que su infraestructura de TI cumpla con los [requisitos de hardware y software de Kaspersky Managed Detection and Response](#).

Activación e implementación

Siga estos pasos para activar e implementar la solución MDR:

Paso 1. Autenticación en la Web Console MDR

Realice los siguientes pasos:

1. Vaya a la [Web Console MDR](#).
2. Haga clic en **Crear cuenta**. Cree una nueva cuenta de usuario.
3. En la [Web Console MDR](#), inicie sesión con la cuenta de usuario creada.
4. Cuando se le solicite, introduzca el código de activación enviado a la dirección de correo electrónico que especificó al crear la cuenta de usuario.

5. Seleccione la región de procesamiento de datos de acuerdo con la ubicación de uso de la licencia.
6. Cuando se le solicite, acepte los acuerdos y confirme la activación de MDR.

Paso 2. Activación de la solución MDR en sus activos

Si utiliza la solución MDR con cualquiera de las siguientes licencias, la solución MDR se activa automáticamente en sus activos, por lo que puede omitir este paso y continuar con la etapa 3:

- Kaspersky NEXT Complete Security
- Kaspersky Symphony MDR
- Kaspersky NEXT MDR Optimum

Active la licencia de MDR en sus activos:

Activación en Kaspersky Security Center Web Console

1. En el menú principal, vaya a **Operaciones** → **Licencias de Kaspersky**.
2. Haga clic en el botón **Añadir**.
3. Añada el archivo clave o aplique el código de activación:
 - **Añadir archivo clave**
Haga clic en el botón **Seleccionar archivo clave** y busque el archivo .key que desea añadir.
 - **Introducir el código de activación**
Introduzca el código de activación y haga clic en el botón **Enviar**.
4. Haga clic en el botón **Cerrar**.
5. En la página **Licencias de Kaspersky**, haga clic en el nombre de la licencia actual.
Se abren las propiedades de la licencia.
6. En la pestaña **General**, active el parámetro **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.
7. Haga clic en **Guardar**.

La clave de licencia se distribuye automáticamente a los activos. Si desea distribuir una clave de licencia a los dispositivos cliente mediante la tarea de distribución de claves de licencia, consulte [la Ayuda en línea de Kaspersky Security Center](#).

Activación en Open Single Management Platform

1. En el menú principal, haga clic en el nombre del Servidor de administración.
Se abre la ventana de propiedades del Servidor de administración.
2. En la pestaña **General**, seleccione la sección **Claves de licencia**.

3. Haga clic en **Añadir nueva clave de licencia** y especifique una nueva clave de licencia.
4. Haga clic en **Guardar**.
5. En la página **Claves de licencia**, haga clic en el nombre de la clave de licencia añadida.
Se abren las propiedades de la clave de licencia.
6. En la pestaña **General**, active el parámetro **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.
7. Haga clic en **Guardar**.

La clave de licencia se distribuye automáticamente a los activos.

En el siguiente artículo se describe cómo ver las claves de licencia y los códigos de activación en uso en el Servidor de administración: [Visualización de información sobre las claves de licencia y los códigos de activación en uso](#).

Paso 3. Activación del uso de KSN

En Kaspersky Security Center Web Console, Kaspersky Next Expert View u Open Single Management Platform, vaya a la sección **Gestión de activos** → **Directivas y perfiles**. Active el uso de KSN en las directivas de todas las aplicaciones utilizadas en sus activos:

Kaspersky Endpoint Security para Windows/Linux

1. Seleccione la directiva de la aplicación. Si no se ha creado la directiva de la aplicación, haga clic en **Añadir** y cree la directiva.
2. En la directiva de la aplicación, vaya a **Configuración de la aplicación** → **Configuración general** → **Kaspersky Security Network**.
3. Active el parámetro **Uso de Kaspersky Security Network**.
4. Active el parámetro **Uso de modo KSN extendido**.
5. Si desea utilizar el Servidor de administración como servidor proxy, active los siguientes parámetros:
 - **Usar el Servidor de administración como servidor proxy de KSN** para enviar la telemetría de activos mediante el proxy de KSN.
 - **Usar servidores de Kaspersky Security Network si el servidor proxy de KSN no está disponible** para enviar la telemetría de activos mediante KSN cuando el proxy de KSN no esté disponible.
6. Haga clic en **Guardar y cerrar**.

Los dispositivos cliente pueden enviar solicitudes a KSN, obtener información de KSN y transferir información a KSN aunque no tengan acceso directo a Internet. El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

Kaspersky Endpoint Security para Mac

1. Seleccione la directiva de la aplicación. Si no se ha creado la directiva de la aplicación, haga clic en **Añadir** y cree la directiva.
2. En la configuración de la directiva de la aplicación, vaya a **Configuración de la aplicación** → **Protección avanzada contra amenazas** → **Kaspersky Security Network**.
3. Active el parámetro **Kaspersky Security Network**.
4. Active el parámetro **Modo KSN extendido**.
5. Si desea utilizar el Servidor de administración como servidor proxy, active los siguientes parámetros:
 - **Usar el Servidor de administración como servidor proxy de KSN** para enviar la telemetría de activos mediante el proxy de KSN.
 - **Usar servidores de Kaspersky Security Network si el servidor proxy de KSN no está disponible** para enviar la telemetría de activos mediante KSN cuando el proxy de KSN no esté disponible.
6. Haga clic en **Guardar y cerrar**.

Los dispositivos cliente pueden enviar solicitudes a KSN, obtener información de KSN y transferir información a KSN aunque no tengan acceso directo a Internet. El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

Paso 4. Configuración de los ajustes de red en sus activos

Para activos con acceso a Internet, permita el tráfico saliente no SSL y desactive la inspección de tráfico en los puertos 443 y 1443 hacia las siguientes direcciones:

*.ksn.kaspersky-labs.com

ksn - *. kaspersky-labs.com

ds.kaspersky.com

Para activos sin acceso a Internet, configure el proxy de KSN para acceder a los servidores de KSN. Permita el tráfico saliente no SSL y desactive la inspección de tráfico para las siguientes variantes:

- Tráfico desde el activo al proxy de KSN a través del puerto 13111 ([puerto predeterminado](#) )
- Tráfico desde el proxy de KSN a través de los puertos 443 y 1443 a las siguientes direcciones:
 - *.ksn.kaspersky-labs.com
 - ksn - *. kaspersky-labs.com
 - ds.kaspersky.com

Recomendamos configurar la conexión directa entre los activos y los servidores de KSN. Este enfoque ayuda a prevenir la pérdida de telemetría en dos casos: en los equipos portátiles que usan conexiones remotas, o si el proxy de KSN no está disponible.

La solución MDR se ha activado e implementado. Los activos administrados por MDR se muestran en Web Console MDR después de la sincronización (hasta 24 horas): mdr.kaspersky.com/assets.

Ahora puede proceder a configurar la solución MDR:

- [Invite a nuevos usuarios en Web Console MDR](#).
- [Configure las notificaciones periódicas](#).
- [Active las notificaciones ampliadas](#).

Activación e implementación de MDR al utilizar versiones actualizadas de las aplicaciones y multiinquilinato

Las siguientes instrucciones para activar y desplegar la solución MDR son adecuadas si se cumplen las siguientes condiciones:

- Hay versiones actualizadas de las aplicaciones instaladas en todos sus activos:
 - Kaspersky Endpoint Security para Windows versión 12.10 o posteriores
 - Kaspersky Endpoint Security for Linux versión 12.3 o posteriores
 - Kaspersky Endpoint Security for Mac versión 12.2 o posteriores
 - Kaspersky Industrial CyberSecurity for Nodes Windows versión 4.5 o posteriores
 - Kaspersky Embedded Systems Security for Windows versión 4.0 o posteriores (solo se puede asignar al inquilino raíz)
 - Kaspersky Embedded Systems Security for Linux versión 4.0 o posteriores (solo se puede asignar al inquilino raíz)
- Tiene previsto utilizar [multiinquilinato](#) inmediatamente después de la implementación.
- Dispone de alguna de las siguientes licencias:
 - Kaspersky NEXT Complete Security
 - Kaspersky Symphony MDR
 - Kaspersky Next MXDR Optimum
 - Kaspersky MDR
 - Kaspersky Managed Detection and Response

- Kaspersky MDR Expert Add-on
- Kaspersky MDR Optimum Add-on
- Kaspersky Managed Detection and Response Basic Add-on
- Kaspersky Managed Detection and Response Advanced Add-on
- Kaspersky Managed Detection and Response Prime Add-on

Prerrequisitos

Asegúrese de que su infraestructura de TI cumpla con los [requisitos de hardware y software de Kaspersky Managed Detection and Response](#).

Activación e implementación

Siga estos pasos para activar e implementar la solución MDR:

Paso 1. Autenticación en la Web Console MDR

Realice los siguientes pasos:

1. Vaya a la [Web Console MDR](#).
2. Haga clic en **Crear cuenta**. Cree una nueva cuenta de usuario.
3. En la [Web Console MDR](#), inicie sesión con la cuenta de usuario creada.
4. Cuando se le solicite, introduzca el código de activación enviado a la dirección de correo electrónico que especificó al crear la cuenta de usuario.
5. Seleccione la región de procesamiento de datos de acuerdo con la ubicación de uso de la licencia.
6. Cuando se le solicite, acepte los acuerdos y confirme la activación de MDR.

Paso 2. Creación de inquilinos y descarga de archivos de configuración

Siga las instrucciones siguientes:

1. [Cree nuevos inquilinos en la Web Console MDR](#).
2. Para cada uno de los inquilinos creados, [descargue el archivo de configuración de MDR y añada el archivo BLOB \(P7\) a las directivas de la aplicación](#).

Paso 3. Activación de la solución MDR en sus activos

Si usa la solución MDR con cualquiera de las siguientes licencias, la solución MDR se activa automáticamente en sus activos, por lo que puede omitir este paso y continuar con el paso 4:

- Kaspersky NEXT Complete Security
- Kaspersky Symphony MDR
- Kaspersky NEXT MDR Optimum

Active la licencia de MDR en sus activos:

Activación en Kaspersky Security Center Web Console

1. En el menú principal, vaya a **Operaciones** → **Licencias de Kaspersky**.

2. Haga clic en el botón **Añadir**.

3. Añada el archivo clave o aplique el código de activación:

- **Añadir archivo clave**

Haga clic en el botón **Seleccionar archivo clave** y busque el archivo .key que desea añadir.

- **Introducir el código de activación**

Introduzca el código de activación y haga clic en el botón **Enviar**.

4. Haga clic en el botón **Cerrar**.

5. En la página **Licencias de Kaspersky**, haga clic en el nombre de la licencia actual.

Se abren las propiedades de la licencia.

6. En la pestaña **General**, active el parámetro **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.

7. Haga clic en **Guardar**.

La clave de licencia se distribuye automáticamente a los activos. Si desea distribuir una clave de licencia a los dispositivos cliente mediante la tarea de distribución de claves de licencia, consulte [la Ayuda en línea de Kaspersky Security Center](#).

Activación en Open Single Management Platform

1. En el menú principal, haga clic en el nombre del Servidor de administración.

Se abre la ventana de propiedades del Servidor de administración.

2. En la pestaña **General**, seleccione la sección **Claves de licencia**.

3. Haga clic en **Añadir nueva clave de licencia** y especifique una nueva clave de licencia.

4. Haga clic en **Guardar**.

5. En la página **Claves de licencia**, haga clic en el nombre de la clave de licencia añadida.

Se abren las propiedades de la clave de licencia.

6. En la pestaña **General**, active el parámetro **Distribuir automáticamente la clave de licencia a los dispositivos administrados**.

7. Haga clic en **Guardar**.

La clave de licencia se distribuye automáticamente a los activos.

En el siguiente artículo se describe cómo ver las claves de licencia y los códigos de activación en uso en el Servidor de administración: [Visualización de información sobre las claves de licencia y los códigos de activación en uso](#).

Paso 4. Activación del uso de KSN

En Kaspersky Security Center Web Console, Kaspersky Next Expert View u Open Single Management Platform, vaya a la sección **Gestión de activos** → **Directivas y perfiles**. Active el uso de KSN en las directivas de todas las aplicaciones utilizadas en sus activos:

Kaspersky Endpoint Security para Windows/Linux

1. Seleccione la directiva de la aplicación. Si no se ha creado la directiva de la aplicación, haga clic en **Añadir** y cree la directiva.
2. En la directiva de la aplicación, vaya a **Configuración de la aplicación** → **Configuración general** → **Kaspersky Security Network**.
3. Active el parámetro **Uso de Kaspersky Security Network**.
4. Active el parámetro **Uso de modo KSN extendido**.
5. Si desea utilizar el Servidor de administración como servidor proxy, active los siguientes parámetros:
 - **Usar el Servidor de administración como servidor proxy de KSN** para enviar la telemetría de activos mediante el proxy de KSN.
 - **Usar servidores de Kaspersky Security Network si el servidor proxy de KSN no está disponible** para enviar la telemetría de activos mediante KSN cuando el proxy de KSN no esté disponible.
6. Haga clic en **Guardar y cerrar**.

Los dispositivos cliente pueden enviar solicitudes a KSN, obtener información de KSN y transferir información a KSN aunque no tengan acceso directo a Internet. El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

Kaspersky Endpoint Security para Mac

1. Seleccione la directiva de la aplicación. Si no se ha creado la directiva de la aplicación, haga clic en **Añadir** y cree la directiva.
2. En la configuración de la directiva de la aplicación, vaya a **Configuración de la aplicación** → **Protección avanzada contra amenazas** → **Kaspersky Security Network**.

3. Active el parámetro **Kaspersky Security Network**.

4. Active el parámetro **Modo KSN extendido**.

5. Si desea utilizar el Servidor de administración como servidor proxy, active los siguientes parámetros:

- **Usar el Servidor de administración como servidor proxy de KSN** para enviar la telemetría de activos mediante el proxy de KSN.
- **Usar servidores de Kaspersky Security Network si el servidor proxy de KSN no está disponible** para enviar la telemetría de activos mediante KSN cuando el proxy de KSN no esté disponible.

6. Haga clic en **Guardar y cerrar**.

Los dispositivos cliente pueden enviar solicitudes a KSN, obtener información de KSN y transferir información a KSN aunque no tengan acceso directo a Internet. El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

Paso 5. Configuración de los ajustes de red en sus activos

Para activos con acceso a Internet, permita el tráfico saliente no SSL y desactive la inspección de tráfico en los puertos 443 y 1443 hacia las siguientes direcciones:

*.ksn.kaspersky-labs.com

ksn - *. kaspersky-labs.com

ds.kaspersky.com

Para activos sin acceso a Internet, configure el proxy de KSN para acceder a los servidores de KSN. Permita el tráfico saliente no SSL y desactive la inspección de tráfico para las siguientes variantes:

- Tráfico desde el activo al proxy de KSN a través del puerto 13111 ([puerto predeterminado](#)).
- Tráfico desde el proxy de KSN a través de los puertos 443 y 1443 a las siguientes direcciones:

*.ksn.kaspersky-labs.com

ksn - *. kaspersky-labs.com

ds.kaspersky.com

Recomendamos configurar la conexión directa entre los activos y los servidores de KSN. Este enfoque ayuda a prevenir la pérdida de telemetría en dos casos: en los equipos portátiles que usan conexiones remotas, o si el proxy de KSN no está disponible.

La solución MDR se ha activado e implementado. Los activos administrados por MDR se muestran en MDR Console después de la sincronización (hasta 24 horas): mdr.kaspersky.com/assets.

Ahora puede proceder a configurar la solución MDR:

- [Invite a nuevos usuarios en MDR Console.](#)
- [Configure las notificaciones periódicas.](#)
- [Active las notificaciones ampliadas.](#)

Activación e implementación de MDR al utilizar versiones heredadas de las aplicaciones

Use las siguientes instrucciones si su infraestructura incluye activos con versiones heredadas de aplicaciones:

- Kaspersky Endpoint Security para Windows 12.9 y versiones anteriores
- Kaspersky Endpoint Security para Linux versión 12.2 y anteriores
- Kaspersky Endpoint Security for Mac versión 12.1 y anteriores
- Kaspersky Security for Virtualization Light Agent versión 5.2
- Kaspersky Security for Windows Server con Kaspersky Endpoint Agent for Windows

Prerrequisitos

Asegúrese de que su infraestructura de TI cumpla con los [requisitos de hardware y software de Kaspersky Managed Detection and Response](#).

Activación e implementación

La activación e implementación de la solución MDR se realiza por etapas:

Paso 1. Autenticación en la Web Console MDR

Realice los siguientes pasos:

1. Vaya a la [Web Console MDR](#) [↗].
2. Haga clic en **Crear cuenta**. Cree una nueva cuenta de usuario.
3. En la [Web Console MDR](#) [↗], inicie sesión con la cuenta de usuario creada.

4. Cuando se le solicite, introduzca el código de activación enviado a la dirección de correo electrónico que especificó al crear la cuenta de usuario.
5. Seleccione la región de procesamiento de datos de acuerdo con la ubicación de uso de la licencia.
6. Cuando se le solicite, acepte los acuerdos y confirme la activación de MDR.

Paso 2. Creación de inquilinos y descarga de archivos de configuración

Siga las instrucciones siguientes:

1. Si necesita multiinquilinato, [cree nuevos inquilinos en la consola de MDR](#).
2. Para cada uno de los inquilinos creados, [descargue el archivo de configuración de MDR y añada el archivo BLOB \(P7\) a las directivas de la aplicación](#).

Paso 3. Configuración de KPSN

[Implemente el archivo de configuración de KPSN](#).

Paso 4. Activación del uso de KSN

En Kaspersky Security Center Web Console, Kaspersky Next Expert View u Open Single Management Platform, vaya a la sección **Gestión de activos** → **Directivas y perfiles**. Active el uso de KSN en las directivas de todas las aplicaciones utilizadas en sus activos:

1. Seleccione la directiva de la aplicación. Si no se ha creado la directiva de la aplicación, haga clic en **Añadir** y cree la directiva.
2. En la configuración de la directiva de la aplicación, vaya a **Configuración de la aplicación** → **Protección avanzada contra amenazas** → **Kaspersky Security Network**.
3. Active el parámetro **Kaspersky Security Network**.
4. Active el parámetro **Modo KSN extendido**.
5. (Opcional) Si el Servidor de administración se utiliza como proxy, active los siguientes parámetros:
 - Active **Usar el Servidor de administración como servidor proxy de KSN** para enviar la telemetría de activos mediante el proxy de KSN.
 - Active **Usar servidores de Kaspersky Security Network si el servidor proxy de KSN no está disponible**.
6. Haga clic en **Guardar y cerrar**.

Los dispositivos cliente pueden enviar solicitudes a KSN, obtener información de KSN y transferir información a KSN aunque no tengan acceso directo a Internet. El servidor proxy de KSN almacena en caché los datos procesados y reduce, de esta manera, la carga en el canal de salida y el período de tiempo que se utiliza para esperar información solicitada por un dispositivo cliente.

Paso 5. Configuración de los ajustes de red en sus activos

Para activos con acceso a Internet, permita el tráfico saliente no SSL y desactive la inspección de tráfico en los puertos 443 y 1443 hacia las siguientes direcciones:

*.ksn.kaspersky-labs.com

ksn - *. kaspersky-labs.com

ds.kaspersky.com

Para activos sin acceso a Internet, configure el proxy de KSN para acceder a los servidores de KSN. Permita el tráfico saliente no SSL y desactive la inspección de tráfico para las siguientes variantes:

- Tráfico desde el activo al proxy de KSN a través del puerto 13111 ([puerto predeterminado](#) ).
- Tráfico desde el proxy de KSN a través de los puertos 443 y 1443 a las siguientes direcciones:

*.ksn.kaspersky-labs.com

ksn - *. kaspersky-labs.com

ds.kaspersky.com

Recomendamos configurar la conexión directa entre los activos y los servidores de KSN. Este enfoque ayuda a prevenir la pérdida de telemetría en dos casos: en los equipos portátiles que usan conexiones remotas, o si el proxy de KSN no está disponible.

La solución MDR se ha activado e implementado. Los activos administrados por MDR se mostrarán en MDR Console después de la sincronización (hasta 24 horas): mdr.kaspersky.com/assets.

Ahora puede proceder a configurar la solución MDR:

- [Invite a nuevos usuarios en MDR Console](#).
- [Configure las notificaciones periódicas](#).
- [Active las notificaciones ampliadas](#).

Implementar un archivo de configuración de KPSN

Debe implementar un archivo de configuración de KPSN si al menos un activo de su infraestructura tiene instalada una versión heredada de la aplicación:

- Kaspersky Endpoint Security para Windows 12.9 y anteriores
- Kaspersky Endpoint Security para Linux versión 12.2 y anteriores
- Kaspersky Endpoint Security for Mac versión 12.1 y anteriores
- Kaspersky Security for Virtualization Light Agent versión 5.2
- Kaspersky Security for Windows Server con Kaspersky Endpoint Agent for Windows

La implementación de un archivo de configuración de KPSN se realiza en dos etapas.

Etapas 1. Descargar el archivo de configuración de MDR

Las instrucciones para descargar el archivo de configuración de MDR dependen de si ha creado inquilinos adicionales e instalado el complemento de MDR para Kaspersky Security Center.

El archivo de configuración de MDR es un archivo comprimido ZIP que contiene un archivo de configuración de KPSN (.pkcs7) para implementar aplicaciones EPP.

Para descargar el archivo de configuración de MDR en MDR Web Console:

1. En la ventana Consola, navegue hasta el elemento del menú **Settings**.
2. Abra la pestaña **Tenants**.
3. Haga clic en la línea que corresponda al inquilino para el que desea descargar el archivo de configuración de MDR.
Aparece el bloque **Tenant settings**.
4. Haga clic en el nombre del archivo comprimido para descargarlo.

Para descargar el archivo de configuración de MDR en la consola de Kaspersky Security Center:

1. En la sección MDR de Kaspersky Security Center Web Console o Kaspersky Next Expert View, haga clic en **Licencias**.
2. Busque la columna **Archivo comprimido para configuración de activos** y haga clic en **Descargar** para descargar el archivo.

Etapa 2. Implementar el archivo de configuración de KPSN

Puede implementar el archivo de configuración de KPSN en Kaspersky Security Center Web Console. Si ha instalado el [complemento MDR](#), también puede implementar el archivo de configuración de KPSN en el menú del complemento MDR.

Descomprima el archivo de configuración de MDR e instale el archivo de configuración de KPSN (.pkcs7).

Para instalar el archivo de configuración de KPSN en Kaspersky Security Center Web Console:

1. Vaya a las propiedades del Servidor de administración; para ello, haga clic en su nombre en el menú principal.
2. En la pestaña **General**, seleccione la sección **Configuración del proxy de KSN**.
3. Active la opción **Activar proxy de KSN en el Servidor de administración**.
4. Active la opción **Usar Kaspersky Private Security Network**.
5. Haga clic en **Seleccionar archivo con proxy de KSN** y cargue el archivo de configuración de KPSN (.pkcs7).
Se muestran los detalles del archivo de configuración de KPSN.
6. Haga clic en **Guardar**.

El archivo de configuración de KPSN se ha instalado.

Para instalar el archivo de configuración de KPSN en el menú del complemento MDR de Kaspersky Security Center Web Console o de Open Single Management Platform:

1. En el menú principal, abra la sección **MDR**.
2. Abra la pestaña **Uso de MDR**.
3. Expanda el bloque **Archivo de configuración de KPSN para la integración con el Servidor de administración de KSC**.
4. Active la opción **Aceptar acuerdo de KPSN** y haga clic en **Aplicar el archivo de configuración de KPSN al Servidor de administración**.

El archivo de configuración de KPSN se ha instalado.

Implementar un archivo de configuración de MDR (BLOB)

Puede utilizar archivos de configuración de MDR (BLOB) para activar la solución MDR en aplicaciones que admitan la integración con MDR mediante directivas de Kaspersky Security Center.

Si utiliza inquilinos que no sean el inquilino raíz, debe descargar los archivos de configuración de MDR para cada inquilino.

Las versiones heredadas de las aplicaciones requieren el uso de archivos de configuración de MDR (BLOB):

- Kaspersky Endpoint Security para Windows 12.6 y anteriores
- Kaspersky Endpoint Security para Linux versión 12.2 y anteriores
- Kaspersky Endpoint Security for Mac versión 12.1 y anteriores
- Kaspersky Security for Virtualization Light Agent versión 5.2
- Kaspersky Security for Windows Server con Kaspersky Endpoint Agent for Windows

La activación de la solución MDR mediante el archivo de configuración de MDR (BLOB) se realiza en dos etapas.

Etapas 1. Descargar el archivo de configuración de MDR

Las instrucciones para descargar el archivo de configuración de MDR dependen de si ha creado inquilinos adicionales e instalado el complemento de MDR para Kaspersky Security Center.

El archivo de configuración de MDR es un archivo comprimido ZIP que contiene un archivo BLOB (P7) para implementar aplicaciones EPP.

Para descargar el archivo de configuración de MDR en MDR Web Console:

1. En la ventana Consola, navegue hasta el elemento del menú **Settings**.
2. Haga clic en la pestaña **Tenants**.
3. Haga clic en la línea que corresponda al inquilino para el que desea descargar el archivo de configuración de MDR.
Aparece el bloque **Tenant settings**.
4. Haga clic en el nombre del archivo comprimido para descargarlo.

Para descargar el archivo de configuración de MDR en la consola de Kaspersky Security Center:

1. En la sección MDR de Kaspersky Security Center Web Console o Kaspersky Next Expert View, haga clic en **Licencias**.
2. Busque la columna **Archivo comprimido para configuración de activos** y haga clic en **Descargar** para descargar el archivo.

Etapas 2. Añadir el archivo de configuración de MDR (BLOB) a las directivas de la aplicación

Descomprima el archivo de configuración de MDR y utilice el archivo BLOB (P7) para activar la solución MDR.

Para activar la solución MDR en las siguientes aplicaciones:

- Kaspersky Endpoint Security para Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security para Mac

1. En Kaspersky Security Center Web Console u Open Single Management Platform, vaya a la sección **Gestión de activos** → **Directivas y perfiles**.
2. Seleccione la directiva de la aplicación. Si no se ha creado la directiva de la aplicación, haga clic en **Añadir** y cree la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Agentes integrados** → **Managed Detection and Response**.
5. Active el parámetro Managed Detection and Response.
6. Haga clic en **Cargar** y seleccione el archivo BLOB (P7) que extrajo del archivo de configuración de MDR.
7. Cierre el icono de candado (🔒) para aplicar la configuración.
8. Haga clic en **Guardar y cerrar**.

El archivo de configuración de MDR (BLOB) se carga y se implementa automáticamente en las aplicaciones.

Para activar la solución MDR en Kaspersky Industrial CyberSecurity for Nodes Windows:

1. En Kaspersky Security Center Web Console u Open Single Management Platform, vaya a la sección **Gestión de activos** → **Directivas y perfiles**.
2. Seleccione la directiva de Kaspersky Industrial CyberSecurity for Nodes Windows. Si no se ha creado la directiva de la aplicación, haga clic en **Añadir** y cree la directiva.
3. Seleccione la pestaña **Configuración de la aplicación**.
4. Vaya a **Servidores de conexión de telemetría**.
5. En la sección **Managed Detection and Response**, haga clic en **Configurar**.
6. Active el parámetro **Managed Detection and Response**.
7. Haga clic en **Cargar** y seleccione el archivo BLOB (P7) que extrajo del archivo de configuración de MDR.
8. Haga clic en **Guardar y cerrar**.

El archivo de configuración de MDR (BLOB) se carga y se implementa automáticamente en las aplicaciones.

Despliegue con la captura y copia de la imagen de un dispositivo

Si necesita instalar aplicaciones en los activos en los que también se debe instalar (o reinstalar) un sistema operativo y otro software, puede utilizar el mecanismo para capturar y copiar la imagen de un activo de referencia.

El despliegue con la captura y copia de la imagen de un dispositivo se lleva a cabo en dos pasos:

1. Prepare un activo de referencia que tenga el software necesario instalado.
2. Capture la imagen del activo de referencia preparado y distribuya la imagen a los activos mediante la tarea dedicada de Kaspersky Security Center.

Si su licencia de Kaspersky Security Center proporciona la función de Administración de sistemas, puede [utilizar la función de Kaspersky Security Center para capturar y distribuir la imagen a los activos](#). De lo contrario, utilice las herramientas de terceros disponibles en la organización.

Preparación de un activo de referencia

Para preparar un activo de referencia basado en Windows, haga lo siguiente:

1. Instale y configure el sistema operativo y otro software que necesite distribuir.
2. En el activo de referencia, en la configuración de Conexiones de red de Windows, desconecte el activo de referencia de la red donde está instalado Kaspersky Security Center.
3. En el activo de referencia, inicie la instalación local del Agente de red con el archivo setup.exe.
Se inicia el asistente de instalación del Agente de red de Kaspersky Security Center. Siga las instrucciones del asistente.
4. En la página Servidor de administración del asistente, especifique la dirección IP del Servidor de administración.
Si no conoce la dirección exacta del Servidor de administración, introduzca localhost. Puede cambiar la dirección IP más adelante [usando la utilidad klmove](#) con la clave -address.
5. En la página Iniciar aplicación del asistente, desactive la opción Iniciar aplicación durante la instalación.
6. Cuando la instalación del Agente de red esté completa, no reinicie el activo antes de crear una imagen del sistema operativo.
Si reinicia el activo, tendrá que repetir todo el proceso y preparar un activo de referencia para la creación de una imagen del sistema operativo.
7. En el activo de referencia, en la línea de comandos, inicie la utilidad sysprep y ejecute el siguiente comando:
sysprep.exe /generalize /oobe /shutdown.

El activo de referencia está listo para crear una imagen del sistema operativo.

Para preparar un activo de referencia basado en Linux, haga lo siguiente:

1. Instale y configure el sistema operativo y otro software que necesite distribuir.
2. Asegúrese de que se cumplan las siguientes condiciones:
 - El activo de referencia no tiene Kaspersky Endpoint Security for Linux instalado.
 - El dispositivo de referencia no se ha conectado a Kaspersky Security Center.

Si se ha infringido alguna de estas condiciones, es probable que la solución de MDR no identifique correctamente los activos que se crearon con la distribución de la imagen del activo de referencia. Para resolver este problema, lleve a cabo los siguientes pasos en los activos que tienen Kaspersky Endpoint Security for Linux instalado:

- a. Ejecute los siguientes comandos para generar un nuevo UUID:

```
uuidgen > /var/opt/kaspersky/kesl/common/pcid
```

```
uuidgen > /var/opt/kaspersky/epagent/install_id
```

- b. Desinstale el Kaspersky Endpoint Security for Linux y, luego, vuelva a instalarlo.

El activo de referencia está listo para crear una imagen del sistema operativo.

Captura y distribución de la imagen de un activo de referencia

Cuando se apliquen las herramientas de terceros para la captura de la imagen de un activo con el Agente de red instalado, utilice uno de los siguientes métodos:

- Método recomendado. Cuando se instale el Agente de red en un activo de referencia, capture la imagen del activo antes de que se ejecute por primera vez el servicio del Agente de red (ya que la información única que identifica al activo se crea en la primera conexión del Agente de red al Servidor de administración). Después de eso, se recomienda no ejecutar el servicio del Agente de red hasta que se complete la operación de captura de la imagen.

En el caso de Windows, consulte el siguiente artículo: [Preparación de un activo de referencia con el Agente de red instalado para crear una imagen del sistema operativo](#).

En el caso de Linux, consulte el siguiente artículo: [Despliegue con la captura y copia de la imagen de un activo](#).

- En el activo de referencia, detenga el servicio del Agente de red y ejecute la utilidad klmover con la clave -dupfix. La utilidad klmover se incluye en el paquete de instalación del Agente de red. Evite cualquier ejecución posterior del servicio del Agente de red hasta que la operación de la captura de imagen se complete.

Asegúrese de que la utilidad klmover se ejecute con la clave -dupfix antes de la primera ejecución del servicio del Agente de red en los dispositivos de destino. Se trata de un requisito obligatorio y debe cumplirse en el primer inicio del sistema operativo tras el despliegue de la imagen.

- Utilice el modo de clonación de disco del Agente de red.

En el caso de Windows, consulte el siguiente artículo: [Modo de clonación de disco del Agente de red](#).

En el caso de Linux, consulte el siguiente artículo: [Modo de clonación de disco del Agente de red](#).

También puede capturar la imagen de un activo sin el Agente de red instalado. Para hacerlo, realice el despliegue de la imagen en los activos de destino y, luego, despliegue el Agente de red. Si se utiliza este método, proporcione acceso a la carpeta de red con los paquetes de instalación independientes desde el activo. Siga las instrucciones:

- En el caso de Windows, consulte el siguiente artículo: [Instalación de imágenes de los sistemas operativos](#).
- En el caso de Linux, consulte el siguiente artículo: [Acerca de las tareas de instalación remota en Kaspersky Security Center Linux](#).

Activar la solución MDR en las aplicaciones de Kaspersky

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Esta sección contiene información de referencia sobre cómo activar la solución MDR en función de la licencia y de las versiones de la aplicación. Para obtener un tutorial completo sobre cómo activar la solución MDR, consulte el siguiente artículo: [Activar e implementar Kaspersky Managed Detection and Response](#).

Los siguientes artículos describen cómo administrar las claves de licencia y los códigos de activación en el Servidor de administración:

- [Distribución automática de claves de licencia y códigos de activación](#)
- [Visualización de información sobre las claves de licencia y los códigos de activación en uso](#)

Licencia de MDR	Aplicaciones compatibles con los siguientes métodos: Código de activación Archivo BLOB	Aplicaciones compatibles con los siguientes métodos: Archivo BLOB
Kaspersky Symphony MDR Kaspersky NEXT Complete Security Kaspersky Optimum Security Kaspersky Next MXDR Optimum Vea: Licencias de Kaspersky Symphony MDR y NEXT Complete Security.	• Kaspersky Endpoint Security para Windows versión 12.6 o posteriores • Kaspersky Endpoint Security para Windows versión 12.8 o posterior en modo Light Agent • Kaspersky Endpoint Security para Windows versión 12.6 o posteriores en el modo de agente de Endpoint Detection and Response • Kaspersky Endpoint Security for Linux versión 12.3 o posteriores • Kaspersky Endpoint Security for Linux versión 12.3 o posteriores en el modo Light Agent • Kaspersky Endpoint Security for Mac versión 12.2 o posteriores Instale el archivo BLOB si su organización tiene varios inquilinos. La activación con un archivo de clave tiene un soporte limitado. Le recomendamos que utilice un código de activación.	• Kaspersky Endpoint Security para Windows 12.5 y versiones anteriores • Kaspersky Endpoint Security para Windows versiones 5.2–6.1 o más recientes en modo Agente ligero • Kaspersky Endpoint Security for Windows versión 12.3–12.5 en modo Endpoint Detection and Response Agent • Kaspersky Endpoint Security para Linux versión 12.2 y anteriores • Kaspersky Endpoint Security para Linux versión 12.2 y anteriores en modo Agente ligero • Kaspersky Endpoint Security for Mac versión 12.1 y anteriores La versión 4.0–7.1 de Kaspersky Anti Targeted Attack Platform (incluido EDR) admite la instalación del archivo de configuración de MDR, que incluye el archivo BLOB y el archivo de configuración de KPSN. Kaspersky Anti Targeted Attack Platform (EDR incluido) versión 8.0 no requiere el archivo de configuración de MDR.
Kaspersky MDR Kaspersky Managed Detection and Response Ver: Licencias de Kaspersky MDR	• Kaspersky Endpoint Security para Windows versión 12.6 o posteriores • Kaspersky Endpoint Security para Windows versión 12.8 o posterior en modo Light Agent • Kaspersky Endpoint Security para Windows versión 12.6 o posteriores en el modo de agente de Endpoint Detection and Response • Kaspersky Endpoint Security for Linux versión 12.3 o posteriores • Kaspersky Endpoint Security for Linux versión 12.3 o posteriores en el modo Light Agent • Kaspersky Endpoint Security for Mac versión 12.2 o posteriores • Kaspersky Embedded Systems Security for Windows versión 4.0 o posteriores • Kaspersky Embedded Systems Security for Linux versión 4.0 o posteriores Instale el archivo BLOB si su organización tiene varios inquilinos. La activación con un archivo de clave tiene un soporte limitado. Le recomendamos que utilice un código de activación.	• Kaspersky Endpoint Security para Windows 12.5 y versiones anteriores • Kaspersky Endpoint Security para Windows versiones 5.2–6.1 o más recientes en modo Agente ligero • Kaspersky Endpoint Security for Windows versión 12.3–12.5 en modo Endpoint Detection and Response Agent • Kaspersky Endpoint Security para Linux versión 12.2 y anteriores • Kaspersky Endpoint Security para Linux versión 12.2 y anteriores en modo Agente ligero • Kaspersky Endpoint Security for Mac versión 12.1 y anteriores La versión 4.0–7.1 de Kaspersky Anti Targeted Attack Platform (incluido EDR) admite la instalación del archivo de configuración de MDR, que incluye el archivo BLOB y el archivo de configuración de KPSN.
Kaspersky MDR Optimum Add-on Kaspersky MDR Expert Add-on Kaspersky Managed Detection and Response Basic Add-on Kaspersky Managed Detection and Response Advanced Add-on Kaspersky Managed Detection and Response Prime Add-on Ver: Licencias de complementos para Kaspersky MDR.	• Kaspersky Endpoint Security para Windows versión 12.6 o posteriores • Kaspersky Endpoint Security para Windows versión 12.8 o posterior en modo Light Agent • Kaspersky Endpoint Security para Windows versión 12.6 o posteriores en el modo de agente de Endpoint Detection and Response Instale el archivo BLOB si su organización tiene varios inquilinos. La activación con un archivo de clave tiene un soporte limitado. Le recomendamos que utilice un código de activación.	• Kaspersky Endpoint Security para Windows 12.5 y versiones anteriores • Kaspersky Endpoint Security para Windows versiones 5.2–6.1 o más recientes en modo Agente ligero • Kaspersky Endpoint Security for Windows versión 12.3–12.5 en modo Endpoint Detection and Response Agent La versión 4.0–7.1 de Kaspersky Anti Targeted Attack Platform (incluido EDR) admite la instalación del archivo de configuración de MDR, que incluye el archivo BLOB y el archivo de configuración de KPSN.
Kaspersky Managed Detection and Response for Industrial CyberSecurity	Kaspersky Industrial CyberSecurity for Nodes Windows versión 4.5 o posterior. Instale el archivo BLOB si su organización tiene varios inquilinos.	Instale el archivo BLOB si su organización tiene varios inquilinos. En este escenario, sigue siendo necesaria una clave de archivo o un código de activación.

Licencia de MDR	Aplicaciones compatibles con los siguientes métodos: Código de activación Archivo BLOB	Aplicaciones compatibles con los siguientes métodos: Archivo BLOB
Ver: Licencia adicional de Kaspersky MDR for Industrial CyberSecurity		

Activar la solución MDR en aplicaciones de Kaspersky. Licencias de complementos de Kaspersky MDR

Las siguientes tablas describen los métodos para activar la solución MDR en las aplicaciones de Kaspersky para las siguientes licencias:

- Kaspersky MDR Expert Add-on
- Kaspersky MDR Optimum Add-on
- Kaspersky Managed Detection and Response Basic Add-on
- Kaspersky Managed Detection and Response Advanced Add-on
- Kaspersky Managed Detection and Response Prime Add-on

Kaspersky Endpoint Security para Windows

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.10 o posteriores	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Para activar tanto la solución Endpoint Detection and Response Optimum como la solución MDR, utilice el código de activación para Endpoint Detection and Response Optimum y un archivo de configuración MDR (BLOB) para la solución MDR.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.9	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Para activar tanto la solución Endpoint Detection and Response Optimum como la solución MDR, utilice el código de activación para Endpoint Detection and Response Optimum y un archivo de configuración MDR (BLOB) para la solución MDR.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
12.6–12.8	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Para activar tanto la solución Endpoint Detection and Response Optimum como la solución MDR, utilice el código de activación para Endpoint Detection and Response Optimum y un archivo de configuración MDR (BLOB) para la solución MDR.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
12.5 y anteriores	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Endpoint Security en modo Windows Endpoint Detection and Response Agent

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.10 o posteriores	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Para activar tanto la solución Endpoint Detection and Response Optimum como la solución MDR, utilice el código de activación para Endpoint Detection and Response Optimum y un archivo de configuración MDR (BLOB) para la solución MDR.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.9	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado.
12.6–12.8	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado.
12.3–12.5	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Security para Virtualization Light Agent

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
6.3 o posteriores Kaspersky Endpoint Security para Windows versión 12.10 o posterior en el modo Light Agent	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Para activar tanto la solución Endpoint Detection and Response Optimum como la solución MDR, utilice el código de activación para Endpoint Detection and Response Optimum y un archivo de configuración MDR (BLOB) para la solución MDR.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
6.2 Kaspersky Endpoint Security para Windows 12.8–12.9 en el modo Light Agent	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Para activar tanto la solución Endpoint Detection and Response Optimum como la solución MDR, utilice el código de activación para Endpoint Detection and Response Optimum y un archivo de configuración MDR (BLOB) para la solución MDR.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
6.0–6.1 Kaspersky Security for Virtualization Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
5.2 Kaspersky Security for Virtualization Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.
6.3 o posteriores Kaspersky Endpoint Security for Linux versión 12.3 o posterior en el modo Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
6.2 Kaspersky Endpoint Security for Linux versión 12.2 en el modo Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Activar la solución MDR en aplicaciones de Kaspersky. Licencias de Kaspersky MDR

Las siguientes tablas describen los métodos para activar la solución MDR en las aplicaciones de Kaspersky para las siguientes licencias:

- Kaspersky MDR
- Kaspersky Managed Detection and Response

Kaspersky Endpoint Security para Windows

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.10 o posteriores	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.9	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
12.6–12.8	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Para activar tanto la solución Endpoint Detection and Response Optimum como la solución MDR, utilice el código de activación para Endpoint Detection and Response Optimum y un archivo de configuración MDR (BLOB) para la solución MDR.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
12.5 y anteriores	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Endpoint Security en modo Windows Endpoint Detection and Response Agent

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.10 o posteriores	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.9	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado.
12.6–12.8	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado.
12.3–12.5	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Security para Virtualization Light Agent

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
6.3 o posteriores Kaspersky Endpoint Security para Windows versión 12.10 o posterior en el modo Light Agent	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
6.2 Kaspersky Endpoint Security para Windows 12.8–12.9 en el modo Light Agent	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Para activar tanto la solución Endpoint Detection and Response Optimum como la solución MDR, utilice el código de activación para Endpoint Detection and Response Optimum y un archivo de configuración MDR (BLOB) para la solución MDR.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
6.0–6.1 Kaspersky Security for Virtualization Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.
5.2 Kaspersky Security for Virtualization Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.
6.3 o posteriores Kaspersky Endpoint Security for Linux versión 12.3 o posterior en el modo Light Agent	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
6.2 Kaspersky Endpoint Security for Linux versión 12.2 en el modo Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Endpoint Security para Windows

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.3 o posteriores	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: - Si está utilizando inquilinos de MDR en el momento dado. - Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: - Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. - Configure la directiva para instalar el archivo BLOB en sus activos.
12.2 y anteriores	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Endpoint Security para Mac

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.2 o posteriores	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: - Si está utilizando inquilinos de MDR en el momento dado. - Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. Una configuración de MDR (BLOB) caducada se debe reemplazar por una nueva.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: - Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. - Configure la directiva para instalar el archivo BLOB en sus activos.
12.1 y anteriores	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Embedded Systems Security para Windows

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
4.0	Aplique un código de activación o un archivo clave para activar la solución MDR. No es necesario usar un archivo de configuración MDR (BLOB), todos los activos se asignan al inquilino raíz de forma predeterminada.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN.

Kaspersky Embedded Systems Security para Linux

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
4.0	Aplique un código de activación o un archivo clave para activar la solución MDR. No es necesario usar un archivo de configuración MDR (BLOB), todos los activos se asignan al inquilino raíz de forma predeterminada.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN.

Activar la solución MDR en aplicaciones de Kaspersky. Licencias de Kaspersky Symphony MDR, Kaspersky Next Complete Security, Kaspersky Optimum Security y Kaspersky Next MXDR Optimum

Las siguientes tablas describen los métodos para activar la solución MDR en las aplicaciones de Kaspersky para las siguientes licencias:

- Kaspersky Symphony MDR
- Kaspersky NEXT Complete Security
- Kaspersky Optimum Security
- Kaspersky Next MXDR Optimum

Kaspersky Endpoint Security para Windows

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.10 o posteriores	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.9	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
12.6–12.8	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
12.5 y anteriores	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Security para Virtualization Light Agent

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
6.0–6.1 Kaspersky Security for Virtualization Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.
5.2 Kaspersky Security for Virtualization Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.
6.3 o posteriores Kaspersky Endpoint Security para Windows versión 12.10 o posterior en el modo Light Agent	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Light Agent no se puede activar con la licencia de NEXT Complete Security.	La aplicación admite el uso de MDR con y sin un archivo de configuración KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
6.2 Kaspersky Endpoint Security para Windows 12.8–12.9 en el modo Light Agent	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación. Light Agent no se puede activar con la licencia de NEXT Complete Security.	La aplicación admite el uso de MDR con y sin un archivo de configuración KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
6.3 o posteriores Kaspersky Endpoint Security for Linux versión 12.3 o posterior en el modo Light Agent	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
6.2 Kaspersky Endpoint Security for Linux versión 12.2 en el modo Light Agent	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Endpoint Security para Windows

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.3 o posteriores	Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación o un archivo de clave en los siguientes casos: • Si está utilizando inquilinos de MDR en el momento dado. • Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: 1. Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. 2. Configure la directiva para instalar el archivo BLOB en sus activos.
12.2 y anteriores	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Kaspersky Endpoint Security para Mac

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
12.2 o posteriores	No se admite la activación de la solución MDR con un archivo clave. Debe tener instalado un archivo de configuración de MDR (BLOB) antes de aplicar un código de activación en los siguientes casos: - Si está utilizando inquilinos de MDR en el momento dado. - Alguna vez ha creado inquilinos de MDR, incluso si se han eliminado inquilinos adicionales. No es necesario cambiar la configuración de MDR caducada (BLOB) instalada antes cuando aplica un código de activación.	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN. Para utilizar la solución MDR sin un archivo de configuración de KPSN, proporcione el código de activación incluso si tiene un archivo de configuración MDR (BLOB) implementado. Si ya tiene archivos de configuración de MDR (BLOB) instalados en sus activos y la solución MDR se activó antes de enero de 2024, deberá volver a descargar y reinstalar los archivos BLOB: - Descargue el archivo de configuración de MDR (BLOB) para el inquilino requerido en Web Console MDR. - Configure la directiva para instalar el archivo BLOB en sus activos.
12.1 y anteriores	La solución MDR se puede activar con un archivo de configuración MDR (BLOB).	La solución MDR solo puede funcionar cuando el archivo de configuración de KPSN está instalado en Kaspersky Security Center.

Activar la solución MDR en aplicaciones de Kaspersky. Licencia del complemento para Kaspersky Managed Detection and Response for Industrial CyberSecurity

En la siguiente tabla se describen los métodos para activar la solución MDR en aplicaciones de Kaspersky con la licencia del complemento de Kaspersky Managed Detection and Response for Industrial CyberSecurity.

Kaspersky Industrial CyberSecurity for Nodes Windows

Versión de aplicación	Método de activación	Requisito de archivo de configuración de KPSN
4.5	Aplique un código de activación o un archivo clave para activar la solución MDR: - Si no utiliza y nunca ha creado inquilinos MDR, no es necesario utilizar un archivo de configuración MDR (BLOB). Si utiliza inquilinos MDR, debe instalar un archivo de configuración MDR (BLOB), incluso si ha caducado. La aplicación admite el uso de MDR con y sin un archivo de configuración KPSN. Use la versión 3.0.0 o posteriores del complemento MDR a fin de aplicar varios códigos de activación para la licencia de Kaspersky Industrial CyberSecurity for Nodes. Puede usar Web Console MDR si solo tiene un código de activación para la licencia de Kaspersky Industrial CyberSecurity for Nodes. La aplicación de nuevos códigos de activación para Kaspersky Industrial CyberSecurity for Nodes no está disponible en la región del Reino de Arabia Saudí, si tiene alguna de las siguientes licencias: - Kaspersky Managed Detection and Response Basic Add-on - Kaspersky Managed Detection and Response Advanced Add-on - Kaspersky Managed Detection and Response Prime Add-on	La aplicación admite el uso de MDR con y sin un archivo de configuración de KPSN.

Licencias

Una *licencia* es un derecho por tiempo limitado para usar la aplicación, otorgado bajo los Términos y condiciones.

Solo puede usar una licencia en la Consola web de MDR y en la versión 2.4.1 y anteriores del complemento MDR. Cuando introduce un nuevo código de activación, este reemplaza al anterior.

A partir de la versión 2.4.2 del complemento MDR, [puede utilizar varias licencias MDR al mismo tiempo](#).

Una licencia le otorga los siguientes tipos de servicios:

- Usar de la aplicación de acuerdo con los Términos y Condiciones
- Obtener soporte técnico

El alcance de los servicios y el período de validez dependen del tipo de licencia bajo la cual se activó la aplicación.

Se proporcionan los siguientes tipos de licencia:

- *De prueba*: licencia gratuita destinada a probar la aplicación.

Una licencia de prueba suele ser de corta duración. Cuando caduca la licencia de prueba, todas las funciones de Kaspersky Managed Detection and Response se desactivan. Para seguir usando la aplicación, debe adquirir una licencia comercial.

Puede activar la aplicación bajo la licencia de prueba solo una vez.

- *Comercial*: licencia de pago que se otorga al comprar la aplicación.

Cuando expira la licencia comercial, la aplicación continúa ejecutándose con funcionalidad limitada (no se proporciona telemetría). Para seguir usando todas las funciones de Kaspersky Managed Detection and Response, debe renovar su licencia comercial.

Recomendamos renovar la licencia antes de que caduque, para garantizar la máxima protección contra todas las amenazas a la seguridad.

- *Suscripción*: licencia de pago que permite el uso de la aplicación durante un período de facturación mensual o anual, con renovación automática, hasta que se cancele o caduque.

La licencia de suscripción puede ser de dos tipos:

- *Limitada*: se renueva automáticamente al final de cada período de facturación hasta la fecha de caducidad definida.
- *Abierta*: se renueva automáticamente al final de cada período de facturación hasta que el cliente la cancele.

Puede administrar la licencia de suscripción a través del Portal de administración de licencias de Kaspersky (LMP).

Si cambia el alcance de su licencia, por ejemplo, cambia la cantidad de activos, los detalles de la licencia se actualizan en MDR Web Console en un plazo de 24 horas.

Cuando la licencia de suscripción se cancela o caduca, la aplicación continúa ejecutándose con funcionalidad limitada (no se proporciona telemetría). Para continuar usando todas las funciones de Kaspersky Managed Detection and Response, debe renovar su licencia de suscripción.

Recomendamos renovar la licencia antes de que caduque, para garantizar la máxima protección contra todas las amenazas a la seguridad.

Comparación de los niveles de licencias comerciales

El conjunto de funciones disponibles en Kaspersky Managed Detection and Response depende del nivel de su licencia comercial (consulte la tabla a continuación).

Comparación de los niveles de licencia comercial de Kaspersky Managed Detection and Response

Característica	MDR / MDR Expert*	MDR Optimum* /MDR Basic*	MDR Advanced*	MDR Prime*
Supervisión ininterrumpida, detección y gestión de incidentes	✓	✓	✓	✓
Búsqueda automática de amenazas	✓	✓	✓	✓
Repuesta automática a incidentes y planes de respuesta manual	✓	✓	✓	✓
Verificación del estado y la visibilidad de los activos	✓	✓	✓	✓
MDR Web Console con paneles e informes	✓	✓	✓	✓
Capacidad para recibir información avanzada sobre incidentes	✓	✓	✓	✓
Período de retención del historial de incidentes	1 año	1 año	1 año	1 año
Período de retención de los datos sin procesar	3 meses	1 mes	3 meses	3 meses
Investigación de incidentes y búsqueda de amenazas administrada	✓	—	✓	✓
Soporte técnico experto ampliado para la gestión de incidentes	✓	—	✓	✓
Acceso a Kaspersky Threat Intelligence Portal (para licencias con fecha de inicio anterior al 12 de julio de 2024)	✓	—	✓	✓
API para exportar datos desde Kaspersky MDR	✓	—	✓	✓
Los clientes pueden crear un incidente personalizado para que lo procese la solución Kaspersky MDR**	✓	—	✓	✓
Almacenamiento de datos localizado*	✓	✓	✓	✓
Multiinquilinato	✓	✓	✓	✓
Añadir y editar comentarios a incidentes	✓	✓	✓	✓
Añadir y editar archivos adjuntos a incidentes	✓	✓	✓	✓
Investigación avanzada de incidentes: análisis para establecer los antecedentes, las circunstancias y el mecanismo detallado del ataque	—	—	✓ Los clientes no pueden elegir qué incidentes enviar a la investigación avanzada ni se garantiza un tiempo de respuesta al incidente	✓ Los clientes pueden elegir qué incidentes enviar a la investigación avanzada y se garantiza un tiempo de respuesta al incidente

*Este nivel o funcionalidad está disponible solo para algunas regiones y es posible que los nuevos clientes no puedan comprarlo. Comuníquese con su proveedor de soluciones de Kaspersky Managed Detection and Response para obtener detalles sobre los niveles de licencias comerciales disponibles.

**La solución Kaspersky Managed Detection and Response garantiza el procesamiento de tres solicitudes por semana, de conformidad con los [objetivos de rendimiento de la entrega de la solución](#). El número de solicitudes procesadas según los objetivos del rendimiento de prestación de la solución aumenta proporcionalmente: por cada 10 000 endpoints conectados, el número de solicitudes se incrementa en 1.

Sobre el código de activación

Un *código de activación* es una secuencia única de 20 letras y números. Debe ingresar un código de activación para [activar Kaspersky Managed Detection and Response](#). Recibirá el código de activación en la dirección de correo electrónico que proporcionó cuando compró Kaspersky Managed Detection and Response.

Para activar la aplicación mediante el código de activación, necesita acceso a Internet para conectarse a los servidores de activación de Kaspersky.

Si ha perdido su código de activación, comuníquese con el socio de Kaspersky a quien le compró la licencia.

Provisión de un nuevo código de activación

Activación inicial de Kaspersky Managed Detection And Response

Consulte estos artículos:

- Activar Kaspersky Managed Detection and Response en Kaspersky Security Center (recomendado)
- Activar Kaspersky Managed Detection and Response en MDR Web Console

Introducir un nuevo código de activación.

Debe proporcionar un nuevo código de activación para Kaspersky Managed Detection and Response, por ejemplo, cuando desee actualizar el servicio o cuando necesite renovar una licencia que está por caducar.

Esta función solo está disponible si tiene configurado el derecho de acceso a la **Integración de la aplicación** en [Kaspersky Security Center Web Console](#) o [Kaspersky Next Expert View](#).

Para obtener detalles sobre cómo administrar varias licencias en Kaspersky Managed Detection and Response en Kaspersky Security Center con el complemento MDR 2.4.2 o versiones posteriores, consulte este artículo: [Administrar licencias en Kaspersky Security Center](#).

Si utiliza una única licencia para la solución MDR, puede renovarla en Web Console MDR. Se requiere la función **Administrador de MDR**.

Si su organización tiene varias licencias vigentes, solo podrá administrarlas en Kaspersky Security Center. El uso de Web Console MDR para la renovación de la licencia en este escenario impide que se envíe telemetría desde los activos.

Le recomendamos utilizar el complemento MDR para Kaspersky Security Center para introducir un nuevo código de activación.

Para introducir un nuevo código de activación para Kaspersky Managed Detection and Response en Kaspersky Security Center con el complemento MDR:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Licencias**.
2. Haga clic en el botón **Activar la solución** e ingrese el código de activación en el panel que aparece.
3. Seleccione los inquilinos a los que tendrán acceso los usuarios de este Servidor de administración.

Se aplica el nuevo código de activación. Kaspersky Managed Detection and Response funciona con la licencia proporcionada.

Para reemplazar el código de activación actual por uno nuevo en Web Console MDR:

1. Haga clic en la pestaña **Licensing**.
2. Haga clic en el enlace **Enter a new activation code**.
3. Introduzca un nuevo código de activación y haga clic en **Continue**.
4. Seleccione su región y haga clic en **Confirm and activate**.

Administrar inquilinos en Kaspersky Security Center

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Si su organización tiene varias licencias vigentes, solo podrá administrarlas en Kaspersky Security Center.

Se requiere el rol **Administrador de MDR** para gestionar claves de licencia.

Para ver las licencias:

En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Licencias**.

Aparece la lista **Licencias en su organización**. El panel superior muestra información general sobre las licencias.

- Región
- [Nivel de licencia comercial](#)
- Número total y límite de activos conectados

En la pestaña **Vigente** solo se muestran las licencias actuales. Haga clic en la pestaña **Todas** para ver todas las claves de licencia de su organización.

La tabla muestra la siguiente información acerca de las licencias:

Nombre de la licencia

Nombre de la licencia que incluye detalles como el nivel de la licencia y el límite de activos.

Activos conectados / límite

La cantidad de activos que utilizan esta licencia y el límite.

Si se supera el límite de activos admitidos por la licencia, se los resalta con rojo.

Este número no incluye hosts con archivos de configuración BLOB creados antes del 1 de enero de 2024. Para solucionar este problema, actualice el archivo BLOB en la configuración del inquilino y aplíquelo a los activos del inquilino. Consulte el siguiente tema para obtener más detalles: [Acerca de el archivo de configuración MDR](#).

Id.

El identificador de licencia.

Fecha de caducidad

La fecha de caducidad de la licencia se resalta en rojo si la licencia ha caducado o caduca en 14 días o antes.

Estado

Uno de los siguientes estados de inquilino:

- Vigente
- Caducada
- Reemplazada
- No usada
- Reemplazadas

Nombre del cliente

Oculto de forma predeterminada. Puede activar esta columna en el menú de la tabla.

Para descargar un archivo CSV que muestre las licencias por inquilino (complemento MDR versión 2.4.2),

En la pestaña **Vigente**, haga clic en **Exportar por inquilinos a CSV**.

El archivo CSV incluye la distribución de activos por inquilino para cada licencia.

Para mostrar las licencias por inquilinos (complemento de MDR versión 2.5.0 o posterior),

En la pestaña **Vigente**, haga clic en **Mostrar el uso de licencias por inquilinos**.

La tabla muestra la distribución de activos por inquilino para cada licencia.

Para descargar el [archivo de configuración MDR](#) de una licencia,

Seleccione la columna **Archivo comprimido para configuración de activos** y haga clic en **Download**.

Para introducir un nuevo código de activación,

Haga clic en el botón **Enter a new activation code** e introduzca el código de activación en el panel correspondiente.

El [nivel de la licencia](#) y la región de la nueva licencia deben coincidir con el nivel de licencia y la región de los demás códigos de activación de su organización.

Para quitar un código de activación:

1. Seleccione el botón de opción junto al código de activación que desea eliminar y haga clic en el icono .
2. En la ventana que aparece, confirme la eliminación de la clave de licencia.

El estado de la licencia cambia a **Not used**. Puede volver a ingresar el código de activación eliminado.

Solución de problemas de licencias

Si ha activado la solución MDR en sus activos y la sección **Licencias** en MDR Web Console muestra menos activos de los que están conectados a la solución MDR, consulte la siguiente lista de posibles causas y sus respectivas soluciones.

La solución MDR se activa con varias licencias

Solución:

Active todas las claves de licencia en el complemento MDR. La consola web de MDR no admite la activación de solo algunas claves de licencia.

La solución MDR se activó en los dispositivos antes del 01.01.2024 usando el archivo de configuración de MDR (BLOB)

Solución 1:

1. [Descargue un nuevo archivo de configuración de MDR \(BLOB\)](#).
2. Aplique el nuevo archivo de configuración de MDR (BLOB) en sus activos.

Solución 2:

[Aplique un código de activación](#) para activar la solución MDR en sus activos.

Algunos de sus activos utilizan Kaspersky Endpoint Security para Windows versión 12.9 o anterior, y la solución MDR en estos activos se ha activado con un archivo clave.

Solución:

[Aplique un código de activación](#) para activar la solución MDR en sus activos. La activación con un archivo clave en dichos activos tiene una compatibilidad limitada y no se recomienda.

Ha utilizado un archivo de clave para la licencia de Kaspersky Next Complete Security, Kaspersky Optimum Security, Kaspersky Next MXDR Optimum o Kaspersky Symphony MDR para activar Kaspersky Endpoint Security para Windows versión 12.9 o anterior

Solución:

[Aplique un código de activación](#) para activar la solución MDR en sus activos.

Acerca del acuerdo de MDR

El *Acuerdo de MDR* es un acuerdo vinculante entre usted y AO Kaspersky Lab, que estipula los términos sobre cómo puede utilizar la solución.

Lea atentamente el acuerdo de MDR antes de comenzar a utilizar la solución.

Puede ver el acuerdo de MDR:

- Durante la activación de Kaspersky Managed Detection and Response.
- Al hacer clic en el enlace de **Condiciones de uso para la solución MDR** en el bloque **Condiciones de uso para la solución MDR** (sección **MDR** de Kaspersky Security Center → **Uso de MDR** → **Condiciones de uso para la solución MDR**).

Usted acepta los términos del acuerdo de MDR al confirmar que está de acuerdo con el Acuerdo de MDR al activar la solución. Si no acepta el Acuerdo de MDR, cancele la activación de Kaspersky Managed Detection and Response y no utilice la solución.

Provisión de datos

Para que algunos componentes de Kaspersky Managed Detection and Response funcionen, es necesario que Kaspersky procese los datos del usuario. Los componentes no envían datos sin el permiso del administrador de Kaspersky Managed Detection and Response.

La lista de datos del usuario depende de la región donde se utiliza la solución. Para su región, la lista de datos del usuario puede diferir de la que se indica en esta sección.

Kaspersky protege cualquier información recibida de acuerdo con la ley y las reglas de Kaspersky aplicables. Los datos se transmiten a través de un canal seguro.

Lista de datos sobre eventos que se producen en los dispositivos del Usuario

Con el fin de identificar las amenazas de seguridad de datos nuevas y complicadas, como también sus orígenes, así como las amenazas de intrusión, y para tomar medidas rápidas para aumentar la protección de los datos almacenados y procesados con el ordenador por el Cliente, el Cliente acepta proporcionar automáticamente lo siguiente información para recibir el Servicio:

- La fecha de instalación y activación del software, nombre completo y versión del software, además de la información sobre las actualizaciones instaladas y la localización de idioma del software.
- Información sobre el software instalado en el equipo, así como la versión del sistema operativo y la fecha de descarga y de instalación de actualizaciones, objetos de kernel, controladores, servicios, entradas de inicio automático, programas que se inician automáticamente en el caso de diversos eventos del sistema (p. ej., inicio del sistema operativo, inicio de sesión del usuario, etc.) y sus configuraciones, extensiones del navegador, extensiones de Microsoft Internet Explorer, extensiones del sistema de impresión, extensiones de Windows Explorer, extensiones de shell del sistema operativo, sumas de comprobación de objetos cargadas (MD5), elementos de configuración activa, aplicaciones del panel de control, versiones del navegador y cliente de correo.
- Información sobre los permisos del sistema de archivos, el bit eficaz para los permisos del sistema de archivos, las versiones de permisos del sistema de archivos, las variables de entorno y los nombres de las llamadas del sistema.
- Información sobre permisos heredados de un archivo de sistema.
- Información sobre el nombre del ordenador, las direcciones IP, las pasarelas predeterminadas, las direcciones MAC y el hardware, así como una suma de comprobación del número de serie del disco duro, los últimos 12 bytes del ID de seguridad del ordenador (SID) y el identificador de la zona de seguridad procedente del flujo de datos NTFS; atributos de Active Directory de la cuenta del equipo, incluyendo el contenido de msDS-AllowedToActOnBehalfOfOtherIdentity, dNSHostName, distinguishedName, sAMAccountName y userAccountControl.
- Información sobre las herramientas de software utilizadas para solucionar problemas en el software instalado en el equipo del Usuario, o para cambiar su funcionalidad, y los códigos de retorno recibidos después de la instalación de cada componente de software.

- Información sobre el estado de la protección antivirus del ordenador, así como las versiones y las fechas y horas de lanzamiento de las bases de datos antivirus en uso, las estadísticas sobre las actualizaciones y las conexiones a los servicios de Kaspersky Lab, los identificadores de trabajos y los identificadores y versiones de los componentes de software que realizan el análisis, los indicadores que muestran el entorno de prueba interno de Kaspersky, los códigos de error principales de un evento específico, los códigos de error secundarios de un evento específico y los números ordinales de los eventos.
- Clave de licencia y número de serie de los productos de Kaspersky Lab, nombres y versiones de estos productos. Identificadores de las instalaciones de los productos de Kaspersky Lab y la descripción del cliente del archivo de información de licencia.
- Información sobre las cuentas de usuario del Cliente: nombre de la cuenta de usuario, nombre del usuario, identificador del sistema operativo, información de inicio de sesión, privilegios, afiliación a grupos, tipos de inicio de sesión en el sistema, nombre del paquete de autenticación, nombres de dominio, nombres DNS utilizados para las sesiones de inicio de sesión del sistema de autenticación, el nombre del servidor utilizado para la autenticación, el nombre principal del usuario (UPN) de la cuenta, el SID y atributos de Active Directory de la cuenta, incluidos mail, altSecurityIdentities y sAMAccountName.
- Contenido completo de los registros del sistema operativo.
- Información sobre los sistemas de llamadas.
- Información sobre las detecciones realizadas por programas de Kaspersky Lab que admiten Kaspersky Managed Detection and Response.
- Información acerca de los correos electrónicos recibidos como las direcciones de correo electrónico del remitente y del destinatario, el asunto, información de archivos adjuntos: nombre del archivo adjunto, tamaño, hash (MD5), resultados del análisis de formato de archivo.
- Información sobre las coordenadas del área de la pantalla en la que se realizó la captura de pantalla.
- Información sobre las conexiones de red, las direcciones IP y los puertos del emisor y el receptor, los índices de zona IPv6, la información sobre la dirección de la conexión de red (entrante/saliente), los tipos y máscaras de las consultas DNS realizadas, los códigos de error de las operaciones de consulta DNS, la respuesta a una consulta DNS e información sobre el servidor DNS solicitado.
- Métodos y datos de conexión HTTP, incluidas direcciones web visitadas, URL del sitio de referencia, agentes de usuario, información sobre el protocolo de enlace TLS: versión del protocolo TLS, nombre de servidor cifrado de la extensión SNI, hash MD5 y hash SHA1 del certificado, nombre común del sujeto principal y lista de nombres DNS de sujetos adicionales, nombre de la autoridad de certificación, número de serie del certificado emitido por la autoridad de certificación, resultado de la verificación del certificado, conjunto de cifrado usado, periodo de validación del certificado, valores decimales JA3 de los paquetes Hello de cliente y servidor y sus hashes MD5 y datos del protocolo de autenticación de red: hash MD5 de datos para autenticación Kerberos, nombre de la cuenta o el equipo, nombre del dominio de Kerberos al que pertenece el nombre del servidor, el nombre del dominio de Kerberos al que pertenece el nombre del servidor, el dominio al que pertenece el nombre del cliente, el UPN de la cuenta, el paquete de criptografía que se utilizó para el ticket de Kerberos emitido, la máscara del indicador del ticket de Kerberos en formato hexadecimal, la hora de emisión del ticket de Kerberos, la hora de vencimiento del ticket de Kerberos, la fecha de vencimiento del ticket (después de la que el ticket no se puede renovar) y el nombre del controlador de dominio utilizado para emitir el ticket de Kerberos.
- Información sobre los protocolos de la capa de aplicaciones: tamaño de la solicitud de búsqueda de LDAP, filtro de solicitud de búsqueda de LDAP, nombre único de la solicitud de búsqueda de LDAP, lista de atributos para la solicitud de búsqueda de LDAP.

- Información de .net: nombre completo del conjunto .NET descargado, indicadores de conjunto del conjunto .NET descargado, indicadores de módulo del módulo .NET descargado, nombre de dominio del conjunto .NET descargado, módulos para el código auxiliar de MSIL generado, información sobre el método administrado: el espacio de nombres del método administrado de interacción, el nombre del método administrado de interacción, la firma del método administrado de interacción, la firma del método nativo y la firma del código auxiliar del método.
- Información sobre los archivos procesada en el sistema operativo: nombre y ruta del archivo, tamaño, atributos, tipos de archivos y objetos, resultados del análisis de formato del archivo, suma de comprobación (MD5), dirección web desde la que se descargó el archivo, dirección de correo electrónico del remitente desde la que se recibió el archivo y el asunto del correo electrónico, el contenido del sistema de archivos de la estructura VERSIONINFO de los metadatos del archivo, información sobre el editor si el archivo está firmado, el ID de usuario del propietario del archivo, el ID de grupo de propietarios del archivo, la hora a la que se accedió por última vez al archivo, la hora a la que se modificaron por última vez los metadatos del archivo, la hora a la que se creó el archivo, las máscaras de indicador de verificación de la firma digital, las fechas de inicio y fin y los códigos de las operaciones en archivos y objetos, el número de lanzamientos de archivos ejecutables, el identificador de formato del archivo, la ruta completa del objeto y la ruta del contenedor del objeto, el contenido del archivo de ejecución automática, el nombre del archivo y la ruta al archivo en la fuente de red remota a la cual se está accediendo.
- Contenido del directorio \etc\.
- Datos de salida de comando.
- Datos de auditoría: resultado de la operación, descripción de la operación, tipo de evento, usuario de la operación.
- Información sobre el proceso: identificador de proceso (PID), rastreo de llamada del proceso, información sobre el archivo ejecutable del proceso y su línea de comando, información sobre el proceso principal, hash MD5 del código de error de computación del archivo ejecutable, códigos de error principales, información de integridad del proceso, información de inicio de sesión, línea de comandos, argumentos de la línea de comandos para el proceso, variables de entorno para el proceso de destino, identificador único del registro de actividad del proceso, nombre o dirección del sitio de inyección de código, información sobre los derechos de acceso del proceso, códigos de error para calcular el hash MD5 de un objeto desde la línea de comandos del proceso, una lista de contenedores de archivos que encapsula el objeto, el directorio de trabajo inicial para el proceso de destino, la matriz de identificadores (PID) para los procesos completados.
- Información de registro: nombres, secciones y valores.
- Información sobre las operaciones remotas: el nombre del equipo remoto y el nombre completo (FQDN) del ordenador remoto en el que se llevó a cabo la operación remota, el nombre de la cuenta de usuario que inició la operación remota, el identificador proporcionado por el sistema del proceso remoto que inició la operación remota, la hora de inicio del proceso remoto que inició la operación remota, el nombre del espacio de nombre para el usuario de los eventos WMI, el nombre del filtro de eventos WMI del usuario, el nombre del usuario creado de los eventos WMI y el código fuente del usuario de los eventos WMI.
- Información de error: código de error para el cálculo MD5, código de error de acceso al archivo, códigos de error principales y códigos de error secundarios.

- Información sobre las tareas de evento de respuesta creadas por especialistas de Kaspersky Lab y del Usuario: nombre y tipo del evento, fecha y hora en que ocurrió el evento, y configuración y resultados de la tarea de respuesta (información sobre el objeto [ruta del objeto, nombre y tamaño del objeto, y sumas de comprobación MD5 y SHA256], información sobre la puesta en cuarentena del objeto, información sobre la supresión del objeto, información sobre la terminación del proceso, información sobre la supresión de una clave/rama de registro, información sobre el inicio del proceso, información sobre objetos solicitados por especialistas de Kaspersky Lab para un análisis detallado a partir del consentimiento del Usuario [nombre, ruta, tamaño y tipo del objeto, sumas de comprobación MD5 y SHA256, descripción del objeto, fecha y hora del procesamiento de la solicitud de archivos, y contenido del archivo], información sobre la instalación y la eliminación del aislamiento de red del dispositivo, e información sobre los errores resultantes de la tarea de respuesta); Resultados de la tarea de análisis de IOC: dirección IP y dirección física de la tabla ARP, nombre y tipo de registro de recursos DNS, dirección IP, historial y información del navegador, ID de registro y nombre de la fuente de datos en el registro de eventos, nombre del registro de eventos, nombre de usuario, hora del evento, hash, nombre completo y tamaño del archivo, dirección IP remota y puerto conectados en el momento del análisis, dirección IP del adaptador local, puerto abierto en el adaptador local, el protocolo como número, nombre del proceso, argumentos del proceso, ruta al archivo de proceso, PID de Windows del proceso y del proceso principal, fecha y hora de inicio del proceso, nombre y descripción del servicio, ruta y nombre del archivo DLL del servicio (para svchost), ruta y nombre del archivo ejecutable del servicio, PID de Windows, tipo, estado y modo de ejecución del servicio, etiqueta, letra y tipo del volumen, valor de Registro de Windows, valor del subárbol del registro, ruta a la clave de registro, parámetro de registro, dirección física del dispositivo, nombre y versión del sistema operativo, nombre de red del dispositivo, dominio o grupo de trabajo.
- Datos sobre los scripts que se ejecuten en el ordenador: argumentos de la línea de comandos, contenido del script o parte del script que se ejecuten en el ordenador, contenido del objeto o parte del objeto recibido por AMSI.
- Datos sobre los comandos recibidos por la aplicación de consola, incluidos los intérpretes de la línea de comandos, que utilicen la redirección de entradas a través de una tubería («pipe») o un archivo, así como los comandos ejecutados por el usuario en las aplicaciones de consola, incluidos los intérpretes de la línea de comandos.

Si la solución MDR se integra con Kaspersky Endpoint Detection and Response Expert, los datos adicionales se detallan a continuación:

- Información sobre archivos analizados:
 - suma de comprobación (MD5) del objeto que se procesa; suma de comprobación (SHA256) del objeto que se procesa; nombre del objeto que se procesa; tamaño del objeto que se procesa; fecha y hora de creación de un objeto que se procesa; indicador que muestra que la firma digital del módulo cargado está presente y es válida; Información sobre el firmante del archivo que se procesa; indicador de confianza del objeto procesado según KSN; formato del objeto que se procesa; información sobre los resultados de la comprobación de la firma del archivo; indicador de confianza del módulo cuya integridad verifica el Software.
- Información sobre alertas y tecnologías de detección:
 - Fecha y hora de lanzamiento de las bases de datos del software; veredicto del software sobre el objeto que se procesa; indicador de detección de depuración; ID del registro activado en las bases de datos Antivirus del software; clase de peligro de vulnerabilidad; ID de detección generada por el software para el usuario; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; ID de imagen del SO invitado de Kaspersky Sandbox; datos del registro interno, generados por el módulo del software antivirus para un objeto que se procesa; hash MD5 de la dirección IP del nodo de Kaspersky Sandbox; número de orden de un objeto que se vuelve a analizar; ID de registro de base de datos de software; valor de nivel del malware detectado o del software legítimo que puede usarse para dañar el equipo o los datos del usuario; Estado de funcionamiento del componente del Software; Fecha y hora de la detección.
- Información sobre los resultados de la comprobación de datos de telemetría tras la activación de reglas IOA:

- funcionalidades asignadas a un objeto que se procesa (para un SO basado en Unix); información sobre eventos de registro del sistema: hora del evento, nombre del registro donde se ha detectado el evento, tipo y categoría del evento, nombre de la fuente del evento y descripción del evento; ID del evento registrado en el Registro de eventos de Windows; marca de tiempo de las bases de datos del software; tamaño del objeto que se procesa; información sobre el grupo de usuarios; fecha y hora de creación de un objeto que se procesa; nombre del objeto que se procesa; suma de comprobación (MD5) del objeto que se procesa; Máscara binaria de los parámetros para el objeto que se procesa; ID del registro activado en las bases de datos Antivirus del software; ID único de la sesión de inicio de sesión; indicador que muestra que la firma digital del objeto que se procesa está presente y es válida; atributos del proceso que atacó el Software Autoprotección; configuración del software actual; nombre del proveedor del Software; nombre del software; ID del dispositivo que estableció la conexión remota con el sistema; ruta hacia el objeto que se procesa; valor del elemento de registro de Windows; tipo de objeto detectado por el software; ID de la cuenta con la cual comenzó el proceso controlado; ID del sistema de proceso (PID); tipo de controlador del dispositivo USB; tipo de función del sistema invocada para bifurcar el nuevo proceso (para un SO basado en Unix); tipo de inicio del servicio de Windows; suma de comprobación (SHA256) del objeto que se procesa; fecha y hora de la última modificación del objeto que se procesa; Dirección web que se procesa; dirección de correo electrónico o partes de la dirección de correo electrónico del remitente que se procesa; código de operación del archivo; Nombre del dispositivo del usuario; Atributos del archivo ejecutable que se procesa; versión del SO, número de compilación del SO, número de actualización del SO, edición del SO, información extendida sobre la edición del SO; familia del sistema operativo; línea de comandos; Información sobre el firmante del archivo que se procesa; Método de solicitud http; veredicto del software sobre el objeto que se procesa; Argumentos de línea de comando para el proceso; direcciones IP o sumas de comprobación de las direcciones IP de la fuente y el destino de la conexión de red que se procesa; nombre de la técnica de ataque MITRE; Fecha y hora de lanzamiento de las bases de datos del software; formato del objeto que se procesa; Descripción de un objeto que se procesa como se define en las propiedades del objeto; remitente HTTP; nombre y versión del SO; fecha y hora de firma del archivo; respuesta del servidor DNS; volumen de tráfico saliente; tipo de sistema de archivos del volumen; derechos de acceso para el objeto que se procesa; marcas abiertas para un objeto que se procesa; El tipo de cuenta de usuario con la que se inició el objeto potencialmente malicioso; fecha y hora de recepción de los datos; Suma de comprobación (SHA1) de un objeto que se procesa; resultado de la acción con el objeto que se procesa; tipo de sesión de inicio; Identificador de zona de seguridad extraído de la secuencia NTFS; ID del mensaje de correo electrónico; operaciones de archivos detectadas con el objeto que se procesa; dirección DNS del servicio web al que se accede; nombre distintivo del objeto; nivel de integridad para el objeto que se procesa; encabezado de la solicitud http que se procesa; datos sobre una aplicación de terceros que ha causado un error: el nombre y la ruta del archivo de imagen de la aplicación, el tamaño del archivo de imagen de la aplicación y la suma de comprobación (MD5, SHA256, SHA-1), el identificador de proceso de la aplicación (PID), la fecha y hora de la compilación y creación del archivo de imagen del proceso de la aplicación, pila de memoria de proceso de aplicación y dirección de memoria de proceso de aplicación donde se produjo un error, tiempo de actividad de la aplicación antes de que ocurriera el error, nombres, versiones y sumas de comprobación (MD5, SHA256, SHA-1) de los archivos de los componentes de la aplicación; indicadores de solicitud de la red HTTP o HTTPS; dirección URL de solicitud, tipo de biblioteca de código abierto, nombre de dominio de solicitud, proveedor CND, método de solicitud, tiempo de inicio de solicitud, tamaño de paquete de solicitud, duración total de la solicitud, código de estado, tamaño del paquete de respuesta, tipo de contenido de respuesta, hora de inicio de solicitud del encabezado de respuesta, hora de finalización de solicitud del encabezado de respuesta, tiempo de inicio del cuerpo de respuesta, tiempo de finalización del cuerpo de respuesta, número de redirecciones, número de fallas de resolución de DNS, número total de resoluciones de DNS, número de hosts resueltos a la vez, resultado de una sola resolución, hora de inicio de una sola resolución, hora de término de una sola resolución, si la resolución es exitosa, la cantidad de fallas de conexión del socket, la cantidad total de conexiones del socket, la dirección de destino de una sola conexión, la hora de inicio de una sola conexión, la hora de término de una sola conexión, la hora de inicio de un protocolo de enlace único, hora de término de un protocolo de enlace único, tipo HTTP, versión HTTP, tipo SSL, tipo de conjunto de cifrado, si la conexión es correcta, información de falla de conexión, información de solicitud de excepción e información de pila cuando la respuesta es anormal; fecha y hora de caducidad del certificado; versión completa del Software; número de objetos transferidos; tipo de unidad; parámetros de las tareas del programador de tareas del sistema operativo; espacio total del disco y cantidad usada actualmente; números de puerto del origen y el destino de la conexión de red que se procesa; valor de confianza de la detección de malware o software lícito que puede usarse para ocasionar daños al equipo o los datos del usuario; fecha y hora de emisión del certificado; ID de la técnica de ataque MITRE; ID del servicio; Nombre de la clave del registro de Windows; asunto del mensaje de correo electrónico que se procesa; fecha y hora cuando el proceso finalizó; nombre del espacio de nombres para el

consumidor de evento WMI; Hora del evento; nombre del filtro usado por el consumidor de evento WMI; el modo de funcionamiento del componente de protección del software; nombre del emisor del certificado; variables de entorno asignadas a un objeto que se procesa (para un SO basado en Unix); tipo de notificación que desencadenó el envío de la estadística; consumidor de evento WMI; Contenido del fragmento del objeto que se procesa; parámetros de la tarea de transferencia de objetos; nombre del protocolo de red usado en el ataque de red detectado; versión del objeto que se procesa; nombre y ruta al elemento de registro de Windows; contador de eventos; ID de la tarea de transferencia de objetos; Máscara binaria de opciones de la consulta DNS; Máscara binaria de opciones de la consulta DNS; nombre del indicador de ataque (IOA); gravedad de la ventana que solicita la acción del usuario; dirección IP local; área de búsqueda de la consulta; número de serie abreviado del disco duro; cadena de la consulta; el servidor proxy utilizado; fuente del objeto que se procesa; Nombre del evento de consumidor WMI creado; número de serie del certificado; versión del indicador de ataque (IOA); identificador del modo del controlador para el dispositivo USB; dirección de correo electrónico o partes de la dirección de correo electrónico del receptor que se procesa; ID del indicador del ataque (IOA); id. de dispositivo; dirección de una conexión de red; origen del tráfico de red que se procesa; host local o host remoto; dirección IP del servidor DNS; Tipo del valor del registro de Windows; ID de la táctica de ataque MITRE; Ubicación donde se inyectó el código en el proceso; error que se produjo en el procesamiento de detección; el host al que se ha establecido una conexión para transferir objetos.

- Atributos de archivo de un objeto que se procesa; parámetros de seguridad extraídos de eventos del Registro de eventos de Windows; motivo de traslado del archivo a la categoría; el nombre del dominio usado para autenticar al propietario de la sesión de inicio; parámetros de objetos de Active Directory; parámetros de operación de eventos del Registro de Eventos de Windows; parámetros de sesión de usuario de los eventos del Registro de eventos de Windows; código del tipo de objeto; versión del componente del Software; ajustes y propiedades del dispositivo de tarjeta inteligente; versión de las estadísticas enviadas; ID del sistema de proceso principal (PID); dirección IP local; parámetros de tareas registrados en los eventos del Registro de Eventos de Windows; dirección DNS del servicio web al que se accede; Dirección web que se procesa; parámetros de conexión de red extraídos de eventos del Registro de eventos de Windows; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; parámetros de objetos de Active Directory; parámetros de operación de eventos del Registro de Eventos de Windows; parámetros adicionales de eventos del Registro de eventos de Windows; parámetros de sesión de usuario de los eventos del Registro de eventos de Windows; el nombre del dominio usado para autenticar al propietario de la sesión de inicio; identificador de seguridad (SID) de la cuenta de usuario; tipo de error; texto del mensaje de error.

Lista de datos sobre eventos que se detectan como resultado del análisis de tráfico de red

Con el fin de identificar los eventos de seguridad de datos nuevos y complicados, como también sus orígenes, así como las amenazas de intrusión, y para tomar medidas rápidas para aumentar la protección de los datos almacenados y procesados con el ordenador por el Cliente, el Cliente acepta proporcionar automáticamente lo siguiente información para recibir el Servicio:

- Información sobre archivos analizados:
suma de comprobación (MD5) del objeto que se procesa; suma de comprobación (SHA256) del objeto que se procesa; nombre del objeto que se procesa; tamaño del objeto que se procesa; fecha y hora de creación de un objeto que se procesa; indicador que muestra que la firma digital del módulo cargado está presente y es válida; Información sobre el firmante del archivo que se procesa; indicador de confianza del objeto procesado según KSN; formato del objeto que se procesa; información sobre los resultados de la comprobación de la firma del archivo; indicador de confianza del módulo cuya integridad verifica el Software.

- Información sobre alertas y tecnologías de detección:
Fecha y hora de lanzamiento de las bases de datos del software; veredicto del software sobre el objeto que se procesa; indicador de detección de depuración; ID del registro activado en las bases de datos Antivirus del software; clase de peligro de vulnerabilidad; ID de detección generada por el software para el usuario; nombre del malware detectado o del software lícito que puede usarse para ocasionar daños al dispositivo o a los datos de usuario; ID de imagen del SO invitado de Kaspersky Sandbox; datos del registro interno, generados por el módulo del software antivirus para un objeto que se procesa; hash MD5 de la dirección IP del nodo de Kaspersky Sandbox; número de orden de un objeto que se vuelve a analizar; ID de registro de base de datos de software; valor de nivel del malware detectado o del software legítimo que puede usarse para dañar el equipo o los datos del usuario; Estado de funcionamiento del componente del Software; Fecha y hora de la detección.
- Información sobre el origen de los objetos procesados y las conexiones de red:
fuente del objeto que se procesa; Dirección web que se procesa; dirección IPv4 del servicio web a la que se accedió; dirección web del origen de la solicitud de servicio web (referenciador); origen del host; el nombre del dominio usado para autenticar al propietario de la sesión de inicio; dirección IP local; Información sobre el cliente que utiliza un protocolo de red (agente de usuario); dirección de correo electrónico o partes de la dirección de correo electrónico del remitente que se procesa; dirección de correo electrónico o partes de la dirección de correo electrónico del receptor que se procesa; asunto del mensaje de correo electrónico que se procesa; direcciones IP o sumas de comprobación de las direcciones IP de la fuente y el destino de la conexión de red que se procesa; números de puerto del origen y el destino de la conexión de red que se procesa; nombre del protocolo de red usado en el ataque de red detectado; nombre del protocolo de red usado en el ataque de red detectado.
- Datos enviados al soporte técnico:
Si se detecta un problema en el lado del usuario que afecta a la calidad de la Solución y requiere la involucración del soporte técnico, la información incluyendo el nombre de la organización y la dirección de correo electrónico de contacto, una descripción del problema y los materiales relacionados que puedan facilitar la comprensión y resolución del problema se transmitirán al equipo de soporte técnico. La dirección de correo electrónico de contacto puede ser: la dirección en la cual se registra la Solución, o la dirección de un empleado específico del usuario si ese empleado ha pedido asistencia a los expertos que proporcionan las Soluciones.
El servicio de soporte técnico crea automáticamente una cuenta en los sistemas de soporte técnico, si no había previamente una cuenta asociada con la dirección de correo electrónico transmitida por los expertos. La creación de una cuenta de empleado de Usuario es necesaria para asegurar la comunicación entre el usuario y el soporte técnico para resolver los problemas relacionados con la Solución.
Esta cuenta solo será utilizada por el Soporte Técnico para resolver problemas relacionados con el Servicio hasta que el propietario de la cuenta cree una solicitud que no esté relacionada con el Servicio.
- Datos enviados al enviar notificaciones e informes de incidentes:
El Usuario puede utilizar el Servicio para enviar notificaciones, cuando se produzcan incidentes de seguridad relacionados con la información y resúmenes de informes sobre incidentes de seguridad relacionados con la información, a los destinatarios especificados por el Usuario.
Si el servicio está configurado para enviar notificaciones e informes a través de correo electrónico, el Encargado procesará los siguientes datos: el ID de usuario y el correo electrónico del Destinatario.
Si el servicio está configurado para enviar notificaciones a través del bot de Telegram, el Encargado procesará los siguientes datos: el ID de usuario, el ID del destinatario de la notificación, una marca que muestra si el destinatario de la notificación se suscribe al bot de Telegram, un enlace al chat del destinatario de la notificación con el bot de Telegram.

Suministro de datos mientras se usa Kaspersky Endpoint Agent

Para obtener detalles sobre el suministro de datos mientras usa Kaspersky Endpoint Agent, consulte el artículo de ayuda correspondiente de [Kaspersky Endpoint Agent for Windows](#).

Regiones donde se realiza el procesamiento de datos

En la siguiente tabla se enumeran las regiones en las que se procesan los datos del usuario de conformidad con el Contrato de procesamiento de datos de Kaspersky Managed Detection and Response.

Regiones donde se realiza el procesamiento de datos

Región de uso de la licencia	Región donde se realiza el procesamiento de datos
Europa, Canadá	Europa
Reino de Arabia Saudí	Reino de Arabia Saudí
Rusia y otras regiones, excepto las mencionadas anteriormente	Rusia

La región de procesamiento de datos depende de la región seleccionada al [activar](#) Kaspersky Managed Detection and Response, para garantizar el cumplimiento de los requisitos legales sobre el procesamiento de datos del usuario.

Acerca del Contrato de procesamiento de datos

El *Contrato de procesamiento de datos* (DPA) es una parte integral del Contrato de Kaspersky Managed Detection and Response. El Contrato de procesamiento de datos se aplica al tratamiento de los datos de los usuarios de AO Kaspersky Lab en nombre del usuario.

El contenido del *Contrato de procesamiento de datos* (DPA), su disponibilidad en las interfaces de la solución y la lista de datos del usuario dependen de la región donde se utiliza la solución.

Puede ver el Contrato de procesamiento de datos:

- Durante la activación de Kaspersky Managed Detection and Response (solo para algunas regiones).
- En la sección **Acerca** de Kaspersky Managed Detection and Response Console:
<https://mdr.kaspersky.com/about> (solo para algunas regiones).

La sección **Acerca de** solo está disponible para usuarios registrados.

- En el conjunto de documentos que obtiene al adquirir la solución Kaspersky Managed Detection and Response (solo para algunas regiones).

Lea atentamente el Contrato de procesamiento de datos antes de comenzar a utilizar la solución.

Usted confirma que ha leído y comprendido por completo el Contrato de procesamiento de datos cuando activa la solución o cuando adquiere la solución Kaspersky Managed Detection and Response. Si no acepta que sus datos se procesen como se describe en el Contrato de procesamiento de datos, cancele la activación de Kaspersky Managed Detection and Response y no utilice la solución.

Interfaces de Kaspersky Managed Detection And Response

En esta sección se proporciona información sobre las interfaces de usuario de Kaspersky Managed Detection and Response.

Puede trabajar con Kaspersky Managed Detection and Response mediante las siguientes interfaces:

- Portal de Kaspersky Managed Detection and Response Console (en lo sucesivo, también denominado MDR Web Console).

MDR Web Console está disponible en <https://mdr.kaspersky.com/> después de iniciar sesión. Para iniciar sesión, utilice la dirección de correo electrónico y la contraseña de la cuenta del [sitio web de Kaspersky creada durante la activación](#) de Kaspersky Managed Detection and Response.

- La sección **MDR** en [Kaspersky Security Center Web Console](#) o en Kaspersky Next Expert View.

Para utilizar Kaspersky Security Center Web Console con Kaspersky Managed Detection and Response, debe [descargar y configurar](#) el complemento de MDR en Kaspersky Security Center Web Console. En Kaspersky Next Expert View, el complemento de MDR viene preinstalado.

Para acceder a las funciones de Kaspersky Managed Detection and Response, en Kaspersky Security Center Web Console o Kaspersky Next Expert View, haga clic en **Monitoreo y reportes** → **MDR**.

Las capacidades y funciones disponibles en estas interfaces son, a grandes rasgos, las mismas, pero recomendamos realizar algunas tareas en una de las interfaces, ya que tiene un conjunto más amplio de funciones o datos disponibles. La interfaz recomendada se especifica en la descripción de tareas y escenarios de uso.

La interfaz de Kaspersky Security Center está diseñada para realizar sobre todo las siguientes tareas:

- [Activar la solución Kaspersky Managed Detection and Response](#)
- Verificar el estado de los activos

La interfaz de la consola web de MDR está destinada a realizar sobre todo las siguientes tareas:

- Tareas de los directores de seguridad: gestionar incidentes
- Tareas del administrador: administrar usuarios de MDR
- Ver y administrar activos

Sección MDR en Kaspersky Security Center

Puede trabajar con Kaspersky Managed Detection and Response en la sección **MDR** de [Kaspersky Security Center Web Console](#) o en Kaspersky Next Expert View. Para acceder a las funciones de Kaspersky Managed Detection and Response, en Kaspersky Security Center haga clic en **Control e informes** → **MDR**.

La sección **MDR** en la interfaz web de [Kaspersky Security Center](#) tiene las siguientes pestañas:

- **Incidentes.** Contiene el enlace a MDR Web Console donde puede administrar sus incidentes.
- **Ajustes.** Permite activar el envío de notificaciones extendidas y cambiar el idioma de los datos de incidentes, notificaciones e informes de incidentes.
- **Licencias.** Le permite administrar las licencias de MDR.
- **API.** Contiene la lista de conexiones API y las funciones para administraras.
- **Inquilinos.** Contiene la lista de inquilinos y las funciones para administrarlos.
- **Estados de los activos de MDR.** Contiene las listas de los activos que funcionan mal y de todos los activos alguna vez vistos.
- **Primeros pasos** (Getting Started). Contiene instrucciones para configurar la solución MDR.
- **Uso de MDR.** Contiene la información sobre el estado de activación de la solución, la licencia, la región de almacenamiento de telemetría, el archivo de configuración de KPSN y el estado de aceptación de las Condiciones de uso.

También puede [añadir](#) el widget **Activos MDR por estado** en el panel **Control e informes** → **Paneles** Kaspersky Security Center.

Configuración del complemento de MDR en Kaspersky Security Center

Esta sección contiene información sobre cómo realizar la configuración inicial del complemento de MDR para trabajar con Kaspersky Managed Detection and Response.

Configurar los derechos de acceso en Kaspersky Security Center

Debe establecer derechos de acceso para cada usuario de Kaspersky Security Center Web Console o Kaspersky Next Expert View que utilice funciones de MDR en Kaspersky Security Center. Los derechos de acceso dependen de las acciones que desee permitir a los usuarios.

Puede crear funciones de MDR con derechos de acceso predefinidos automáticamente haciendo clic en el enlace en el primer paso en la pestaña **Primeros pasos** (Getting Started) del complemento de **MDR** en Kaspersky Security Center.

Para establecer derechos de acceso:

1. En Kaspersky Security Center Web Console, vaya a la sección **Usuarios y funciones** → **Funciones** y cree una nueva función. Para obtener detalles sobre cómo crear funciones, consulte la [Ayuda de Kaspersky Security Center Windows](#), la [Ayuda de Kaspersky Security Center Linux](#) o la [Ayuda de Kaspersky Next Expert View](#).

2. En la pestaña **Derechos de acceso** de una nueva función, establezca el derecho **Permitir** para las áreas funcionales siguientes:

- **Servidor de administración de Kaspersky Security Center** → **Funciones generales** → **Integración de la aplicación**

Servidor de administración de Kaspersky Security Center → **Funciones generales** → **Funcionalidad básica**

Servidor de administración de Kaspersky Security Center → **Funciones generales** → **Acceder a objetos independientemente de sus ACL**

Estos derechos de acceso permiten a los usuarios activar, configurar, usar y finalizar el uso de Kaspersky Managed Detection and Response

- **Kaspersky Managed Detection and Response** → **Acceso a incidentes**

Es necesario configurar el derecho **Permitir** para el área funcional **Acceso a incidentes** para que los usuarios tengan acceso a la sección **MDR** en Kaspersky Security Center. Si el área funcional **Acceso a incidentes** tiene configurado el derecho **Denegar**, los usuarios solo pueden ver la pestaña **Primeros pasos** de la sección **MDR** en Kaspersky Security Center.

- **Kaspersky Managed Detection and Response** → **Administración de inquilinos**

Permite a los usuarios crear, ver y modificar inquilinos.

- **Kaspersky Managed Detection and Response** → **Acceso a la API de REST**

Permite a los usuarios administrar Kaspersky Managed Detection and Response a través de la API de REST.

3. Asigne el rol creado a todos los usuarios que utilizarán las funciones de MDR en Kaspersky Security Center. La siguiente tabla muestra el conjunto mínimo de derechos de acceso.

Conjunto mínimo de derechos de acceso

Área funcional	Permitir	Negar
Integración de la aplicación	—	✓
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	—	✓
Administración de respuestas	—	✓
Administración de inquilinos	—	✓
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

Los derechos de acceso quedan establecidos.

Ver y editar la configuración de MDR en Kaspersky Security Center

Puede ver y editar en Kaspersky Security Center la configuración del complemento de MDR instalado.

Para ver y editar la configuración:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Ajustes**.
2. Si quiere activar las [notificaciones ampliadas](#) por correo electrónico, active la opción **Active las notificaciones ampliadas por correo electrónico** y seleccione la casilla a continuación para confirmar que ha leído y comprendido los términos de envío de notificaciones ampliadas.
3. Puede utilizar el ajuste **Idioma** para seleccionar el idioma inglés o ruso para mostrar los informes y las notificaciones.
4. Haga clic en el botón **Guardar** en la parte inferior de la ventana para guardar la configuración.
El botón **Guardar** se activa solo si usted cambia la configuración.

Usar funciones del complemento MDR en un Servidor de administración virtual

Para usar las funciones de MDR en Kaspersky Security Center en un Servidor de administración virtual:

- Si utiliza Kaspersky Security Center Windows:
 1. Descargue el [archivo de configuración de MDR](#) en Kaspersky Security Center Web Console o en [Web Console MDR](#).
 2. En Kaspersky Security Center Web Console, seleccione el Servidor de administración principal (físico) donde se encuentra su Servidor de administración virtual.
 3. Active [Kaspersky Private Security Network](#) ☒ en las propiedades del Servidor de administración principal (físico).
 4. Haga clic en el botón **Seleccionar archivo con configuración de Proxy KSN** y seleccione el archivo de configuración de MDR que ha descargado.
- Si utiliza Kaspersky Next Expert View:
 1. Active Kaspersky Managed Detection and Response en el Servidor de administración principal (físico).
 2. En el Servidor de administración principal (físico), haga clic en **Supervisión e informes** → **MDR**, abra la pestaña **Uso de MDR** y asegúrese de que la sección **Archivo de configuración de KPSN para la integración con el Servidor de administración de KSC** contenga el estado y la versión correctos del archivo de configuración de KPSN. Ejemplo de estado y versión correctos:

Para enviar datos de telemetría a la infraestructura Kaspersky MDR, se utiliza el archivo de configuración de KPSN con la versión

Si el estado o la versión del archivo es incorrecto, póngase [en contacto con el Servicio de soporte técnico](#).

Usar funciones de MDR en Kaspersky Security Center mediante un servidor proxy

Si se utiliza un servidor proxy en la red donde se está ejecutando Kaspersky Security Center, debe establecer dos variables de entorno con la configuración del servidor proxy, una para el protocolo HTTP y otra para el protocolo HTTPS para que las funciones de MDR en Kaspersky Security Center funcionen como es debido. Estas variables de entorno se deben configurar en el host donde está instalado Kaspersky Security Center Web Console.

Las variables de entorno tienen el siguiente formato:

`HTTP_PROXY=<protocol>://<proxy_user_name>:<proxy_user_password>@<host>:<port>`

donde:

- <protocol> es http o https.
- <nombre_usuario_proxy> es el nombre de usuario para la autorización en el servidor proxy.
- <contraseña_usuario_proxy> es la contraseña de autorización en el servidor proxy.
- <host>:<port> son el nombre o la dirección IP del servidor proxy y su número de puerto.

Ejemplo de variables de entorno:

```
HTTP_PROXY=http://proxy_user_name:proxy_user_password@proxy.domain.com:8080
HTTPS_PROXY=https://proxy_user_name:proxy_user_password@proxy.domain.com:443
```

Puede establecer las variables de entorno de dos formas:

- Si desea aplicar la configuración del proxy a todas las aplicaciones en el host donde está instalado Kaspersky Security Center Web Console, añada las variables de entorno mediante el componente **Editar las variables de entorno del sistema** del sistema operativo Windows. Para obtener información sobre el uso de este componente, consulte la documentación de la versión del sistema operativo que está utilizando.
- Si desea aplicar esta configuración de proxy solo a Kaspersky Security Center Web Console, agregue estas variables de entorno en el archivo .env ubicado en la carpeta de instalación de Kaspersky Security Center Web Console (de forma predeterminada, C:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center Web Console\). Si la carpeta de instalación no contiene el archivo .env, créelo.

Después de configurar las variables de entorno, debe reiniciar el host donde está instalado Kaspersky Security Center Web Console para que se apliquen los cambios.

Cambiar los certificados para usar las funciones de MDR en Kaspersky Security Center con un servidor proxy o un software antivirus

Debe redefinir la cadena de certificados para la conexión entre Kaspersky Security Center Web Console con el complemento de MDR y la infraestructura de la solución MDR en los siguientes casos:

- En la red donde se ejecuta Kaspersky Security Center, se utiliza un servidor proxy con conexión TLS.
- En un host donde está instalado Kaspersky Security Center Web Console se está ejecutando un software antivirus con cifrado de tráfico TLS.

Para redefinir la cadena de certificados:

1. Guarde los certificados necesarios como archivos en su ordenador.
 - Para guardar el archivo de certificado del software que cifra el tráfico, en el host con Kaspersky Security Center Web Console abra <https://mdr-ksc.kaspersky.com/> en el navegador Chrome, haga clic en el icono de candado en la barra de direcciones junto a la dirección del sitio, haga clic en **La conexión es segura**, luego haga clic en **El certificado es válido**, vaya a la pestaña **Detalles** y haga clic en el botón **Exportar**. Para obtener instrucciones para otros navegadores, consulte la documentación de estos navegadores.
 - Para obtener el certificado que se utiliza para conectarse al servidor proxy, póngase en contacto con el administrador de la red.
2. Añada los certificados guardados al archivo con la extensión .PEM (por ejemplo, KL_Root.pem).
3. Coloque el archivo .PEM creado en la carpeta de instalación de Kaspersky Security Center Web Console (de forma predeterminada, C:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center Web Console\).
4. Agregue la variable de entorno NODE_EXTRA_CA_CERTS al archivo .env ubicado en la carpeta de instalación de Kaspersky Security Center Web Console. Si la carpeta de instalación no contiene el archivo .env, créelo.

Ejemplo de la variable:

```
NODE_EXTRA_CA_CERTS="C:\Archivos de programa\Kaspersky Lab\Kaspersky Security Center Web Console\KL_Root.pem"
```

Para aplicar los cambios después de establecer la variable de entorno, reinicie el host donde está instalado Kaspersky Security Center Web Console.

Ocultar y mostrar las funciones de MDR en Kaspersky Security Center

De forma predeterminada, los elementos de la interfaz relacionados con Kaspersky Managed Detection and Response se muestran en la interfaz de Kaspersky Security Center. Si no utiliza Kaspersky Managed Detection and Response, puede ocultar sus funciones desde la interfaz. Más tarde, puede [cambiar la configuración de la interfaz](#) para mostrar los elementos ocultos nuevamente.

Para ocultar las funciones de MDR en Kaspersky Next Expert View:

1. En Kaspersky Security Center Web Console o Kaspersky Next Expert View, desplace el puntero del ratón sobre su nombre de usuario, en la parte inferior del panel izquierdo. Aparece el menú de configuración de la interfaz.
2. Haga clic en **Opciones de interfaz**.
3. Desactive o active **Mostrar funciones MDR**.
4. Haga clic en el botón **Guardar**.

Kaspersky Security Center guarda el valor de esta opción solo para su cuenta de usuario. Otros usuarios puede establecer un valor diferente.

La sección **MDR** se oculta o se muestra.

MDR Web Console

Puede trabajar con Kaspersky Managed Detection and Response en la interfaz web denominada [MDR Web Console](#).

La ventana de MDR Web Console tiene los siguientes elementos:

- Menú principal en el panel izquierdo de la ventana
- Área de trabajo en el panel derecho de la ventana

Menú principal

El menú principal contiene las siguientes secciones:

- **Monitoring.** Contiene los widgets con información resumida sobre los incidentes, activos y respuestas activos.
- **Incidents.** Contiene información detallada sobre los incidentes y las herramientas para trabajar con ellos.
- **Assets.** Contiene información detallada sobre los activos y las herramientas para trabajar con ellos.
- **Settings.** Contiene las pestañas para trabajar con las cuentas de usuario, notificaciones, configuración de incidentes, informes resumidos, API, inquilinos y la configuración general.
- **About.** Contiene información sobre la solución, enlaces al Contrato de MDR, el Contrato de procesamiento de datos, esta ayuda en línea y el sitio web del Servicio de soporte técnico.

En la parte inferior del panel izquierdo, está el control **Account settings** que le permite acceder a la página *Getting started* (Guía de inicio). Cambie el idioma de la interfaz, acceda a la página de su perfil de usuario y salga de la Web Console MDR.

Área de trabajo

El área de trabajo muestra la información que usted elige ver en la consola web de MDR. El área de trabajo también contiene elementos de control que puede utilizar para configurar cómo se muestra la información.

Cambiar el idioma de la interfaz en Kaspersky Security Center

La interfaz de MDR en Kaspersky Security Center está disponible en los siguientes idiomas:

- Inglés
- ruso
- alemán
- español
- francés
- italiano

Para cambiar el idioma de la interfaz en Kaspersky Security Center:

1. En Kaspersky Security Center Web Console o Kaspersky Next Expert View, en el menú principal, vaya a **Configuración** → **Idioma**.

2. Seleccione uno de los idiomas admitidos.

El idioma cambia.

Si lo desea, puede cambiar a otro idioma en cualquier momento en el futuro.

Cambiar el idioma de las notificaciones y los informes en Kaspersky Security Center

En Kaspersky Security Center puede seleccionar el idioma inglés o ruso para mostrar los datos, las notificaciones y los informes de incidentes.

Para cambiar el idioma de las notificaciones y los informes en Kaspersky Security Center:

1. En Kaspersky Security Center Web Console o Kaspersky Next Expert View, haga clic en **MDR** → **Configuración**.

2. En el área de **Idioma**, seleccione **Ruso** o **Inglés**.

3. Haga clic en el botón **Guardar**.

El idioma cambia.

Si lo desea, puede cambiar a otro idioma en cualquier momento en el futuro.

El cambio de idioma solo se aplica a las nuevas notificaciones e informes. Las notificaciones e informes ya generados conservan el idioma anterior.

Cambiar el idioma de la interfaz en MDR Web Console

La interfaz de MDR Web Console está disponible en los siguientes idiomas:

- Inglés
- Ruso

Para cambiar el idioma de la interfaz de MDR Web Console:

1. En MDR Web Console, navegue hasta la sección **Account settings**, ubicada en la parte inferior del panel izquierdo. Esta sección contiene el área **Language**.
2. En el área **Language**, haga clic en el idioma que desea aplicar a la interfaz de MDR Web Console.

El idioma cambia. Puede cambiar a otro idioma en cualquier momento en el futuro.

Acerca del archivo de configuración de MDR

Kaspersky Managed Detection and Response utiliza un archivo de configuración de MDR para activar la solución en aplicaciones de Kaspersky EPP para estaciones de trabajo (como Kaspersky Endpoint Security para Windows) instaladas en [activos](#).

Kaspersky Managed Detection and Response genera automáticamente el archivo de configuración de MDR cuando un cliente de MDR activa el servicio mediante un código de activación. El archivo de configuración de MDR es un archivo ZIP que contiene los siguientes archivos:

- Archivo de configuración de [KPSN](#).
- Archivo BLOB (P7) para la implementación de aplicaciones EPP que admiten la integración con MDR a través de directivas de Kaspersky Security Center.

El archivo BLOB generado caduca en 5 años, incluso si la licencia es perpetua o se ha emitido para un plazo más largo.

Es posible que no necesite el archivo BLOB (P7) en las siguientes situaciones:

Tenga en cuenta que incluso si no utiliza el archivo de configuración MDR, es necesario activar la solución mediante la consola web MDR o el complemento MDR en Kaspersky Security Center.

- Solo está utilizando las siguientes aplicaciones EPP:
 - Kaspersky Endpoint Security para Windows versión 12.6 o posterior
 - Kaspersky Endpoint Security para Windows versión 12.8 o posterior en el modo Light Agent
 - Kaspersky Endpoint Security para Linux 12.3 o posteriores
 - Kaspersky Endpoint Security for Mac 12.2 o posteriores
- Su organización solo usa el inquilino raíz y nunca creó inquilinos adicionales.
- No está utilizando la solución Kaspersky Endpoint Detection and Response Optimum simultáneamente con la solución Kaspersky MDR. Para obtener más información, consulte [Activación de la solución MDR en las aplicaciones de Kaspersky](#).

En este caso, Kaspersky Endpoint Security para Windows aplica la licencia de Kaspersky Security Center. Si utiliza inquilinos que no sean el inquilino raíz, debe descargar el archivo de configuración de MDR para cada inquilino.

[Descargue el archivo de configuración de MDR](#) y utilícelo según las instrucciones para las aplicaciones EPP instaladas en sus activos:

- [Kaspersky Endpoint Security para Windows](#)
- [Kaspersky Endpoint Security para Windows](#)
- [Kaspersky Endpoint Security para Mac](#)

Acerca de Kaspersky Security Network

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

La solución MDR utiliza Kaspersky Security Network (KSN) para las siguientes tareas:

- Envío de telemetría desde los activos.
- Integración con el servidor de Kaspersky Anti Targeted Attack Platform (EDR).
- Integración con Kaspersky Endpoint Detection and Response Expert dentro de la Open Single Management Platform.

Se instala un archivo de configuración de KPSN cuando configura la integración con Kaspersky Anti Targeted Attack Platform (EDR) o con Kaspersky Endpoint Detection and Response Expert dentro de Open Single Management Platform.

Recomendamos no utilizar un archivo de configuración de KPSN para enviar telemetría desde los activos. Sin embargo, si la configuración no cumple con los [requisitos para operar sin archivos de configuración de KPSN](#), deberá instalar un archivo de configuración de KPSN en el servidor de administración. Para obtener detalles sobre la configuración de KSN, consulte [la documentación de Kaspersky Security Center](#). Para garantizar la transmisión segura de la telemetría del cliente a Kaspersky Managed Detection and Response, Kaspersky actualiza periódicamente las claves de cifrado de los datos de telemetría de MDR. Consulte el siguiente artículo para obtener más detalles: [Actualización periódica de los archivos de configuración de KPSN](#).

Si instala un archivo de configuración de KPSN en el Servidor de Administración de Kaspersky Security Center, KSN se desactiva automáticamente cuando [revoca su consentimiento a los términos de uso de la solución MDR](#).

Si ha añadido manualmente un archivo de configuración de KPSN en el Servidor de administración y no ha activado el complemento MDR para Kaspersky Security Center, debe reemplazar o eliminar manualmente el archivo de configuración de KPSN del Servidor de administración.

Actualización periódica de los archivos de configuración de KPSN

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Recomendamos que configure la solución MDR para que funcione sin utilizar los archivos de configuración de KPSN. Consulte el siguiente artículo para obtener más detalles: [Hacer que la solución MDR pase a funcionar sin archivos de configuración de KPSN](#). Si tiene activos que utilizan archivos de configuración de KPSN, debe actualizar los archivos de configuración de KPSN una vez al año. De lo contrario, los datos de telemetría de estos activos dejarán de enviarse a Kaspersky Managed Detection and Response.

Si actualmente no puede cambiar al modo de funcionamiento sin archivos de configuración de KPSN, consulte la información que aparece a continuación y siga las instrucciones.

Por qué es necesario actualizar los archivos de configuración

Para garantizar la transmisión segura de la telemetría del cliente a Kaspersky Managed Detection and Response, Kaspersky actualiza periódicamente las claves de cifrado de los datos de telemetría de MDR. La clave pública se transmite como parte del archivo de configuración de KPSN.

Si utiliza el complemento de MDR para Kaspersky Next Expert View o Kaspersky Security Center local, en algunos casos (consulte los detalles en la siguiente tabla), el archivo de configuración de KPSN se actualizará automáticamente. Sin embargo, en muchos casos debe reemplazar manualmente el archivo de configuración de KPSN instalado.

A más tardar un mes antes de la caducidad del archivo de configuración actual de KPSN, Kaspersky le notificará sobre la caducidad inminente del archivo de configuración de KPSN. Hay dos opciones de notificación:

- Se creará una incidencia que le notificará sobre la próxima caducidad del archivo de configuración actual de KPSN.
- Se publicará una notificación sobre la próxima caducidad del archivo de configuración actual de KPSN en MDR Web Console. Cualquier usuario que inicie sesión en MDR Web Console verá esta notificación.

La solución que utiliza para administrar sus activos	La interfaz que utilizan sus analistas de SOC	Medidas necesarias
Kaspersky Next Expert View	Complemento MDR instalado en Kaspersky Next Expert View	Inicie sesión en Kaspersky Next Expert View. Al iniciar sesión, el complemento MDR le solicita que acepte el nuevo Acuerdo de KPSN. El archivo de configuración de KPSN se actualizará automáticamente después de que el Administrador acepte el Acuerdo de KPSN. Si el complemento MDR actualiza correctamente el archivo, recibirá una notificación sobre el cambio del archivo de configuración de KPSN. Si el complemento MDR no actualiza el archivo de configuración de KPSN, recibirá una notificación sobre la causa del problema: • Su cuenta no tiene suficientes derechos de acceso para actualizar el archivo. • Ha ocurrido un error inesperado al actualizar el archivo de configuración de KPSN. Si no se muestran notificaciones, es probable que el archivo de configuración de KPSN se haya actualizado correctamente cuando otro especialista se conectó a Kaspersky Next Expert View. Si ve una notificación sobre derechos de acceso insuficientes para actualizar el archivo de configuración de KPSN, póngase en contacto con el administrador de Kaspersky Next Expert View (función Administrador principal) para obtener ayuda: Pida al administrador que se conecte a Kaspersky Next Expert View. Cuando el administrador se conecte, se actualizará el archivo de configuración de KPSN. Puede verificar en cualquier momento si el archivo de configuración de KPSN está actualizado. Para hacerlo, en la sección MDR de Kaspersky Security Center, haga clic en la pestaña Uso de MDR. Se mostrará información sobre la versión actual del archivo de configuración de KPSN. Si hay una nueva versión del archivo de configuración de KPSN disponible, puede usar el botón para actualizar el archivo de configuración de KPSN. Si se produce un error inesperado durante la actualización, póngase en contacto con el soporte técnico de Kaspersky.
Kaspersky Next Expert View	El portal web de MDR, O BIEN , una API para descargar los incidentes con el fin de procesarlos en su propio sistema	Inicie sesión en Kaspersky Next Expert View. Inicie el Asistente de configuración inicial para activar el complemento MDR. Si su cuenta no tiene suficientes derechos de acceso para activar el complemento MDR, póngase en contacto con el administrador del servidor de Kaspersky Next Expert View para obtener ayuda. A continuación, siga las instrucciones anteriores para el servidor de Kaspersky Next Expert View y el complemento MDR. Si se produce un error inesperado durante la actualización, póngase en contacto con el soporte técnico de Kaspersky.
Open Single Management Platform	Complemento MDR instalado en Open Single Management Platform	Cuando un Administrador de MDR inicia sesión en Open Single Management Platform, debe aceptar el nuevo Acuerdo de KPSN. El archivo de configuración de KPSN se actualiza automáticamente después de que el Administrador acepte el Acuerdo de KPSN. Si no se ha aceptado el acuerdo, los usuarios con la función Administrador de MDR pueden aceptarlo más adelante en la consola de OSMP. <i>Para aceptar el acuerdo y actualizar el archivo de configuración de KPSN:</i> 1. En la sección MDR de la interfaz de la Consola OSMP, haga clic en la pestaña Uso de MDR. 2. Expanda el bloque Archivo de configuración de KPSN para la integración con el Servidor de administración de KSC. 3. Active la opción Aceptar acuerdo de KPSN y haga clic en Aplicar el archivo de configuración de KPSN en el Servidor de administración. 4. Además, si ha configurado la integración con Kaspersky Endpoint Detection and Response Expert (local), haga lo siguiente: a. Expanda el bloque Archivo de configuración de KPSN para la integración con KEDR Expert. b. Active la opción Aceptar acuerdo de KPSN y haga clic en Aplicar el archivo de configuración de KPSN para la integridad con KEDR Expert.

La solución que utiliza para administrar sus activos	La interfaz que utilizan sus analistas de SOC	Medidas necesarias
Kaspersky Security Center local versión 14 y posteriores	Complemento MDR instalado en Kaspersky Security Center en los predios del cliente	Inicie sesión en Kaspersky Security Center. Cuando inicia sesión, según la versión del complemento MDR, el archivo de configuración de KPSN se actualiza automáticamente o después de que un usuario con la función Administrador de MDR acepte el nuevo Acuerdo de KPSN. Si el complemento MDR actualiza correctamente el archivo, recibirá una notificación sobre el cambio del archivo de configuración de KPSN. Si el complemento MDR no actualiza el archivo de configuración de KPSN, recibirá una notificación sobre la causa del problema: • Su cuenta no tiene suficientes derechos de acceso para actualizar el archivo. • Ha ocurrido un error inesperado al actualizar el archivo de configuración de KPSN. Si no se muestran notificaciones, es probable que el archivo de configuración de KPSN se haya actualizado correctamente cuando otro especialista se conectó a Kaspersky Next Expert View. Si ve una notificación sobre la falta de derechos de acceso para actualizar el archivo de configuración de KPSN, contacte al administrador del servidor de Kaspersky Security Center para obtener ayuda. Pídale al administrador que se conecte al servidor de Kaspersky Security Center. Cuando el administrador se conecte, se actualizará el archivo de configuración de KPSN. Si el administrador no ve la notificación sobre el cambio del archivo de configuración de KPSN, debe verificar la versión del complemento de MDR instalado y, si es necesario, actualizarlo a la versión vigente (complemento de MDR versión 2.1.17 o posteriores). Puede verificar en cualquier momento si el archivo de configuración de KPSN está actualizado. Para hacerlo, en la sección MDR de Kaspersky Security Center, haga clic en la pestaña Uso de MDR. Se mostrará la información sobre la versión vigente del archivo de configuración de KPSN. Si hay una nueva versión del archivo de configuración de KPSN disponible, puede usar un botón para actualizar el archivo de configuración de KPSN. Si se produce un error inesperado durante la actualización, póngase en contacto con el soporte técnico de Kaspersky.
Kaspersky Security Center local versión 14 o posterior	Portal web de MDR (el complemento de MDR no está instalado en Kaspersky Security Center local), O BIEN, Utiliza una API para descargar los incidentes con el fin de procesarlos en su propio sistema	Solicite al administrador del portal web de MDR que: 1. Descargue el archivo ZIP MDR desde la página Licencias. 2. Extraiga el archivo de configuración de KPSN del archivo ZIP. 3. Envíe este archivo al administrador del servidor de administración de Kaspersky Security Center.
Kaspersky Security Center local versión 13. * o anterior	Complemento MDR instalado en Kaspersky Security Center local O El cliente utiliza la API para descargar las incidencias con el fin de procesarlas en su propio sistema	Solicite al administrador del servidor de Kaspersky Security Center que cargue el archivo de configuración de KPSN haciendo clic en Propiedades del Servidor de administración → Configuración del servidor proxy de KSN → Archivo de configuración del servidor proxy de KSN. Si se produce un error inesperado durante la actualización, póngase en contacto con el soporte técnico de Kaspersky.

Si hay varios servidores de Kaspersky Security Center instalados en su red, debe actualizar el archivo de configuración de KPSN en cada servidor.

Actualizar el archivo de configuración de KPSN en servidores KATA

Si hay servidores KATA conectados a Kaspersky Managed Detection and Response en su red, debe actualizar el archivo de configuración de MDR en estos servidores KATA.

Los pasos para actualizar el archivo de configuración de MDR dependen de la versión de KATA.

Para actualizar el archivo de configuración de MDR en servidores KATA versión 8.0-8.1:

1. Inicie sesión en la interfaz web de KATA con la cuenta de administrador.
2. Seleccione la sección **Configuración** y la subsección **KSN/KPSN y MDR**.
3. En **Integración de MDR**, haga clic en **Iniciar sesión de nuevo**.
4. En la ventana que se abre, introduzca las credenciales de Kaspersky Account.

Después de verificar correctamente las credenciales, el archivo de configuración de MDR se actualiza automáticamente en el servidor.

Para actualizar el archivo de configuración de MDR en servidores KATA versión 7.1 y anteriores:

1. Inicie sesión en la consola de MDR con la cuenta de Administrador de MDR.
2. Descargue el archivo comprimido ZIP de configuración de MDR desde la página **Getting Started**: <https://mdr.kaspersky.com/guide>.
3. Inicie sesión en la interfaz web de KATA con la cuenta de administrador.
4. Seleccione la sección **Configuración** y la subsección **KSN/KPSN y MDR**.
5. En **Integración de MDR**, haga clic en **Cargar** para cargar el archivo de configuración.
Se abre la ventana de selección de archivos.
6. Seleccione el archivo comprimido descargado de Web Console MDR y haga clic en **Abrir**.

El archivo de configuración de MDR se actualiza en el servidor.

En caso de problemas durante la actualización del archivo de configuración MDR, el administrador del servidor KATA debe comunicarse con el Servicio de soporte técnico de Kaspersky para obtener instrucciones sobre cómo actualizar el archivo de configuración MDR en el servidor KATA.

Hacer que la solución MDR pase a funcionar sin archivos de configuración de KPSN

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

La solución MDR debe utilizar la configuración KPSN en los siguientes escenarios:

- Para garantizar que los datos estadísticos y de consultas de KSN nunca se envíen a otra región. Sin la configuración de KPSN, Kaspersky solo garantiza que los datos se remitan a la región especificada. Consulte el siguiente artículo para obtener más detalles: [Actualización periódica de los archivos de configuración de KPSN](#).
- Para garantizar el funcionamiento de la solución MDR cuando se instala una aplicación EPP obsoleta en cualquiera de sus dispositivos.

Puede cambiar la solución MDR para que funcione sin archivos de configuración de KPSN si se cumplen los siguientes requisitos:

1. Las versiones de la aplicación EPP que admiten el funcionamiento sin KPSN están instaladas en todos sus activos:
 - Kaspersky Endpoint Security para Windows versión 12.6 o posteriores
 - Kaspersky Endpoint Security para Windows versión 12.6 o posterior en la configuración de Endpoint Detection and Response Agent
 - Kaspersky Endpoint Security para Windows Light Agent versión 12.8 o posteriores
 - Kaspersky Endpoint Security para Linux 12.3 o posteriores
 - Kaspersky Endpoint Security for Mac 12.2 o posteriores
 - Kaspersky Embedded Systems Security for Windows versión 4.0 o posteriores
 - Kaspersky Embedded Systems Security for Linux versión 4.0 o posteriores
 - Kaspersky Industrial CyberSecurity for Nodes Windows 4.5
2. La solución MDR se activa en todos sus activos con un código de activación o con un archivo BLOB que haya sido creado no antes del 1 de enero de 2024.

Los archivos BLOB que se crearon a partir del 1 de enero de 2024 contienen datos necesarios para el funcionamiento sin KPSN.

Se recomienda utilizar un código de activación para activar la solución MDR para las aplicaciones EPP que la admiten. Ciertas versiones de aplicaciones EPP no admiten el funcionamiento sin KPSN si utiliza un archivo clave para activar la solución MDR. Consulte el siguiente artículo para obtener más información: [Requisitos de hardware y software](#).

Para hacer que la solución MDR pase a funcionar sin KPSN:

1. [Genere y revise un informe de versiones de software de Kaspersky en Kaspersky Security Center](#).
2. Actualice las aplicaciones EPP de conformidad con los requisitos:
 - Kaspersky Endpoint Security para Windows versión 12.6 o posteriores
 - Kaspersky Endpoint Security para Windows versión 12.6 o posterior, modo Agente de Endpoint Detection and Response (requiere la instalación de un archivo BLOB)

- Kaspersky Endpoint Security para Windows Light Agent versión 12.8 o posteriores
- Kaspersky Endpoint Security para Linux 12.3 o posteriores
- Kaspersky Endpoint Security for Mac 12.2 o posteriores
- Kaspersky Embedded Systems Security for Windows versión 4.0 o posteriores
- Kaspersky Industrial CyberSecurity for Nodes Windows 4.5

3. Desactivar el uso de KPSN en el servidor de administración.

- En las instancias de Kaspersky Security Center que utilicen el complemento MDR:

1. Asegúrese de que el complemento MDR esté actualizado a la versión 2.5.1.
2. Para hacerlo, en la sección MDR de Kaspersky Security Center, haga clic en la pestaña **Uso de MDR**.
3. Expanda el bloque **KPSN** y haga clic en **Desactivar KPSN**.

- En las instancias de Kaspersky Security Center que no utilicen el complemento MDR:

1. En el menú principal, haga clic en el icono de configuración () junto al nombre del Servidor de Administración requerido.
2. Se abre la ventana de propiedades del Servidor de administración.
3. En la pestaña **General**, seleccione la sección Configuración del proxy de KSN.
4. Desactive la opción **Usar Kaspersky Private Security Network**.
5. Active la opción **Activar proxy de KSN en el servidor de administración**.

4. Si implementa activos desde una imagen del sistema operativo, realice una actualización de la imagen para que la aplicación EPP no utilice la configuración de KPSN.

5. Edite las directivas para las aplicaciones EPP (necesarias tanto para el uso del código de activación como para los escenarios de uso de archivos BLOB).

1. Desactive el uso de Kaspersky Security Network y guarde la directiva. Consulte este artículo para obtener más información: [Configuración de Kaspersky Security Network](#) ².
2. Si la aplicación EPP solo se puede activar con un archivo BLOB, [descargue el archivo de configuración MDR](#) y cargue el archivo BLOB a la directiva.
3. Vuelva a activar el uso de Kaspersky Security Network y acepte el Acuerdo de KSN. Asegúrese de que la opción Forzar esté activada en la configuración de la directiva.

Supervisar paneles en MDR Web Console

MDR Web Console proporciona paneles de supervisión para ver información resumida.

Para ver los paneles:

1. En la ventana Consola, navegue hasta el elemento del menú **Monitoring**.

Se abre la página **Summary**.

2. Los siguientes paneles están presentes en la página **Summary**:

- **Number of connected assets**

Esta sección muestra el número de activos conectados frente al número objetivo de activos.

- **Assets by status**

Este es un gráfico circular que muestra la distribución de los activos, según sus estados.

- **Active incidents**

Gráfico circular que muestra la distribución de los incidentes activos, según sus estados.

- **Responses**

Gráfico circular que muestra la distribución de las respuestas, según sus estados.

El número de activos conectados representa los activos que se vieron en MDR Web Console en los últimos 7 días. Si desea consultar el número de activos conectados en un período de tiempo específico, navegue hasta el elemento del menú **Assets** de MDR Web Console.

- **Telemetry statistics**

Este es un panel que muestra las estadísticas de telemetría de la solución MDR para un cliente, incluidas las estadísticas de inquilinos específicos. Puede ver datos de 1, 7, 30, 90, 180 días, de 1 año o de todo el período en el que un cliente utiliza continuamente la solución MDR.

Este panel muestra el número de cada uno de los siguientes objetos:

- Los *Telemetry events** son todos los eventos que se envían desde los activos de un cliente a Kaspersky Managed Detection and Response.
- Los *Suspicious events* son eventos de telemetría que Kaspersky Managed Detection and Response determina como eventos que requieren una verificación adicional.
- Los *Security events* son eventos de telemetría que las reglas de detección determinan como posibles incidentes.
- Los *Incidents* son acciones que la tecnología de detección determina como críticas. Los incidentes requieren una reacción inmediata (acción de respuesta) de Kaspersky Managed Detection and Response.
- *Detection rules triggered* son una serie de reglas de detección únicas que se activan en eventos de telemetría especificados durante un período especificado.

Los paneles se actualizan cada vez que se actualiza la página **Summary**.

Para cambiar los paneles a estadísticas específicas del inquilino:

1. En la parte superior de la página **Summary**, haga clic en **Filtrar**.
2. En el menú que aparece, seleccione uno o varios inquilinos.
3. Haga clic en **Save**.

Las estadísticas específicas de cada inquilino están disponibles para los siguientes widgets:

- **Assets limit for this license**
- **Assets by status**
- **Active incidents**
- **Incidents**
- **Responses**
- **Telemetry statistics**

Recepción de información resumida

Kaspersky Managed Detection and Response proporciona varios tipos de información resumida que puede recibir por correo electrónico. En esta sección se describe cómo configurar la recepción de información resumida.

Recibir un resumen de todos los activos en formato CSV (MDR Web Console)

Puede recibir un resumen en formato CSV con información sobre todos los activos de su cuenta. No se aplican filtros al resumen, es decir, la cantidad de activos en este resumen corresponde a la de todos los activos que se vieron en MDR Web Console.

Puede ocultar los activos con estado **Ausente** en el resumen marcando la casilla correspondiente en **Configuración**.

Para recibir un resumen en CSV:

1. En MDR Web Console, navegue hasta el elemento del menú **Assets**.

Se abre la lista de activos.

2. Haga clic en el botón **Receive a CSV summary by email** en la parte superior de la ventana.

El resumen se envía a la dirección de correo electrónico que especificó durante la activación de Kaspersky Managed Detection and Response.

Recibir información del incidente en un documento PDF (MDR Web Console)

Puede recibir información resumida sobre un incidente en particular en formato PDF.

Para recibir un resumen en PDF:

1. En la ventana de la Consola, navegue hasta el elemento **Incidents** del menú.

Se abre la lista de incidentes.

2. Haga clic en el incidente con el incidente cuyo resumen desea recibir.

Aparece la tarjeta de incidentes.

3. Haga clic en el botón **Receive a PDF by email** en la parte superior de la ventana.

El resumen se envía a la dirección de correo electrónico que especificó durante la activación de Kaspersky Managed Detection and Response.

Configurar envío regular de informes en MDR Web Console

Esta función solo está disponible en MDR Web Console.

Puede programar recibir un informe resumido que contenga datos sobre los incidentes abiertos. Cada conjunto de parámetros de entrega se guarda como una programación. Puede crear hasta 50 programaciones para una organización y hasta 10 programaciones para cada inquilino.

Para crear o editar programaciones de entrega de informes, debe tener la [función de usuario Administrador de MDR](#).

El informe se envía por correo electrónico en formato PDF abierto y no cifrado a las direcciones que ha especificado y según la programación definida.

El informe siempre contiene datos de los últimos siete días. El día de generación del informe no se incluye. En otras palabras, si configura recibir el informe resumido cada día, su informe diario contendrá datos de los siete días anteriores, excluyendo el día en curso. Si configura recibir el informe resumido cada miércoles, este contendrá datos desde el miércoles anterior hasta el siguiente martes.

Para configurar la recepción del informe resumido como PDF:

1. En la sección **Settings** de la consola web de MDR, haga clic en la pestaña **Schedules**.

2. Haga clic en el botón **Add**.

Se abre la ventana **Add new schedule**.

3. Encienda el interruptor de palanca a la posición **Enabled**.

4. Lea atentamente la notificación de abajo acerca de los términos y condiciones de envío de los informes resumidos. A continuación, marque la casilla para confirmar que ha leído y comprendido los términos y condiciones. Si la casilla no está marcada, no podrá guardar los cambios que realice.

5. Especifique la siguiente configuración:

- En el campo **Schedule name**, asigne al informe resumido un nombre comprensible para humanos. El nombre puede contener letras latinas, dígitos y caracteres especiales; no puede tener más de 1000 caracteres.
- En el campo **Tenant**, seleccione el inquilino cuyo informe resumido desea recibir. El informe solo contendrá datos del inquilino seleccionado. Como alternativa, si desea recibir un informe resumido sobre todos los inquilinos, seleccione **All tenants**.

- En el campo **To emails**, especifique una dirección de correo electrónico (o una lista de direcciones de correo electrónico separadas por comas) de los usuarios que recibirán el resumen.

Verifique bien las direcciones de correo electrónico ingresadas, ya que se añadirán sin más confirmaciones. Los informes resumidos pueden contener datos confidenciales y se enviarán en formato PDF abierto y sin cifrar.

- En el campo **Sending day**, seleccione el día de la semana en el que se debe enviar el resumen a los correos electrónicos especificados. Puede elegir un día o **Every day**.
- En el campo **Time, UTC**, especifique la hora en formato UTC de 24 horas. Por ejemplo, 15:00.

La programación solo afecta a la hora en que se recibe el informe, pero no al período de datos en el informe.

El informe siempre contiene datos de los últimos siete días. El día de generación del informe no se incluye. En otras palabras, si configura recibir el informe resumido cada día, su informe diario contendrá datos de los siete días anteriores, excluyendo el día en curso. Si configura recibir el informe resumido cada miércoles, este contendrá datos desde el miércoles anterior hasta el siguiente martes.

6. Haga clic en el botón **Guardar**.

El resumen se envía a la dirección (o direcciones) de correo electrónico especificada cada día o cada semana.

Recepción de notificaciones

Puede configurar la entrega de notificaciones sobre los eventos que ocurren con incidentes y respuestas, a medida que se procesan en Kaspersky Managed Detection and Response.

Kaspersky Managed Detection and Response envía notificaciones a los clientes a través de Telegram o correo electrónico, según los ajustes que haya especificado. El cuerpo de la notificación contiene una descripción del evento y un enlace al objeto donde ocurrió el evento.

Puede configurar las notificaciones en Web Console MDR.

Configurar notificaciones en MDR Web Console

Para configurar la entrega de notificaciones en MDR Web Console:

1. En la sección **Settings** de la Consola, haga clic en la pestaña **Notification settings**.
2. Seleccione las casillas correspondientes a los eventos cuyas notificaciones desea recibir por correo electrónico o Telegram.

Las casillas disponibles son:

- **All:** todos los eventos sobre los que Kaspersky Managed Detection and Response envía notificaciones.
 - **Incidents:** notificaciones sobre la creación, actualización, resolución y cierre de incidentes.
 - **Extended notifications:** descripción del ataque detectado como parte del incidente y recomendaciones sobre cómo responder. Esta casilla está disponible si la función de notificaciones ampliadas [está activada en la pestaña General settings](#). Estas notificaciones solo se pueden habilitar en Web Console MDR, pero no en el complemento MDR.
 - **Comments:** notificaciones sobre la creación, actualización y eliminación de comentarios dentro de los incidentes.
 - **Responses:** notificaciones sobre la creación, aceptación y rechazo de respuestas.
 - **Information on license expiration:** describe los siguientes eventos: faltan menos de 30 días para que caduque la licencia, licencia ha caducado. Kaspersky Managed Detection and Response envía estas notificaciones todos los días, pero no después de que la licencia expira o es renovada.
3. Haga clic en el botón **Subscribe** ubicado sobre las casillas para suscribirse a las notificaciones del bot de Telegram. Al hacer clic en el botón **Subscribe**, la aplicación genera y muestra un enlace único para activar el bot de chat en Telegram. Puede usar este enlace para una sola cuenta de Telegram.

Use este enlace solo en un dispositivo (escritorio o móvil) donde esté instalada la aplicación Telegram. El enlace no puede activar el chatbot en la versión web de Telegram.

Si desea recibir notificaciones en otra cuenta de Telegram, haga clic en el botón **Unsubscribe** y luego repita el procedimiento de suscripción para generar un nuevo enlace. Utilícelo para activar el bot de chat para otra cuenta.

4. Haga clic en el botón **Save** en la parte inferior de la ventana para guardar la configuración. El botón **Save** se activa solo si usted cambia la configuración.

La entrega de notificaciones queda configurada.

Notificaciones sobre el estado de los activos

Puede configurar la entrega de notificaciones cuando el número de activos con un estado específico supere un umbral.

Las notificaciones del estado de los activos le permiten recibir información puntual sobre los siguientes problemas:

- Disminución de la cobertura de supervisión de MDR
- Problemas de conexión de activos con MDR
- Transición masiva de activos a estados de advertencia o críticos

Para obtener información detallada sobre los estados de los activos, consulte el siguiente artículo: [Estados de los activos](#).

Cómo funcionan las notificaciones automáticas

Para cada uno de los estados enumerados a continuación, puede establecer un valor de umbral como porcentaje del número total de activos. Cuando se supera el umbral, se envía una notificación.

Estado	Condición
Aceptar	El número de activos está por debajo del umbral.
Advertencia	El número de activos está por encima del umbral.
Crítico	El número de activos está por encima del umbral.
Sin conexión	El número de activos está por encima del umbral.

Las comprobaciones automáticas de activos se realizan con un intervalo de 1 hora.

Las notificaciones se envían por separado para cada inquilino que supera sus umbrales. No se envía más de una notificación para un estado determinado al día por inquilino.

Solo reciben las notificaciones los usuarios que tienen acceso al inquilino cuyos umbrales se han superado y que han activado las notificaciones en su configuración de usuario.

Configuración de reglas de notificación por parte del Administrador de MDR

Para configurar las notificaciones de estado de los activos, se requiere la función de Administrador de MDR.

Para configurar reglas de notificación de estado de los activos:

1. En la consola de MDR, vaya a **Configuración** → **Configuración general**.
2. Active una o ambas de las siguientes opciones:
 - **Recibir notificaciones ampliadas por correo electrónico**
 - **Recibir notificaciones ampliadas por Telegram**
3. Active el parámetro **Activar notificaciones de cambios de estado de los activos**.

El panel **Regla base** pasa a ser editable y contiene la configuración de la regla de notificación. Puede añadir reglas adicionales (por ejemplo, para otro conjunto de inquilinos) haciendo clic en el botón **Añadir regla** situado debajo del panel **Regla base**.
4. En el panel, seleccione los inquilinos a los que se aplicará la regla o active **Aplicar a todos los inquilinos**.
5. Establezca los valores de umbral para los estados de los activos o mantenga los valores predeterminados.
6. Haga clic en **Guardar**.

La regla se ha creado y está activa. Para recibir notificaciones, los usuarios de MDR deben configurar las notificaciones de estado de los activos como se describe a continuación.

Configuración de notificaciones de estado de los activos por parte de los usuarios de MDR

Para recibir notificaciones de estado de los activos:

1. En la consola de MDR, vaya a **Configuración** → **Configuración de notificaciones**.
2. Active **Notificaciones de estado de los activos**.
3. Haga clic en **Guardar**.

Ahora recibirá notificaciones de estado de los activos de los inquilinos a los que tiene acceso, de acuerdo con las reglas configuradas.

Recibir notificaciones ampliadas

Puede configurar la entrega de notificaciones de incidentes ampliados por correo electrónico a los usuarios de MDR. Las notificaciones ampliadas contienen una descripción del ataque detectado como incidente y las recomendaciones de respuesta. La descripción del ataque incluye algunos datos que la solución MDR recibe como telemetría de los dispositivos conectados a la solución MDR, por lo que la descripción puede incluir la siguiente información confidencial:

- Nombres de hosts
- Direcciones IP de host
- Nombres de cuentas
- Contraseñas de cuentas (si en un dispositivo se ejecutó un script que contiene una contraseña)
- URL de servicio
- Nombres de archivos
- Direcciones de correo electrónico
- Nombres de los departamentos e inquilinos

La lista completa de los datos que recibe la solución MDR se encuentra en la sección [Provisión de datos](#).

Habilitar notificaciones ampliadas en MDR Web Console

Para habilitar la entrega de notificaciones extendidas:

1. En la sección **Settings** de MDR Web Console, haga clic en la pestaña **General settings**.
2. Active una o ambas opciones:
 - **Enable extended email notification**
 - **Enable extended Telegram notification**
3. Marque la casilla en la parte inferior del panel para confirmar que ha leído y comprendido los términos del envío de notificaciones ampliadas.
4. Haga clic en el botón **Save**.

Ahora puede [suscribirse](#) a notificaciones extendidas en la **Notification settings** de la consola web de MDR.

Administrar usuarios

Los usuarios de Kaspersky Managed Detection and Response pueden tener diferentes funciones, con una funcionalidad diferente disponible para cada función. El *modelo de función* es un conjunto de reglas que especifican las funciones de los usuarios.

Las siguientes funciones están presentes en Kaspersky Managed Detection and Response:

MDR Administrator

Superusuario que tiene acceso a todas las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia. El administrador de MDR puede otorgar acceso a los orígenes de datos del cliente a otros usuarios. Cuando activa Kaspersky Managed Detection and Response, usted se convierte automáticamente en el administrador de MDR. Por esto, le recomendamos utilizar una dirección de correo electrónico corporativa para el proceso de activación y no una dirección de correo electrónico personal. Crear el Administrador de MDR con una dirección de correo electrónico personal puede suponer riesgos de seguridad, como el robo de la cuenta de Administrador de MDR.

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	✓	—
Administración de respuestas	✓	—
Administración de inquilinos	✓	—
Información consolidada sobre incidentes	✓	—
Acceso a la API de REST	✓	—

Senior Security Officer

Empleado que tiene acceso a las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia, pero que no tiene acceso a la API de REST. El Director de seguridad tiene derecho a aceptar y rechazar [respuestas](#).

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	✓	—
Administración de respuestas	✓	—
Administración de inquilinos	—	✓
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

Security Officer

Empleado que tiene acceso a las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia, pero que no tiene acceso a la API de REST. El Encargado de seguridad no puede aceptar ni rechazar [respuestas](#).

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	—	✓
Administración de respuestas	—	✓
Administración de inquilinos	—	✓
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

Invitar a nuevos usuarios en MDR Web Console

Para invitar a un nuevo usuario a Kaspersky Managed Detection and Response:

Si una cuenta de [Kaspersky Account](#) creada anteriormente (con su correo electrónico) se ha utilizado para acceder a Kaspersky Managed Detection and Response, podría estar asociada con los datos de MDR de otra organización y no estar disponible para activar un nuevo código de activación. Para usar su cuenta de Kaspersky Account existente para la nueva activación, comuníquese con el [Servicio de soporte técnico](#). Tenga en cuenta: cuando el personal del Servicio de soporte técnico elimina la asociación de su Cuenta de Kaspersky existente con los datos de otra organización en MDR, su Cuenta de Kaspersky existente ya no se puede usar para acceder a los datos de la otra organización.

1. En la ventana de MDR Console, navegue hasta el elemento **Settings** del menú.

Se abre la lista de usuarios.

2. Haga clic en el botón **Add** ubicado encima de la lista de usuarios.

Aparece la tarjeta de invitación.

3. En el campo **Email**, especifique una dirección de correo electrónico.

4. En el campo **User role**, especifique una función para el nuevo usuario.

Están disponibles los siguientes roles de usuario:

MDR Administrator

Superusuario que tiene acceso a todas las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia. El administrador de MDR puede otorgar acceso a los orígenes de datos del cliente a otros usuarios. Cuando activa Kaspersky Managed Detection and Response, usted se convierte automáticamente en el administrador de MDR. Por esto, le recomendamos utilizar una dirección de correo electrónico corporativa para el proceso de activación y no una dirección de correo electrónico personal. Crear el Administrador de MDR con una dirección de correo electrónico personal puede suponer riesgos de seguridad, como el robo de la cuenta de Administrador de MDR.

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	✓	—
Administración de respuestas	✓	—
Administración de inquilinos	✓	—

Área funcional	Permitir	Negar
Información consolidada sobre incidentes	✓	—
Acceso a la API de REST	✓	—

Solo un usuario con el [rol](#) **MDR Administrator** asignado puede asignar el rol **MDR Administrator** a un nuevo usuario.

Senior Security Officer

Empleado que tiene acceso a las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia, pero que no tiene acceso a la API de REST. El Director de seguridad tiene derecho a aceptar y rechazar [respuestas](#).

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	✓	—
Administración de respuestas	✓	—
Administración de inquilinos	—	✓
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

Security Officer

Empleado que tiene acceso a las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia, pero que no tiene acceso a la API de REST. El Encargado de seguridad no puede aceptar ni rechazar [respuestas](#).

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	—	✓
Administración de respuestas	—	✓
Administración de inquilinos	—	✓
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

5. Si es necesario, seleccione el valor (o valores) en la lista desplegable **Tenant**.

Se sugieren los inquilinos que ya existen y que tienen el valor **Root tenant**.

El usuario puede ver solo los activos e incidentes relacionados con los inquilinos especificados. Si tiene activos e incidentes que no estén asignados a ningún inquilino, el usuario puede verlos si usted selecciona el valor **Root tenant**.

Puede seleccionar el valor **Root tenant** además de especificar los nombres de los inquilinos.

6. Haga clic en **Invite**.

La tarjeta de invitación desaparece.

Ingresa la dirección de correo electrónico. La dirección de correo electrónico primero debe registrarse y verificarse en el portal web auth.hq.uis.kaspersky.com.

Se envía un mensaje con el enlace de invitación desde noreply@mail.account.uis.kaspersky.com a la dirección de correo electrónico especificada.

El usuario invitado debe verificar su dirección de correo electrónico siguiendo el enlace del mensaje. El usuario no puede iniciar sesión y utilizar Kaspersky Managed Detection and Response si no verifica su correo electrónico. Los permisos correspondientes a la función del usuario se otorgarán después del primer inicio de sesión del usuario.

Cambiar las funciones de usuario en MDR Web Console

Puede cambiar la función de un usuario existente. Por ejemplo, un empleado con la función de Director de seguridad asignado obtiene responsabilidades adicionales que requieren que se le asigne la función de Director senior de seguridad.

Para cambiar una función para un usuario existente:

1. En la ventana de MDR Console, navegue hasta el elemento **Settings** del menú.
Se abre la lista de usuarios.
2. Haga clic en la cadena que contiene el usuario cuya función desea cambiar.
Aparece la tarjeta de usuario.
3. En la tarjeta de usuario, cambie la función del usuario existente seleccionando otro rol de la lista desplegable de roles.
4. Haga clic en **Guardar**.

Se cambia la función de usuario existente.

Editar métodos de notificación de usuario en MDR Web Console

La modificación de métodos de notificación de usuarios está disponible solo para el usuario que tenga asignada la [función](#) de administrador de MDR. El usuario con esa función puede modificar la configuración de notificaciones de todos los usuarios con el estado activo, incluido él mismo.

Los usuarios con el estado activo pueden recibir notificaciones de Kaspersky Managed Detection and Response por correo electrónico y/o Telegram.

Para modificar los métodos de notificación de usuario para un usuario existente:

1. En la ventana de MDR Console, navegue hasta el elemento **Settings** del menú.
Se abre la lista de usuarios.
2. Haga clic en la cadena que contiene el usuario cuyos métodos de notificación desea cambiar.
Aparece la tarjeta de usuario.

3. En la tarjeta de usuario, especifique las siguientes opciones:

- **Email notifications enabled**

El usuario recibe notificaciones a la dirección de correo electrónico especificada cuando se invitó a este usuario.

- **Telegram notifications enabled**

El usuario recibe notificaciones del bot de Telegram.

Si un usuario ha perdido el acceso a la cuenta de Telegram, marque la casilla **Unsubscribe Telegram account from notifications**. Luego, solicite al usuario que inicie sesión en MDR Web Console, vaya a **Settings** → **Notification settings** y repita el procedimiento de suscripción para generar un nuevo enlace para activar la suscripción de otra cuenta de Telegram.

4. En la parte inferior de la tarjeta de usuario, haga clic en el botón **Save** para cerrar la tarjeta.

Los métodos de notificaciones de usuario quedan modificados y se guardan.

Editar el acceso de los usuarios a los inquilinos en MDR Web Console

Puede cambiar el acceso de los usuarios a los inquilinos de su cuenta, por ejemplo, si agrega un nuevo inquilino y desea que un usuario existente tenga acceso a él.

Para cambiar el acceso a los inquilinos:

1. En la ventana de MDR Console, navegue hasta el elemento **Settings** del menú.

Se abre la lista de usuarios.

2. Haga clic en la cadena que contiene el usuario cuyos derechos de acceso desea cambiar.

Aparece la tarjeta de usuario.

3. En la tarjeta de usuario, cambie el valor (o valores) en la lista desplegable **Tenant**.

4. En la parte inferior de la tarjeta de usuario, haga clic en el botón **Save** para cerrar la tarjeta.

El acceso de los usuarios a los inquilinos queda cambiado.

Eliminar cuentas de usuario

La eliminación de cuentas de usuario está disponible en la consola de MDR y en el sitio web de Kaspersky.

Eliminación de cuentas de usuario de MDR en la consola de MDR

Se requiere una cuenta de Administrador de MDR para eliminar cuentas de usuario de MDR.

El correo electrónico asociado a una cuenta eliminada deja de recibir notificaciones e informes. Para restaurar el acceso a la consola de MDR, [debe enviarse una nueva invitación al correo electrónico](#).

Si solo dispone de una cuenta de Administrador de MDR, esta no se puede eliminar.

Para eliminar una cuenta de usuario de MDR:

1. En la ventana de MDR Console, navegue hasta el elemento **Settings** del menú.
Se abre la lista de usuarios.
2. En la lista de usuarios, sitúe el puntero del ratón sobre el usuario que desea eliminar y haga clic en el icono de la papelera situado a la derecha.
Aparece la ventana **Confirm user deletion**.
3. Haga clic en el botón **Delete** para eliminar al usuario.

Eliminación de cuentas de Kaspersky Account

Los usuarios pueden eliminar su propia Kaspersky Account en el sitio web de Kaspersky independientemente de los derechos de usuario asignados.

Al eliminar una Kaspersky Account, se elimina automáticamente la cuenta de usuario de MDR correspondiente. El correo electrónico asociado a la Kaspersky Account eliminada deja de recibir notificaciones e informes de MDR.

Si se eliminan todas las cuentas de usuario de Administrador de MDR, ya no se podrán añadir nuevos usuarios ni configurar la consola de MDR. En este caso, [póngase en contacto con el Soporte técnico](#).

Si elimina la Kaspersky Account que se utilizó para configurar el complemento de MDR en el Servidor de administración o en Open Single Management Platform, deberá volver a configurar el complemento de MDR.

Administrar activos

Un *activo* con una aplicación Kaspersky EPP instalada (por ejemplo, Kaspersky Endpoint Security para Windows). Esta sección proporciona información sobre la visualización, clasificación y filtrado de activos.

Ver y buscar activos en MDR Web Console

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Puede ver y buscar en los activos disponibles utilizando la lista de activos.

Para ver activos:

1. En la ventana de MDR Web Console, navegue hasta el elemento del menú **Assets**.

Se abre la lista de activos. Cada línea representa un activo. Puede hacer clic en cualquier parte de la línea para ver la información del activo.

Los siguientes atributos de activos están disponibles para mostrarse encima de la lista:

Asset name

Nombre de red de un equipo.

Puede hacer clic en **Asset name** para ver la información del activo en Kaspersky Security Center Web Console.

Asset ID

Identificador único de un activo. Kaspersky Managed Detection and Response genera automáticamente el id. de activo antes de que el activo envíe telemetría por primera vez.

Applications

Aplicación Endpoint Protection Platform (EPP) que está instalada en el activo y configurada para su uso con Kaspersky Managed Detection and Response.

Interfaces

Número de todas las interfaces de red disponibles del dispositivo.

Operating system

Sistema operativo que está instalado en el activo.

Domain

Dominio de red al que pertenece el activo.

Tenant

Nombre del [inquilino](#), si el activo pertenece a uno de los inquilinos. Si el activo no pertenece a un inquilino, el campo está en blanco.

Last seen

Cantidad de días desde la última vez que se vio el activo en la Web Console MDR.

Los activos se ordenan según este atributo, en orden descendente.

De forma predeterminada, se muestran los activos que se vieron en los últimos 30 días. Puede ampliar el intervalo de tiempo filtrando activos.

Status

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

El estado refleja la condición actual del activo. Para los activos con los estados *Correcto*, *Advertencia* o *Crítico*, la aplicación también enumera los problemas (si los hay) de las últimas 72 horas.

Los activos tienen uno de los siguientes estados:

- **OK** (verde)

La telemetría se está enviando, la protección está completamente operativa.

- **Warning** (amarillo)

Posibles razones del estado **Warning**:

- Pequeñas pérdidas de telemetría. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Las bases de datos antivirus están desactualizadas desde hace más de 7 días.
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

Firewall

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protección frente a amenazas en la red

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protección frente a amenazas en el correo y extensión adicional para Microsoft Office Outlook

En el siguiente artículo se describe cómo activar o configurar este componente: [Kaspersky Endpoint Security para Windows](#) [↗].

Protección frente a amenazas web

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Endpoint Security for Linux](#) [↗]
- [Kaspersky Endpoint Security para Mac](#) [↗]
- [Kaspersky Security para Virtualization Light Agent](#) [↗]
- [Kaspersky Embedded Systems Security para Linux](#) [↗]

Autodefensa del producto

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Security para Virtualization Light Agent](#) [↗]
- [Kaspersky Embedded Systems Security para Windows](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]

Estos componentes afectan la integridad de la telemetría que se envía. Si un componente está desactivado o ausente, Kaspersky Managed Detection and Response no envía los eventos de telemetría relacionados con este componente. La aplicación EPP instalada podría no incluir todos los componentes enumerados.

- El archivo de configuración de KPSN está por caducar. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#). Si continúa trabajando con el archivo de configuración actual, el estado cambiará a **Critical** algunos días antes de la fecha de caducidad.

El estado **Warning** se aplica a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(EDR Agent\)](#) [↗], este estado no se muestra.

- **Critical** (rojo)

Posibles razones del estado **Critical**:

- Grandes pérdidas de telemetría. Los datos de telemetría son insuficientes para el análisis. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

- **System Watcher o Detección de comportamiento**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 

- **Protección frente a amenazas en archivos**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si alguno de estos componentes está desactivado o ausente, Kaspersky Managed Detection and Response deja de enviar telemetría desde el activo. Es posible que la aplicación EPP instalada no incluya todos los componentes enumerados.

- El archivo de configuración de KPSN caduca pronto o ya ha caducado. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#).

Este estado es aplicable a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(Agente de EDR\)](#) , este estado no se muestra.

- **Offline (negro)**

Sin telemetría durante más de 7 días (valor predeterminado) Puede cambiar el número de días de ausencia de telemetría, después de lo cual se muestra el estado **Offline** para el activo, en la sección **Configuración**. El rango disponible es de 2 a 29 días.

Si ve que sus activos tienen el estado **Offline**:

- Asegúrese de que los componentes de la aplicación EPP enumerados en los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

El estado **Offline** no se aplica a los activos de VDI (máquinas virtuales temporales).

- **Absent** (negro)

Sin telemetría durante más de 30 días para activos físicos o durante más de 24 horas para activos VDI (máquinas virtuales temporales).

Si ve que sus activos tienen el estado **Absent**:

- Asegúrese de que los componentes de la aplicación EPP con los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

Puede ocultar los activos con estado **Absent** en la [lista de activos](#), en los [informes](#) y en los datos recibidos a través de la [interfaz de API](#).

En la parte superior de la lista de incidentes se encuentran los siguientes botones:

- El botón **Columns** con el icono de engranaje, que sirve para seleccionar qué columnas mostrar en la pestaña **History**.
- El botón **Filter** con el icono de embudo, que sirve para mostrar los cambios relacionados solo con las casillas marcadas.
- El botón **Search** con el icono de lupa, que sirve para mostrar los cambios relacionados solo con las palabras o caracteres ingresados.

2. Si desea cambiar el número de activos que se muestran por página de la lista, seleccione el número haciendo clic en la opción **entries per page** en la parte inferior de la página.

Puede seleccionar 10, 20 o 50 activos por página.

Puede ocultar los activos con estado **Absent** en la lista de activos. Para hacerlo, marque la casilla correspondiente en la pestaña **Settings** → **General settings**.

Si desea navegar por la lista de activos, seleccione la página utilizando los controles de paginación ubicados debajo de la lista. Puede utilizar las opciones **Previous** y **Next** para cambiar entre páginas adyacentes.

De manera predeterminada, la lista de activos contiene los activos que se vieron en la Web Console MDR en los últimos 30 días.

Para cambiar este período:

1. Haga clic en el icono del embudo que se encuentra sobre la lista.
2. En el panel **Filter** de la derecha, seleccione el período en el campo **Last seen**.
3. Haga clic en **Save**.

Puede buscar entre los activos haciendo clic en el icono de lupa junto al icono de embudo sobre la lista de activos.

Filtrar activos en MDR Web Console

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Puede crear filtros y aplicarlos a la lista de activos.

Para crear un filtro para la lista de activos:

1. En MDR Web Console, navegue hasta el elemento del menú **Assets**.
Se abre la lista de activos.
2. Haga clic en el icono de embudo que se encuentra sobre la lista de activos.
Aparece el menú **Filter**.
Los parámetros disponibles para el filtrado son:

- **Last seen**

El momento en el que se vio el activo por última vez en la Web Console MDR.

- **Asset name**

Nombres de activos disponibles.

El nombre del activo es el nombre de la red de un equipo.

- **Tenant**

Nombres de inquilinos disponibles.

Puede seleccionar el valor **Root tenant** para ver los activos que no están asignados a ninguno de sus inquilinos.

Puede seleccionar el valor **Root tenant** además de especificar los nombres de los inquilinos.

- **Status**

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

El estado refleja la condición actual del activo. Para los activos con los estados *Correcto*, *Advertencia* o *Crítico*, la aplicación también enumera los problemas (si los hay) de las últimas 72 horas.

Los activos tienen uno de los siguientes estados:

- **OK** (verde)

La telemetría se está enviando, la protección está completamente operativa.

- **Warning** (amarillo)

Posibles razones del estado **Warning**:

- Pequeñas pérdidas de telemetría. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Las bases de datos antivirus están desactualizadas desde hace más de 7 días.
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

Firewall

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protección frente a amenazas en la red

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protección frente a amenazas en el correo y extensión adicional para Microsoft Office Outlook

En el siguiente artículo se describe cómo activar o configurar este componente: [Kaspersky Endpoint Security para Windows](#) .

Protección frente a amenazas web

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 

- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 

Autodefensa del producto

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Estos componentes afectan la integridad de la telemetría que se envía. Si un componente está desactivado o ausente, Kaspersky Managed Detection and Response no envía los eventos de telemetría relacionados con este componente. La aplicación EPP instalada podría no incluir todos los componentes enumerados.

- El archivo de configuración de KPSN está por caducar. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#). Si continúa trabajando con el archivo de configuración actual, el estado cambiará a **Critical** algunos días antes de la fecha de caducidad.

El estado **Warning** se aplica a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(EDR Agent\)](#) , este estado no se muestra.

• Critical (rojo)

Posibles razones del estado **Critical**:

- Grandes pérdidas de telemetría. Los datos de telemetría son insuficientes para el análisis. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

• System Watcher o Detección de comportamiento

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 

- **Protección frente a amenazas en archivos**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si alguno de estos componentes está desactivado o ausente, Kaspersky Managed Detection and Response deja de enviar telemetría desde el activo. Es posible que la aplicación EPP instalada no incluya todos los componentes enumerados.

- El archivo de configuración de KPSN caduca pronto o ya ha caducado. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#).

Este estado es aplicable a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(Agente de EDR\)](#) , este estado no se muestra.

- **Offline** (negro)

Sin telemetría durante más de 7 días (valor predeterminado) Puede cambiar el número de días de ausencia de telemetría, después de lo cual se muestra el estado **Offline** para el activo, en la sección **Configuración**. El rango disponible es de 2 a 29 días.

Si ve que sus activos tienen el estado **Offline**:

- Asegúrese de que los componentes de la aplicación EPP enumerados en los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

El estado **Offline** no se aplica a los activos de VDI (máquinas virtuales temporales).

- **Absent** (negro)

Sin telemetría durante más de 30 días para activos físicos o durante más de 24 horas para activos VDI (máquinas virtuales temporales).

Si ve que sus activos tienen el estado **Absent**:

- Asegúrese de que los componentes de la aplicación EPP con los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

Puede ocultar los activos con estado **Absent** en la [lista de activos](#), en los [informes](#) y en los datos recibidos a través de la [interfaz de API](#).

- **Isolation**

Si el aislamiento de la red está activado o no Los posibles valores de filtro son:

- **Isolated**

El aislamiento de red está activado.

- **Not isolated**

El aislamiento de red está desactivado.

3. Haga clic en **Save** para aplicar el filtro creado.

Solo los activos que cumplen con los parámetros seleccionados del filtro se muestran en la lista de activos después de que se aplica el filtro.

Puede ocultar los activos con estado **Absent** en la lista de activos. Para hacerlo, marque la casilla correspondiente en la pestaña **Settings** → **General settings**.

Ver información detallada sobre activos en MDR Web Console

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Para ver información detallada sobre los activos:

1. En la ventana de MDR Web Console, navegue hasta el elemento del menú **Assets**.

Se abre la lista de activos.

2. Haga clic en la cadena del activo cuyos detalles desea ver.

Aparece la tarjeta de activos. La tarjeta de activos contiene dos pestañas:

- **Properties** tiene información general sobre el activo
- **Incidents** tiene información sobre los incidentes que han ocurrido con el activo

La información general de la pestaña **Properties** contiene la siguiente información:

- **Asset name**

Nombre de red de un equipo.

Puede hacer clic en **Asset name** para ver la información del activo en Kaspersky Security Center Web Console.

- **Status**

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

El estado refleja la condición actual del activo. Para los activos con los estados *Correcto*, *Advertencia* o *Crítico*, la aplicación también enumera los problemas (si los hay) de las últimas 72 horas.

Los activos tienen uno de los siguientes estados:

- **OK** (verde)

La telemetría se está enviando, la protección está completamente operativa.

- **Warning** (amarillo)

Posibles razones del estado **Warning**:

- Pequeñas pérdidas de telemetría. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Las bases de datos antivirus están desactualizadas desde hace más de 7 días.
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

Firewall

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Security para Virtualization Light Agent](#) [↗]
- [Kaspersky Embedded Systems Security para Windows](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]

Protección frente a amenazas en la red

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Endpoint Security for Linux](#) [↗]
- [Kaspersky Endpoint Security para Mac](#) [↗]
- [Kaspersky Embedded Systems Security para Windows](#) [↗]
- [Kaspersky Embedded Systems Security para Linux](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]

Protección frente a amenazas en el correo y extensión adicional para Microsoft Office Outlook

En el siguiente artículo se describe cómo activar o configurar este componente: [Kaspersky Endpoint Security para Windows](#) [↗].

Protección frente a amenazas web

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Endpoint Security for Linux](#) [↗]
- [Kaspersky Endpoint Security para Mac](#) [↗]
- [Kaspersky Security para Virtualization Light Agent](#) [↗]
- [Kaspersky Embedded Systems Security para Linux](#) [↗]

Autodefensa del producto

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Security para Virtualization Light Agent](#) [↗]
- [Kaspersky Embedded Systems Security para Windows](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]

Estos componentes afectan la integridad de la telemetría que se envía. Si un componente está desactivado o ausente, Kaspersky Managed Detection and Response no envía los eventos de telemetría relacionados con este componente. La aplicación EPP instalada podría no incluir todos los componentes enumerados.

- El archivo de configuración de KPSN está por caducar. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#). Si continúa trabajando con el archivo de configuración actual, el estado cambiará a **Critical** algunos días antes de la fecha de caducidad.

El estado **Warning** se aplica a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(EDR Agent\)](#) [↗], este estado no se muestra.

- **Critical** (rojo)

Posibles razones del estado **Critical**:

- Grandes pérdidas de telemetría. Los datos de telemetría son insuficientes para el análisis. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:
 - **System Watcher o Detección de comportamiento**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Endpoint Security for Linux](#) [↗]

- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 

- **Protección frente a amenazas en archivos**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si alguno de estos componentes está desactivado o ausente, Kaspersky Managed Detection and Response deja de enviar telemetría desde el activo. Es posible que la aplicación EPP instalada no incluya todos los componentes enumerados.

- El archivo de configuración de KPSN caduca pronto o ya ha caducado. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#).

Este estado es aplicable a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(Agente de EDR\)](#) , este estado no se muestra.

- **Offline (negro)**

Sin telemetría durante más de 7 días (valor predeterminado) Puede cambiar el número de días de ausencia de telemetría, después de lo cual se muestra el estado **Offline** para el activo, en la sección **Configuración**. El rango disponible es de 2 a 29 días.

Si ve que sus activos tienen el estado **Offline**:

- Asegúrese de que los componentes de la aplicación EPP enumerados en los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

El estado **Offline** no se aplica a los activos de VDI (máquinas virtuales temporales).

- **Absent (negro)**

Sin telemetría durante más de 30 días para activos físicos o durante más de 24 horas para activos VDI (máquinas virtuales temporales).

Si ve que sus activos tienen el estado **Absent**:

- Asegúrese de que los componentes de la aplicación EPP con los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

Puede ocultar los activos con estado **Absent** en la [lista de activos](#), en los [informes](#) y en los datos recibidos a través de la [interfaz de API](#).

- **IP address**

La dirección IP del activo.

- **Physical address**

- **Tenant**

Nombre del [inquilino](#), si el activo pertenece a uno de los inquilinos. Si el activo no pertenece a un inquilino, el campo está en blanco.

- **First seen**

- **Last seen**

- **Operating system**

Sistema operativo que está instalado en el activo.

- **Kaspersky applications that work with MDR**

- **Domain**

La pestaña **Incidents** contiene la lista de incidentes. La columna **ID/Created** de la lista contiene un identificador del incidente y la hora en que se creó. La columna **Status** de la lista contiene información sobre el estado del incidente.

Estados de los activos

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

El estado refleja la condición actual del activo. Para los activos con los estados *Correcto*, *Advertencia* o *Crítico*, la aplicación también enumera los problemas (si los hay) de las últimas 72 horas.

Los activos tienen uno de los siguientes estados:

- **OK** (verde)

La telemetría se está enviando, la protección está completamente operativa.

- **Warning** (amarillo)

Posibles razones del estado **Warning**:

- Pequeñas pérdidas de telemetría. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Las bases de datos antivirus están desactualizadas desde hace más de 7 días.
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

Firewall

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protección frente a amenazas en la red

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protección frente a amenazas en el correo y extensión adicional para Microsoft Office Outlook

En el siguiente artículo se describe cómo activar o configurar este componente: [Kaspersky Endpoint Security para Windows](#) .

Protección frente a amenazas web

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 

Autodefensa del producto

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Security para Virtualization Light Agent](#) [↗]
- [Kaspersky Embedded Systems Security para Windows](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]

Estos componentes afectan la integridad de la telemetría que se envía. Si un componente está desactivado o ausente, Kaspersky Managed Detection and Response no envía los eventos de telemetría relacionados con este componente. La aplicación EPP instalada podría no incluir todos los componentes enumerados.

- El archivo de configuración de KPSN está por caducar. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#). Si continúa trabajando con el archivo de configuración actual, el estado cambiará a **Critical** algunos días antes de la fecha de caducidad.

El estado **Warning** se aplica a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(EDR Agent\)](#) [↗], este estado no se muestra.

- **Critical** (rojo)

Posibles razones del estado **Critical**:

- Grandes pérdidas de telemetría. Los datos de telemetría son insuficientes para el análisis. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

- **System Watcher o Detección de comportamiento**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Endpoint Security for Linux](#) [↗]
- [Kaspersky Embedded Systems Security para Windows](#) [↗]
- [Kaspersky Embedded Systems Security para Linux](#) [↗]
- [Kaspersky Industrial CyberSecurity for Nodes](#) [↗]
- [Kaspersky Security para Virtualization Light Agent](#) [↗]

- **Protección frente a amenazas en archivos**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) [↗]
- [Kaspersky Endpoint Security for Linux](#) [↗]
- [Kaspersky Endpoint Security para Mac](#) [↗]

- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Si alguno de estos componentes está desactivado o ausente, Kaspersky Managed Detection and Response deja de enviar telemetría desde el activo. Es posible que la aplicación EPP instalada no incluya todos los componentes enumerados.

- El archivo de configuración de KPSN caduca pronto o ya ha caducado. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#).

Este estado es aplicable a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(Agente de EDR\)](#) , este estado no se muestra.

- **Offline** (negro)

Sin telemetría durante más de 7 días (valor predeterminado) Puede cambiar el número de días de ausencia de telemetría, después de lo cual se muestra el estado **Offline** para el activo, en la sección **Configuración**. El rango disponible es de 2 a 29 días.

Si ve que sus activos tienen el estado **Offline**:

- Asegúrese de que los componentes de la aplicación EPP enumerados en los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

El estado **Offline** no se aplica a los activos de VDI (máquinas virtuales temporales).

- **Absent** (negro)

Sin telemetría durante más de 30 días para activos físicos o durante más de 24 horas para activos VDI (máquinas virtuales temporales).

Si ve que sus activos tienen el estado **Absent**:

- Asegúrese de que los componentes de la aplicación EPP con los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

Puede ocultar los activos con estado **Absent** en la [lista de activos](#), en los [informes](#) y en los datos recibidos a través de la [interfaz de API](#).

Verificar el estado de los activos en Kaspersky Security Center

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Puede verificar el estado de sus activos utilizando la función de estados de activos de MDR. Le permite verificar qué activos están protegidos por Kaspersky Managed Detection and Response y qué activos nunca enviaron [telemetría](#) a Kaspersky Managed Detection and Response.

Para los activos con Kaspersky Endpoint Security para Windows 12.3 o versiones posteriores que funcionen en la [configuración de Endpoint Detection and Response Agent \(EDR Agent\)](#), el estado que se muestra en MDR no refleja el estado real.

Estados de los activos que han enviado telemetría al menos una vez

Para comprobar el estado de los activos:

1. En la sección **MDR** de Kaspersky Security Center, vaya a la pestaña **Estados de los activos de MDR**.
2. Seleccione la pestaña **Todos los activos alguna vez vistos**.

Se muestra la lista de todos los activos que enviaron telemetría a Kaspersky Managed Detection and Response al menos una vez.

Se muestran los siguientes detalles de cada activo:

Estado

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

El estado refleja la condición actual del activo. Para los activos con los estados *Correcto*, *Advertencia* o *Crítico*, la aplicación también enumera los problemas (si los hay) de las últimas 72 horas.

Los activos tienen uno de los siguientes estados:

- **OK** (verde)

La telemetría se está enviando, la protección está completamente operativa.

- **Warning** (amarillo)

Posibles razones del estado **Warning**:

- Pequeñas pérdidas de telemetría. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Las bases de datos antivirus están desactualizadas desde hace más de 7 días.

- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

Firewall

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protección frente a amenazas en la red

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Protección frente a amenazas en el correo y extensión adicional para Microsoft Office Outlook

En el siguiente artículo se describe cómo activar o configurar este componente: [Kaspersky Endpoint Security para Windows](#) .

Protección frente a amenazas web

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Endpoint Security for Linux](#) 
- [Kaspersky Endpoint Security para Mac](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Linux](#) 

Autodefensa del producto

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#) 
- [Kaspersky Security para Virtualization Light Agent](#) 
- [Kaspersky Embedded Systems Security para Windows](#) 
- [Kaspersky Industrial CyberSecurity for Nodes](#) 

Estos componentes afectan la integridad de la telemetría que se envía. Si un componente está desactivado o ausente, Kaspersky Managed Detection and Response no envía los eventos de telemetría relacionados con este componente. La aplicación EPP instalada podría no incluir todos los componentes enumerados.

- El archivo de configuración de KPSN está por caducar. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#). Si continúa trabajando con el archivo de configuración actual, el estado cambiará a **Critical** algunos días antes de la fecha de caducidad.

El estado **Warning** se aplica a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(EDR Agent\)](#)², este estado no se muestra.

- **Critical** (rojo)

Posibles razones del estado **Critical**:

- Grandes pérdidas de telemetría. Los datos de telemetría son insuficientes para el análisis. Consulte este artículo: [Cómo evitar la pérdida de datos de telemetría de los activos](#)
- Al menos uno de los siguientes componentes de la aplicación EPP en el activo no está instalado o está desactivado:

- **System Watcher o Detección de comportamiento**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#)²
 - [Kaspersky Endpoint Security for Linux](#)²
 - [Kaspersky Embedded Systems Security para Windows](#)²
 - [Kaspersky Embedded Systems Security para Linux](#)²
 - [Kaspersky Industrial CyberSecurity for Nodes](#)²
 - [Kaspersky Security para Virtualization Light Agent](#)²

- **Protección frente a amenazas en archivos**

Los siguientes artículos describen cómo habilitar o configurar este componente:

- [Kaspersky Endpoint Security para Windows](#)²
 - [Kaspersky Endpoint Security for Linux](#)²
 - [Kaspersky Endpoint Security para Mac](#)²
 - [Kaspersky Security para Virtualization Light Agent](#)²
 - [Kaspersky Embedded Systems Security para Windows](#)²
 - [Kaspersky Embedded Systems Security para Linux](#)²
 - [Kaspersky Industrial CyberSecurity for Nodes](#)²

Si alguno de estos componentes está desactivado o ausente, Kaspersky Managed Detection and Response deja de enviar telemetría desde el activo. Es posible que la aplicación EPP instalada no incluya todos los componentes enumerados.

- El archivo de configuración de KPSN caduca pronto o ya ha caducado. La aplicación muestra la fecha de caducidad. Considere la posibilidad de [actualizar el archivo de configuración de KPSN](#).

Este estado es aplicable a los activos con Kaspersky Endpoint Security para Windows 11 o posteriores, Kaspersky Endpoint Security for Linux 11.2 o posteriores, Kaspersky Endpoint Security for Mac 11.2 o posteriores, o Kaspersky Security for Virtualization Light Agent 5.2 o posteriores instalados. Para los activos con [Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent \(Agente de EDR\)](#),^[2], este estado no se muestra.

- **Offline** (negro)

Sin telemetría durante más de 7 días (valor predeterminado) Puede cambiar el número de días de ausencia de telemetría, después de lo cual se muestra el estado **Offline** para el activo, en la sección **Configuración**. El rango disponible es de 2 a 29 días.

Si ve que sus activos tienen el estado **Offline**:

- Asegúrese de que los componentes de la aplicación EPP enumerados en los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

El estado **Offline** no se aplica a los activos de VDI (máquinas virtuales temporales).

- **Absent** (negro)

Sin telemetría durante más de 30 días para activos físicos o durante más de 24 horas para activos VDI (máquinas virtuales temporales).

Si ve que sus activos tienen el estado **Absent**:

- Asegúrese de que los componentes de la aplicación EPP con los estados **Warning** y **Critical** estén instalados y activados en los activos.
- Asegúrese de que Kaspersky Managed Detection and Response esté [correctamente implementado](#) en su infraestructura.

Puede ocultar los activos con estado **Absent** en la [lista de activos](#), en los [informes](#) y en los datos recibidos a través de la [interfaz de API](#).

Nombre del activo

Nombre de red de un equipo.

Puede hacer clic en **Asset name** para ver la información del activo en Kaspersky Security Center Web Console.

Id. del activo

Identificador único de un activo. Kaspersky Managed Detection and Response genera automáticamente el id. de activo antes de que el activo envíe telemetría por primera vez.

Dominio

Dominio de red al que pertenece el activo.

Versión del sistema operativo

Sistema operativo que está instalado en el activo.

Aplicaciones de EPP

Aplicación Endpoint Protection Platform (EPP) que está instalada en el activo y configurada para su uso con Kaspersky Managed Detection and Response.

Interfaces

Número de todas las interfaces de red disponibles del dispositivo.

Inquilino

Nombre del [inquilino](#), si el activo pertenece a uno de los inquilinos. Si el activo no pertenece a un inquilino, el campo está en blanco.

Visto por última vez

Cantidad de días desde la última vez que se vio el activo en la Web Console MDR.

Los activos se ordenan según este atributo, en orden descendente.

De forma predeterminada, se muestran los activos que se vieron en los últimos 30 días. Puede ampliar el intervalo de tiempo aplicando filtros a los activos.

3. Utilice las siguientes opciones de ordenación y filtrado para trabajar con esta lista:

- Haga clic en el encabezado de cualquier columna para ordenar la lista según los valores de columna seleccionados.
- Haga clic en la columna **Estado** y luego seleccione los estados requeridos. La lista se filtrará para mostrar solo los activos con los estados seleccionados.
- Haga clic en **Filtrar** y seleccione un periodo de tiempo. Así puede ver solo los activos que se vieron por última vez durante el periodo de tiempo seleccionado. También puede especificar un período de tiempo personalizado.
- Haga clic en **Exportar** encima de la lista de activos para exportar en CSV.
- Utilice el campo **Buscar** para buscar activos por nombre.

Estados de los activos que nunca enviaron telemetría

Esta función funciona correctamente en Kaspersky Security Center 15.1 Windows o versiones posteriores, Kaspersky Security Center 15.1 Linux o versiones posteriores, y Kaspersky Next Expert View.

Para ver los activos que nunca enviaron telemetría:

1. En la sección **MDR** de Kaspersky Security Center, vaya a la pestaña **Estados de los activos de MDR**.
2. Seleccione la pestaña **No se puede obtener el estado de los activos**.

MDR Web Console muestra una lista de los activos que se añadieron a Kaspersky Security Center, pero que nunca han enviado telemetría a Kaspersky Managed Detection and Response.

Se muestran los siguientes detalles de cada activo:

- **Nombre del activo**

Nombre de red de un equipo.

Puede hacer clic en **Asset name** para ver la información del activo en Kaspersky Security Center Web Console.

- **Aplicaciones de EPP**

Aplicación Endpoint Protection Platform (EPP) que está instalada en el activo y configurada para su uso con Kaspersky Managed Detection and Response.

- **Estado de MDR**

El componente MDR de una aplicación EPP instalada en un activo puede tener uno de los siguientes estados:

- *Desconocida*: a diferencia de otros estados, las aplicaciones no envían el estado Desconocido. Esta opción muestra que las aplicaciones no tienen información sobre el estado del componente seleccionado. Por ejemplo, esto puede suceder cuando el componente seleccionado no pertenece a ninguna de las aplicaciones instaladas en el dispositivo, o cuando el dispositivo está apagado.
- *Detenido*: el componente está desactivado y no funciona en este momento.
- *En pausa*: el componente está en pausa, por ejemplo, después de que el usuario ha desactivado la protección en la aplicación EPP.
- *Iniciando*: el componente se encuentra en proceso de inicialización.
- *En ejecución*: el componente está activado y trabajando correctamente.
- *Con errores*: se ha producido un error durante la operación del componente.
- *No instalado*: el usuario no seleccionó el componente para la instalación al configurar la instalación personalizada de la aplicación.
- *Sin licencia*: falta o ha caducado la licencia que cubre la funcionalidad de MDR.

- **Servidor KSC**

Nombre del Servidor de administración de Kaspersky Security Center que administra el activo seleccionado.

- **Estado de los componentes críticos**

Lista de componentes de la aplicación EPP críticos para el funcionamiento de MDR. Cada componente tiene una indicación cuyo color indica el estado del componente:

- La indicación amarilla se utiliza cuando el componente tiene uno de los siguientes estados: **En pausa**, **Iniciando** o **Desconocido**.
- La indicación roja se utiliza cuando el componente tiene uno de los siguientes estados: **Detenido**, **Con errores**, **Sin licencia** o **No instalado**.

Además, la [función Autodefensa](#) aparece junto con los componentes de la aplicación EPP. Si esta función está desactivada, también tiene una indicación roja.

- Los componentes que tienen el estado **En ejecución** no se enumeran en la tabla y no tienen ninguna indicación.

Para ver la lista completa de componentes, incluidos los que no son críticos para el funcionamiento de MDR, haga clic en el nombre del activo. Los componentes y sus estados se mostrarán en la ventana de detalles del activo.

3. Si es necesario, puede filtrar los activos por estado de MDR. Para hacerlo, haga clic en **Filtrar** y luego seleccione los estados de MDR que desea ver. MDR Web Console mostrará solo aquellos activos en los que el componente MDR tenga uno de los estados de MDR seleccionados. También puede seleccionar una de las siguientes opciones:

- **Instalado y activado:** la lista se filtrará para mostrar los activos que tengan uno de los siguientes estados de MDR: *Desconocido*, *Detenido*, *En pausa*, *Iniciando*, *En ejecución* o *Con errores*.
- **La licencia falta o ha caducado:** la lista se filtrará para mostrar los activos MDR que tienen el estado *Sin licencia*.

4. Si es necesario, haga clic en el botón **Exportar** para exportar la lista de activos a un archivo CSV.

Cómo evitar la pérdida de datos de telemetría de los activos

Recomendamos utilizar las últimas versiones de las aplicaciones y soluciones de Kaspersky para garantizar la mejor protección y obtener acceso completo a las nuevas funciones y actualizaciones.

Los activos [envían datos de telemetría](#) a Kaspersky Managed Detection and Response para detectar y analizar incidentes de seguridad en su infraestructura. Si ve que hay pérdidas de telemetría en el [estado de los activos](#), asegúrese de seguir hasta el final las siguientes instrucciones:

1. Las versiones recomendadas de las aplicaciones de Kaspersky están instaladas en sus activos (consulte la columna *Versiones recomendadas y su periodo de soporte* en la sección *Versiones de aplicaciones de Kaspersky compatibles* de [Requisitos de hardware y software](#)).
2. El ancho de su canal de red cumple con las especificaciones proporcionadas en la sección *Canal de red* de los [Requisitos de hardware y software](#).
3. Su [servidor proxy de KSN](#) ² puede proporcionar la suficiente capacidad de rendimiento.

Si hay problemas con la capacidad de rendimiento del servidor proxy de KSN, desactive el proxy de KSN en la [directiva de KSC](#) para forzar a los activos a conectarse a KSN directamente:

- a. En el menú principal de Kaspersky Security Center, vaya a **Dispositivos** → **Directivas y perfiles**.
 - b. Haga clic en la directiva de Kaspersky Endpoint Security para Windows, Linux o Mac. Se abre la ventana de propiedades de la directiva seleccionada.
 - c. En las propiedades de la directiva, haga clic en **Configuración de la aplicación** → **Protección frente a amenazas avanzadas** → **Kaspersky Security Network**.
 - d. Active **Usar servidores de KSN cuando las opciones de proxy de KSN no estén disponibles** (si corresponde para la directiva).
 - e. Haga clic en **Aceptar**.
4. El proxy de KSN está activado en el lado del punto de distribución en [Kaspersky Next Expert View](#) o en Kaspersky Security Center [Web Console](#) para optimizar la carga de la red.
5. La carga de trabajo del Servidor de administración de Kaspersky Security Center no supera las [limitaciones](#).
6. Se utiliza la versión recomendada de Kaspersky Security Center especificada en [Requisitos de hardware y software](#); están instaladas las últimas revisiones y parches disponibles.

Administración de incidentes

Un *incidente* es una actividad considerada crítica por la tecnología de detección y que requiere una reacción inmediata del servicio online. Esta sección proporciona información sobre cómo administrar incidentes existentes y añadir nuevos incidentes.

Puede gestionar incidentes en [MDR Web Console](#).

Para administrar los incidentes en MDR Web Console, debe crear una cuenta de [Kaspersky Account](#) y pedirle a su [administrador de MDR](#) (el usuario de MDR Web Console con función de **MDR Administrator**) que lo [invite a MDR Web Console](#) usando la dirección de correo electrónico que usa para Kaspersky Account. Después, reciba el correo electrónico de invitación que contiene el enlace a MDR Web Console.

La solución MDR ofrece acciones de respuesta, que puede [procesar manualmente](#) o para las que puede [configurar la aceptación automática](#).

Puede configurar integraciones con [KUMA](#) y [XDR](#), lo que permite a MDR procesar datos de estas plataformas.

Sobre los incidentes

Que es un incidente

En el contexto de la seguridad informática, un incidente es cualquier evento imprevisto o no deseado capaz de interrumpir las actividades normales o la seguridad de la información.

Un evento son los signos externos identificados de un estado particular de un sistema, servicio o red.

Dentro del marco de la solución Kaspersky MDR, el criterio principal para decidir si la actividad observada es un incidente es la capacidad de implementar medidas eficientes para contrarrestar, prevenir o reducir posibles daños derivados de esta actividad. Consulte la tabla a continuación para ver ejemplos de posibles criterios de incidentes y medidas de respuesta según el origen del evento.

Ejemplos de criterios de detección de incidentes y medidas de respuesta

Origen del evento	Criterios posibles del incidente	Respuestas posibles del incidente
Dispositivo endpoint	- La fase activa del ataque que no se ha prevenido automáticamente - Evidencia de persistencia maliciosa en el sistema - Indicadores de incidentes pasados - Indicadores de actividad de infiltración interna por parte del cliente (incluidos los casos en los que se repelió el ataque)	- Detección de problemas mediante los productos de AO Kaspersky Lab instalados en los dispositivos endpoint y evaluación de la eficiencia de la corrección automática (si es técnicamente posible) - Acciones de respuesta manuales recomendadas - Acciones de respuesta automáticas solicitadas - Recomendaciones para concienciar a los usuarios sobre la seguridad de la información
Dispositivo endpoint + red	Evento de seguridad de una tecnología compatible de detección de red que ha sido confirmado en el dispositivo endpoint.	- Detección de problemas mediante las soluciones de AO Kaspersky Lab instaladas en dispositivos endpoint, así como las soluciones de AO Kaspersky Lab para monitorización del tráfico de red, y evaluación de la eficiencia de la respuesta automática (si es técnicamente posible) - Acciones de respuesta manuales recomendadas - Acciones de respuesta automáticas solicitadas - Informar al cliente

Detección de incidentes

Caso 1. Detección de incidentes mediante la solución Kaspersky MDR

En este caso, se detecta un incidente de seguridad de la información como resultado del funcionamiento de Kaspersky MDR. El incidente se registra automáticamente en el sistema de seguimiento de incidentes. El nivel de prioridad del incidente predeterminado se puede cambiar más adelante, pero será necesario especificar el motivo del cambio según la tabla de niveles de prioridad del incidente (consulte a continuación). Kaspersky MDR procesa los incidentes registrados para obtener rápidamente información acerca del estado de la infraestructura de TI del Cliente.

Si como resultado del análisis se logra identificar las causas raíz del incidente, se proporcionan al cliente recomendaciones de respuesta. Si no hay suficiente información para identificar la causa raíz del incidente, se proporcionan al cliente toda la información disponible y los resultados del análisis para que haga una investigación independiente.

Caso 2. Detección de incidentes por parte del cliente (la creación de incidentes personalizados no está disponible en algunos de los [niveles de licencias comerciales](#))

En este caso, el cliente detecta los incidentes de seguridad de la información, independientemente del funcionamiento de Kaspersky MDR. Si se necesita que Kaspersky MDR procese los incidentes, el cliente puede registrarlo manualmente y proporcionar toda la información disponible sobre el incidente detectado mediante las funciones de Kaspersky MDR. De forma predeterminada, el nivel de prioridad del incidente se establece en **Bajo**, a menos que el cliente especifique lo contrario al registrarlo.

El procesamiento posterior del incidente es similar al del caso 1.

Niveles de prioridad de incidentes

Niveles de prioridad de incidentes y sus descripciones

Nivel de prioridad del incidente	Descripción
Alta	Incidentes que, en opinión de los expertos de AO Kaspersky Lab, pueden provocar interrupciones importantes o acceso no autorizado a los activos del cliente supervisados por Kaspersky MDR. Ejemplo: rastros identificados de un ataque selectivo o una amenaza desconocida que requieren más investigación mediante métodos forenses digitales.
Media	Incidentes que, en opinión de los expertos de AO Kaspersky Lab, pueden afectar la eficiencia o el rendimiento de los activos del cliente supervisados por Kaspersky MDR, o pueden resultar en un evento único de corrupción de los datos.
Baja	Incidentes que, en opinión de los expertos de AO Kaspersky Lab, no afectan en gran medida la eficiencia o el rendimiento de los activos del cliente supervisados por Kaspersky MDR. Por ejemplo, software potencialmente no deseado identificado, como adware o software de riesgo.

El nivel de prioridad del incidente predeterminado es **Baja**.

Objetivos de rendimiento de la prestación de la solución

Tiempo de reacción estimado y valor de rapidez de la entrega de respuesta de Kaspersky MDR según la prioridad del incidente

Nivel de prioridad del incidente	Tiempo de reacción	Valor objetivo
Alta	1 hora	90 %
Media	4 horas	90 %
Baja	24 horas	90 %

El incidente se considerará resuelto si se proporcionaron al cliente recomendaciones sobre qué medidas de respuesta tomar.

* El tiempo de reacción es el tiempo entre la detección del incidente (hora de creación) y su publicación en MDR Web Console (hora de actualización).

Valor objetivo: porcentaje de incidentes en los que el tiempo de reacción coincide con el valor estimado especificado en la tabla.

Ver y buscar incidentes en MDR Web Console

Para ver incidentes:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Incidentes** del menú.

Se abre la lista de incidentes. Cada línea representa un incidente. Puede hacer clic en cualquier parte de la línea para ver la información del incidente.

Los siguientes atributos de incidentes están presentes encima de la lista:

- **ID/Created:** identificador numérico del incidente en la Consola / fecha en que se creó el incidente.
- **Status:** uno de los siguientes estados de incidentes:
 - **Open:** el incidente debe ser procesado por el equipo de seguridad.
 - **Resolved:** el incidente recibió una respuesta creada por el equipo de seguridad.
 - **On hold:** el equipo de seguridad dejó de procesar temporalmente el incidente.
 - **Closed:** el equipo de seguridad procesó el incidente y no es necesario trabajar más en él.
- **Summary:** Un breve comentario sobre el incidente.
- **Tenant** un inquilino al que se le ha asignado un incidente.
- **Updated:** fecha y hora en que se actualizó el incidente.

Los incidentes se ordenan según su fecha y hora de actualización en orden descendente.

En la parte superior de la lista de incidentes se encuentran los siguientes botones:

- El botón **Columns** con el icono de engranaje, que sirve para seleccionar qué columnas mostrar en la pestaña **History**.
- El botón **Filter** con el icono de embudo, que sirve para mostrar los cambios relacionados solo con las casillas marcadas.
- El botón **Search** con el icono de lupa, que sirve para mostrar los cambios relacionados solo con las palabras o caracteres ingresados.

2. Si desea cambiar el número de incidentes que se muestran por página de la lista, seleccione un número haciendo clic en la opción **entries per page** en la parte inferior de la página. Puede seleccionar 10, 20 o 50 incidentes por página.

Para navegar por la lista de incidentes, seleccione una página debajo de la lista. Puede utilizar las opciones **Anterior** y **Siguiente** para cambiar entre páginas adyacentes.

Para [filtrar los incidentes](#), haga clic en el icono del embudo que se encuentra sobre la lista.

Puede buscar a través de los incidentes haciendo clic en el ícono de la lupa, ubicado junto al ícono del embudo sobre la lista de incidentes.

Filtrar incidentes en MDR Web Console

Para ver incidentes específicos, puede crear y aplicar filtros a la lista de incidentes.

Para crear un filtro para la lista de incidentes:

1. En MDR Web Console, haga clic en el elemento del menú **Incidents**.

Se abre la lista de incidentes.

2. Haga clic en el icono de embudo que se encuentra sobre la lista de incidentes.

Aparece el bloque **Filter**.

Los parámetros disponibles para el filtrado son:

- **Created**
Período de tiempo en que se creó el incidente.
- **Updated**
Período de tiempo en que se actualizó el incidente.
- **Priority**
Prioridad del incidente. Las prioridades disponibles son Baja, Normal y Alta.
- **Status**
Estado del incidente.
- **Resolution**
Resolución aplicada al incidente.

- **Assets**

Activos disponibles.

- **Tenant**

Nombres de inquilinos disponibles.

Puede seleccionar el valor **Root tenant** para ver los incidentes que no están asignados a ninguno de sus inquilinos.

Puede seleccionar el valor **Root tenant** además de especificar los nombres de los inquilinos.

- **Tactics**

Tácticas MITRE disponibles para respuesta a incidentes.

- **Response statuses**

Muestra solo los incidentes con los estados de las respuestas correspondientes seleccionados.

3. Haga clic en **Save** para aplicar el filtro creado. Haga clic en **Clear** para descartar el filtro creado.

Solo los incidentes que cumplen con los parámetros seleccionados del filtro se muestran en la lista de incidentes después de que se aplica el filtro.

Crear incidentes personalizados en MDR Web Console

La creación de incidentes personalizados no está disponible en algunos [niveles de licencias comerciales](#).

Si considera que alguna actividad en su infraestructura es una amenaza, pero Kaspersky Managed Detection and Response no creó un incidente automáticamente, puede añadir un nuevo incidente manualmente.

De acuerdo con los términos del acuerdo de nivel de servicio (SLA), la cantidad de incidentes creados manualmente que son elegibles para ser procesados por el equipo de seguridad es limitada. La información sobre las limitaciones está disponible en la pestaña [Uso de MDR en Kaspersky Security Center](#). En esta pestaña, puede realizar un seguimiento del uso de los incidentes creados manualmente para el período actual (por ejemplo, para la semana actual):

- El número total de incidentes que puede crear para el período actual. Estos incidentes serán procesados por el equipo de seguridad, según el SLA. Puede crear más incidentes de los que se especifican en el acuerdo de MDR, pero el cumplimiento de los plazos del SLA no está garantizado para el procesamiento de dichos incidentes.
- El número restante de incidentes que puede crear para el período actual.

Para añadir un nuevo incidente:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Incidents** del menú.

Se abre la lista de incidentes.

2. En la parte superior de la ventana, haga clic en el botón **Add**.

Aparece el nuevo bloque de incidentes.

3. Rellene los siguientes campos:

- **Summary**

Un breve comentario sobre el incidente.

- **Descripción**

Información detallada, escrita de forma libre, sobre el incidente. Compatible con Markdown

- **Assets**

Los activos afectados por el incidente. En este campo se sugieren los activos que ya existen en MDR Web Console y Kaspersky Security Center.

4. Si es necesario, rellene el campo **Tenant**.

Para el campo **Tenant**, se sugieren los inquilinos que ya existen y el valor **Raíz sin inquilinos**.

5. Haga clic en el botón **Send**.

El nuevo bloque de incidentes desaparece.

El nuevo incidente se añade a la lista de incidentes en MDR Web Console. Puede ver información detallada sobre este incidente y procesar las respuestas que se le da.

Ver información detallada sobre incidentes en MDR Web Console

Para ver información detallada sobre incidentes:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Incidents** del menú.

Se abre la lista de incidentes.

2. Haga clic en la cadena del incidente cuyos detalles desea ver.

Se abre la página de incidentes.

El título de la página contiene un identificador de incidente. Debajo del título hay cuatro pestañas:

- **Summary**

Contiene información general sobre el incidente.

- **Responses**

Contiene información sobre las respuestas al incidente.

- **Communication**

Contiene información sobre la comunicación y los archivos relacionados con el incidente.

- **History**

Contiene información sobre los cambios del incidente.

La información general de la pestaña **Summary** comienza con un breve resumen del incidente. La información adicional enumerada en esta sección incluye:

- Prioridad del incidente
- Estado del incidente
- Resolución de incidentes
- Marcas de tiempo del incidente, hora y fecha de creación y de actualización
- Tácticas MITRE
- Técnicas MITRE
- Tecnología de detección

Debajo del resumen del incidente, se enumera la siguiente información:

- **Affected assets**
- **Asset-based IOCs**
- **Network-based IOCs**

La información general en la pestaña **Summary** concluye con una descripción del cliente y un botón **Close incident**.

3. Si sabe que el incidente es un duplicado o no lo va a resolver, haga clic en el botón **Close incident**.
4. Si es necesario, [envíe el incidente a IR Retainer](#) para su investigación y la eliminación de posibles consecuencias.
5. Consulte la pestaña **Responses** para ver información sobre las solicitudes de respuesta.

La información de la pestaña **Responses** se presenta como una lista. Las columnas de la lista son:

- **Status**
- **Asset ID**
- **Type**
- **Details**
- **Comment**
- **Changed by**
- **Update time**

6. Si desea añadir un comentario a un incidente:

- a. En la pestaña **Communication** de la página de detalles del incidente, escriba su comentario en el campo de texto.

Se admite el uso de Markdown y la posibilidad de adjuntar archivos. El tamaño máximo de archivo es de 10 MB.

b. Haga clic en el botón **Send**.

El comentario se añade a la pestaña **Communication** en la página de detalles del incidente. Puede editar o eliminar su comentario 10 minutos después de publicarlo.

7. Consulte la pestaña **History** para ver información sobre los cambios del incidente.

Debajo del título hay un interruptor para mostrar los cambios relacionados con:

- **All events**
- **Only incidents**
- **Only responses**
- **Only communication**

Junto a este interruptor, se encuentran los siguientes botones:

- El botón **Columns** con el icono de engranaje, que sirve para seleccionar qué columnas mostrar en la pestaña **History**.
- El botón **Filter** con el icono de embudo, que sirve para mostrar los cambios relacionados solo con las casillas marcadas.
- El botón **Search** con el icono de lupa, que sirve para mostrar los cambios relacionados solo con las palabras o caracteres ingresados.

Procesar respuestas a incidentes en MDR Web Console

Puede ver, aceptar y rechazar [respuestas](#) a incidentes.

Para ver las respuestas a un incidente:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Incidents** del menú.

Se abre la lista de incidentes.

2. Haga clic en la cadena del incidente cuyos detalles desea ver.

Se abre la página de incidentes.

3. En la página del incidente, haga clic en la pestaña **Responses**.

Se abre la lista de respuestas.

Cada línea representa una respuesta. Se muestra la siguiente información sobre la respuesta:

- **Status**
Estado de la respuesta.
- **Asset ID**
Identificador del activo para el que se ejecutará la respuesta.
- **Type**
Tipo del objeto que compone la respuesta.

- **Parameters**

Ruta local específica del sistema operativo para obtener el archivo de respuesta y tamaño esperado del archivo en MB. El tamaño máximo de archivo es de 10 MB.

- **Comment**

Último comentario a la respuesta.

- **Changed by**

Último usuario que modificó la descripción de la respuesta.

Para ver la descripción de la respuesta, haga clic en la cadena con la respuesta.

Para aceptar o rechazar respuestas a un incidente:

1. En la ventana Consola, navegue hasta el elemento del menú **Incidents**.

Se abre la lista de incidentes.

2. Haga clic en la cadena del incidente cuyos detalles desea ver.

Se abre la página de incidentes.

3. En la página del incidente, haga clic en la pestaña **Responses**.

Se abre la lista de respuestas.

4. Seleccione una respuesta que desee aprobar o rechazar marcando la casilla en el extremo izquierdo de la cadena que contiene la respuesta.

También puede marcar varias casilla a la izquierda para seleccionar varias respuestas. Para seleccionar todas las respuestas, marque la casilla en la parte izquierda del encabezado de la tabla de respuestas.

5. Para aprobar o rechazar una respuesta, seleccione el botón **Accept** o **Reject** ubicado debajo de la lista de respuestas. Aparece el cuadro de comentarios. Escriba su comentario y haga clic en el botón **Send**.

También puede hacer clic en una respuesta en la pestaña **Responses** para ver sus detalles y aceptarla o rechazarla en el panel lateral que allí aparece. Para rechazar la respuesta, debe ingresar su comentario en el campo del panel lateral.

El estado de la respuesta cambia.

Tipos de respuesta

La solución MDR examina los incidentes y crea respuestas que puede aceptar o rechazar. Esta es la forma predeterminada de manejar los incidentes en Kaspersky Managed Detection and Response.

Sin embargo, puede crear respuestas manualmente [mediante las funciones de Kaspersky Endpoint Detection y Response Optimum](#).

Este artículo solo describe los tipos de respuestas creadas por la solución MDR.

Cada respuesta puede tener un conjunto de parámetros que están presentes en la pestaña **Responses** de un incidente.

Los tipos de respuesta disponibles son:

- **Get file**

Copiar un archivo de su infraestructura a Kaspersky SOC. Si acepta esta respuesta, el archivo especificado se copiará en Kaspersky SOC.

Tenga en cuenta que este tipo de respuesta puede obtener archivos que contengan datos personales o confidenciales.

Los posibles parámetros son:

- **Infected file path**

La ruta absoluta del archivo. Por ejemplo, C:\\file.exe.

- **Maximum file size**

El tamaño máximo del archivo, en MB.

Si el archivo infectado excede el tamaño de archivo máximo especificado, el intento de aceptar la respuesta fallará y la respuesta no se realizará, pero aparecerá en la pestaña **History** de un incidente.

- **Isolate**

Aislar de la red el activo especificado.

Si surge la necesidad urgente de desactivar el aislamiento de red, [comuníquese con el soporte técnico](#) o escriba una solicitud en la pestaña **Communication** del incidente.

Los posibles parámetros son:

- **Password for disabling isolation**

La contraseña para desactivar el aislamiento. Una vez que el soporte técnico reciba su solicitud para deshabilitar el aislamiento de red, le enviarán el procedimiento con detalles sobre el uso de la contraseña.

- **Id. de tarea**

El identificador de tarea único que se usa junto con la **Password for disabling isolation** para desactivar manualmente el aislamiento de la red.

- **Password details**

Puede comprobar la validez de la **contraseña** generando una clave derivada a partir de ella y comparando el valor resultante con el valor del parámetro **Derived key**.

- **Version**

La versión numérica de las reglas de creación de contraseñas. Una versión de 1 significa que se aplican los siguientes parámetros de PBKDF2 para crear una clave derivada:

- Algoritmo hash HMACSHA256
- 10 000 iteraciones
- Longitud de clave de 32 bytes

- **Salt**

La sal en formato HEX para obtener una clave derivada a través de PBKDF2.

- **Derived key**

La clave derivada en formato HEX.

- **Exclude rules**

Matriz de reglas con puertos, protocolos, direcciones IP y procesos personalizados a los que no se aplica el aislamiento.

- **Direction**

La dirección del tráfico. Los valores posibles son: **Inbound**, **Outbound** y **Both**.

- **Protocolo**

El número de protocolo de acuerdo con la [especificación de IANA](#) ¹.

Los posibles valores son:

- **1** (ICMP)
- **6** (TCP)
- **17** (UDP)
- **58** (IPv6-ICMP)

- **Remote port range**

El rango de puertos remotos especificado en los campos anidados **From** y **To**.

- **Remote IPv4 address**

La dirección IPv4 o máscara de subred remota.

- **Remote IPv6 address**

La dirección IPv6 o máscara de subred remota.

- **Local port range**

El rango de puertos locales especificados en los campos anidados **From** y **To**.

- **Local IPv4 address**

La dirección IPv4 local o máscara de subred.

- **Local IPv6 address**

La dirección IPv6 local o máscara de subred.

- **Process**

La ruta a la imagen de proceso especificada en el campo anidado **Image** → **Path**.

- **Disable isolation**

Desactivar el aislamiento de red del activo especificado.

- **Delete registry key**

Eliminar una clave de registro o una rama de registro en el activo especificado.

Esta acción es irreversible.

Los posibles parámetros son:

- **Key**

La ruta de la clave absoluta, que comienza con HKEY_LOCAL_MACHINE o HKEY_USERS. Por ejemplo, HKEY_LOCAL_MACHINE\\SYSTEM\\WebClient.

Si la clave es un enlace simbólico, solo esta clave se eliminará, mientras que la clave de destino del enlace permanecerá intacta.

- **Value**

El valor de la clave.

Si no se especifica este parámetro, la clave se eliminará de forma recursiva. Durante la eliminación recursiva, cada subclave que sea un enlace simbólico se eliminará, mientras que su clave de destino permanecerá intacta.

Si el valor de la clave es una cadena vacía, se eliminará el valor predeterminado.

- **Memory dump**

Crear un volcado de memoria y enviarlo a Kaspersky SOC.

Los posibles parámetros son:

- **Dump type**

Un volcado de memoria puede ser de dos tipos:

- **Full memory dump**

Un volcado de toda la memoria de un activo.

- **Process dump**

Un volcado de un proceso específico.

- **Maximum file size**

El tamaño máximo de archivo para el volcado en formato ZIP, en MB. El valor predeterminado es 100 MB.

- **Process**

El id. del proceso y los detalles de la imagen.

- **Image**

- **Path**

La ruta absoluta del archivo. Por ejemplo, %systemroot%\\system32\\svchost.exe.

- **SHA-256**

La suma de comprobación SHA256 en formato HEX.

- **MD5**

La suma de comprobación MD5 en formato HEX.

- **Unique ID**

El identificador de proceso único.

- **Process count limit**

El número máximo de procesos que puede contener el archivo de volcado.

- **Terminate process**

Finalizar un proceso en el activo especificado con Kaspersky Endpoint Security para Windows. Se puede especificar qué proceso finalizar por su nombre o identificador de proceso (PID).

- **Run process**

Ejecutar un script en el activo especificado con Kaspersky Endpoint Security para Windows.

Para que esta respuesta funcione, el activo debe tener instalado el componente PowerShell. Puede ver el script que se ejecutará y su descripción en [MDR Web Console](#).

- **Quarantine file**

Coloca un archivo potencialmente peligroso en un almacenamiento local especial. En este almacenamiento, los archivos se guardan cifrados y no representan una amenaza a la seguridad del dispositivo. En la solicitud de confirmación se especifica el activo, la ruta al archivo y el hash del archivo (MD5 o SHA256).

- **Restaurar archivo almacenado en cuarentena**

Restaura a su ubicación original un archivo previamente puesto en cuarentena. La restauración no se lleva a cabo si hay un archivo con el mismo nombre en la ubicación original.

- **Get artefacts**

En este tipo de acción de respuesta se pueden transmitir archivos que contienen datos personales y confidenciales.

Disponible si ha configurado la integración con la versión 8.0 o posteriores de Kaspersky Anti Targeted Attack

Copia los archivos relacionados con las alertas de Kaspersky Anti Targeted Attack desde la infraestructura de Kaspersky Anti Targeted Attack a Kaspersky SOC. Los Analistas de SOC de MDR utilizan los archivos copiados para investigar las alertas de Kaspersky Anti Targeted Attack.

Los posibles parámetros son:

- Id. del nodo de la solución Kaspersky Anti Targeted Attack.
- Id. de la alerta de Kaspersky Anti Targeted Attack.

- Categorías de archivos relacionados con alertas para copiar a Kaspersky SOC:
 - Archivos PCAP y de carga útil relacionados con una alerta de IDS.
 - Informe sobre el resultado del análisis de archivos en el Entorno aislado (Sandbox). Incluye capturas de pantalla de la ejecución de objetos, registro de actividad y otros datos del análisis.
 - El archivo infectado que se envió a Entorno aislado.
 - Archivo que contiene los detalles de la alerta.

Disponible si ha configurado la integración con Kaspersky Next XDR Expert 2.1

Copia los archivos relacionados con las alertas o los incidentes de Kaspersky Endpoint Detection and Response Expert dentro de la infraestructura de Open Single Management Platform al SOC de Kaspersky. Los analistas del SOC de MDR utilizan los archivos copiados para investigar las alertas y los incidentes de Kaspersky Endpoint Detection and Response Expert.

Los posibles parámetros son:

- ID del nodo de la solución.
- ID de la alerta o del incidente de XDR.
- Categorías de archivos para copiar a Kaspersky SOC que están relacionadas con las alertas o incidentes:
 - Archivos cargados en la alerta o el incidente de XDR.
 - Informe sobre el resultado del análisis de archivos en el Entorno aislado (Sandbox). Incluye capturas de pantalla de la ejecución de objetos, registro de actividad y otros datos del análisis.
 - El archivo infectado que se envió a Entorno aislado.
 - Archivos relacionados con las acciones de respuesta del usuario a la alerta o incidente:
 - Recuperación de archivos
 - Recopilación de datos necesarios para el análisis forense
 - Adquisición de claves del registro
 - Recuperación de archivos del servicio del sistema de archivos NTFS
 - Adquisición del volcado de memoria del proceso
 - Cuarentena de archivos
- Detalles acerca de todos los archivos relacionados con la alerta.
- Nombres e id. de los archivos copiados.

Aceptación automática de respuestas en MDR Web Console

Puede activar la aceptación automática de las respuestas ofrecidas. En este caso, las acciones ofrecidas en las respuestas, por ejemplo, la eliminación de un archivo infectado, se realizarán automáticamente. Si esta característica está desactivada, las [medidas ofrecidas en las respuestas](#) deben aceptarse o rechazarse manualmente.

Si usa inquilinos, puede habilitar la aceptación automática de respuestas para todos los inquilinos o solo para los inquilinos que seleccione. Si no utiliza inquilinos, puede activar o desactivar esta función para su organización actual.

Para activar la aceptación automática de respuestas:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Settings** del menú.

2. Haga clic en la pestaña **Incidents**.

3. Seleccione una de las siguientes opciones:

- **Enabled for all tenants**

Cuando se selecciona esta opción, se activa la aceptación automática de respuestas tanto para los inquilinos existentes como para los recién creados.

- **Enabled for the tenants selected below**

Seleccione los inquilinos para los que desea activar la aceptación automática de respuestas. Para los inquilinos recién creados, la aceptación automática de respuestas está desactivada de forma predeterminada.

4. Haga clic en el botón **Save**.

La aceptación automática de respuestas está activada y las acciones ofrecidas dentro de las respuestas se realizarán automáticamente para todos los inquilinos o los inquilinos que haya seleccionado. Puede desactivar esta opción en cualquier momento.

Derechos de acceso para ver o cambiar la configuración de aceptación automática

Las [funciones de usuario de Kaspersky Managed Detection and Response](#) tienen los siguientes derechos de acceso a la configuración de aceptación automática:

Operación	Administrador de MDR	Director de seguridad	Encargado de seguridad
Haga clic en la pestaña Incidents .	✓	✓	—
Cambiar la opción seleccionada actualmente	✓	—	—
Ver la opción seleccionada actualmente	✓	✓	—
Activar la aceptación automática para todos los inquilinos	✓	—	—

Operación	Administrador de MDR	Director de seguridad	Encargado de seguridad
Activar la aceptación automática para inquilinos específicos	✓	✓ (solo para los inquilinos a los que el usuario tiene acceso)	—
Ver la configuración de aceptación automática de un inquilino específico	✓	✓ (solo para los inquilinos a los que el usuario tiene acceso)	—

Aceptación automática de respuestas en Kaspersky Security Center

Puede activar la aceptación automática de las respuestas ofrecidas. En este caso, las acciones ofrecidas en las respuestas, por ejemplo, la eliminación de un archivo infectado, se realizarán automáticamente. Si esta característica está desactivada, las [medidas ofrecidas en las respuestas](#) deben aceptarse o rechazarse manualmente.

Si usa inquilinos, puede habilitar la aceptación automática de respuestas para todos los inquilinos o solo para los inquilinos que seleccione. Si no utiliza inquilinos, puede activar o desactivar esta función para su organización actual.

Puede cambiar la configuración de aceptación automática si tiene la función de usuario Administrador de MDR. Los usuarios con la función de Director de seguridad no pueden cambiar la configuración. Los usuarios con la función de Director de seguridad sénior pueden realizar las siguientes operaciones:

- Ver la opción seleccionada actualmente
- Activar o desactivar la aceptación automática de respuestas para inquilinos específicos si la opción **Permitir cambiar la opción de aceptación automática de respuestas para cada inquilino** está seleccionada

Para configurar la aceptación automática de respuestas:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Ajustes**.
2. En el grupo de parámetros **Aceptación automática de respuestas**, seleccione la opción requerida:

- **Desactivar la aceptación automática de respuestas para todos los inquilinos**
Seleccione esta opción si desea aceptar o rechazar manualmente las acciones de respuesta.
- **Permitir cambiar la opción de aceptación automática de respuestas para todos los inquilinos**
Seleccione esta opción si desea habilitar la aceptación automática de respuestas para todos los inquilinos de su organización, incluidos los inquilinos existentes y los recién creados.
- **Permitir cambiar la opción de aceptación automática de respuestas para cada inquilino**
Seleccione esta opción si desea configurar individualmente la aceptación automática de respuestas para cada inquilino. A continuación, seleccione las casillas de verificación de los inquilinos para los que desea que las acciones de respuesta se realicen automáticamente. Para los inquilinos recién creados, la aceptación automática de respuestas está desactivada de forma predeterminada.

Si selecciona la opción **Todos los inquilinos**, la aceptación automática de respuestas se activará para los inquilinos que se creen a partir de ese momento.

3. Haga clic en el botón **Guardar**.

El botón **Guardar** se activa solo si usted cambia la configuración.

Cerrar incidentes en MDR Web Console

Puede cerrar un incidente si sabe que es un duplicado o no lo va a solucionar. En otros casos, no debe cerrar los incidentes, ya que debe resolverlos la solución MDR. La solución MDR resuelve un incidente si se aplican las medidas recomendadas en dicho incidente. Un incidente resuelto se cierra automáticamente después de 72 horas.

Para cerrar un incidente:

1. En la ventana de la Consola, navegue hasta el elemento **Incidents** del menú.

Se abre la lista de incidentes.

2. Haga clic en la cadena del incidente cuyos detalles desea ver.

Se abre la página de incidentes.

3. En la pestaña **Summary** haga clic en el botón **Close incident** en la parte inferior de la ventana.

No hay un botón **Close incident** para los incidentes con el estado **Closed**.

Aparece el bloque **Close incident**.

4. En el campo **Reason why you are closing this incident**, especifique la información adicional que desee comunicar a los analistas de SOC de Kaspersky Managed Detection and Response. Por ejemplo, puede dar detalles por qué considera que este incidente es una situación estándar y no representa amenazas para su infraestructura. Puede dejar este campo en blanco.

5. Debajo del campo de comentario, seleccione la opción **True positive** o **False positive**, según el motivo del cierre.

Seleccione la opción **True positive** si Kaspersky Managed Detection and Response detectó una amenaza, pero no desea que los analistas SOC de MDR investiguen y resuelvan el incidente.

Seleccione la opción **False positive** si Kaspersky Managed Detection and Response detectó una actividad no amenazante como una amenaza. Kaspersky Managed Detection and Response utiliza esta información para mejorar los algoritmos de detección automatizada.

6. En la parte inferior del bloque, haga clic en el botón **Close**.

Aparece el formulario **Comparta sus comentarios**.

7. En el formulario **Comparta sus comentarios**, seleccione una calificación del 1 al 5. Puede dejar un comentario de texto acerca del manejo de este incidente. Los expertos de Kaspersky procesan los comentarios para mejorar el rendimiento de la solución MDR.

8. Haga clic en **Enviar**.

Desaparece el bloque **Close incident**.

El incidente se cierra. A partir de ahora, Kaspersky Managed Detection and Response no realiza ninguna acción en relación con este incidente.

Enviar un incidente al equipo de respuesta a incidentes para una investigación adicional

Puede [enviar un incidente al Equipo de respuesta a incidentes](#) para su investigación. Este servicio incluye el conjunto completo de acciones de respuesta, desde el análisis inicial y las acciones iniciales hasta la detección de indicios adicionales de ataque y la preparación de un plan para eliminar posibles consecuencias.

Cuando paga la suscripción al servicio, obtiene cierta cantidad de horas de investigación. Las horas de investigación se consumen al enviar un incidente al equipo de Respuesta ante incidentes. Si no tiene horas de investigación disponibles, aún puede enviar un incidente para su investigación comprando un servicio comercial y creando una solicitud manualmente.

Recibirá los resultados de la investigación en la pestaña **Communication** del incidente.

Los usuarios con las funciones de MDR Administrator o Senior Security Officer tienen permiso para enviar incidentes al equipo de Respuesta a incidentes.

Para enviar un incidente al Equipo de respuesta a incidentes:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Incidents** del menú.
Se abre la lista de incidentes.
2. Haga clic en la cadena con el incidente que desea enviar al equipo de Respuesta a incidentes.
Se abre la página de incidentes.
3. En la pestaña **Summary**, en la sección **Actions**, realice una de las siguientes acciones:
 - Si tiene horas de investigación, haga clic en el botón **Escalate incident to the IR team** y luego confirme que desea enviar el incidente al Equipo de respuesta a incidentes.
 - Si no tiene horas de investigación, haga clic en el enlace y luego complete el formulario de creación de solicitud para adquirir el servicio comercial.

El incidente se envía. Los expertos del equipo de Respuesta a incidentes se pondrán en contacto con usted a través de la Web Console MDR lo antes posible después de recibir el incidente.

Integración de Kaspersky Unified Monitoring and Analysis

Kaspersky Unified Monitoring and Analysis Platform (KUMA) es una solución de software integrada que combina las siguientes funciones:

- Recepción, procesamiento y almacenamiento de eventos de seguridad de la información
- Análisis y correlación de datos entrantes
- Búsqueda en eventos recibidos
- Creación de notificaciones sobre indicadores detectados de amenazas de seguridad de la información

Puede configurar la integración de Kaspersky Managed Detection and Response en KUMA versión 4.0 o posterior para importar automáticamente los datos de KUMA a MDR.

El siguiente artículo describe cómo configurar la integración: [Integración de Kaspersky Endpoint Managed Detection and Response](#).

Creación de incidentes de Managed Detection and Response a partir de incidentes de XDR

Puede crear un incidente de MDR a partir de un incidente de XDR si la integración de Managed Detection and Response está activada en Open Single Management Platform y las alertas de incidentes de XDR cumplen con las siguientes condiciones:

- La fuente de detección es el endpoint.
- La alerta incluye al menos un activo relacionado.
- La tecnología de detección es alguna de las siguientes:
 - Reglas de Kaspersky IOA
 - SB (Entorno aislado)
 - AM (Anti-Malware Engine)
 - IOC
 - YARA

Recomendamos que active la solución MDR en todos los activos administrados para garantizar una protección administrada continua y automatizar la detección de amenazas, lo que permite liberar al personal de seguridad de TI para que puedan abordar las tareas que requieran su intervención.

Para exportar un incidente de XDR a MDR:

1. En el menú principal de la interfaz de la Consola OSMP, vaya a **Supervisión → Incidentes**.
2. En la tabla de incidentes, haga clic en el ID del incidente requerido. Se muestra la ventana con los detalles del incidente.
3. Haga clic en el icono de tres puntos en la barra de herramientas y elija **Crear incidente de MDR**.
4. En el panel **Crear incidente de MDR**, especifique el nombre y la descripción del incidente, y haga clic en **Crear**.
Si el incidente se crea correctamente, se muestra el mensaje correspondiente. Ahora puede acceder al incidente en Web Console MDR. El enlace al incidente está disponible en la sección **Resumen** del incidente de XDR.

Integración de Kaspersky Digital Footprint Intelligence para MDR

La solución MDR puede utilizar las credenciales comprometidas identificadas por Kaspersky Digital Footprint Intelligence (DFI) para mejorar los flujos de trabajo de detección, investigación y búsqueda de amenazas.

Los clientes no necesitan disponer de una licencia activa de Kaspersky DFI para utilizar esta función. Los datos de Kaspersky DFI están disponibles como parte de la función de MDR correspondiente.

La solución MDR analiza las filtraciones de credenciales relevantes para la organización del cliente y los activos asociados a ella que están cubiertos por la supervisión de MDR. La atención se centra principalmente en las filtraciones de credenciales relacionadas con malware de robo de información, que pueden indicar que el dispositivo de un empleado está en riesgo.

MDR utiliza los datos de Kaspersky DFI para las siguientes funciones:

- Enriquecimiento de alertas con contexto de filtraciones de credenciales;
- Correlación de credenciales filtradas con eventos de seguridad;
- Búsqueda de amenazas y detección de posibles riesgos en función de la información de las credenciales.

La integración de Kaspersky DFI ayuda a la solución MDR a identificar más rápidamente las cuentas que pueden estar comprometidas, priorizar mejor los incidentes relacionados y reducir el riesgo de acceso no autorizado.

Además de las filtraciones relacionadas con malware de robo de información, Kaspersky DFI puede analizar las credenciales expuestas públicamente en recursos de terceros, donde también pueden aparecer credenciales de empleados. El ámbito de supervisión también puede ampliarse a socios y otras entidades asociadas a la organización.

En resumen, Kaspersky DFI proporciona a MDR información sobre credenciales comprometidas, mientras que MDR aplica estos datos en los flujos de trabajo del SOC mediante el enriquecimiento de alertas, la correlación y la búsqueda de amenazas.

Uso de las funciones de Kaspersky Endpoint Detection and Response Expert

La integración de Kaspersky Endpoint Detection and Response Expert con Open Single Management Platform permite las siguientes funciones:

- Kaspersky Endpoint Detection and Response envía datos de alertas a MDR, lo que permite procesar la telemetría y las alertas de Endpoint Detection and Response en la solución MDR.
- [La capacidad de crear incidentes de MDR a partir de incidentes de XDR.](#)
- [Tipo de respuesta](#) Obtener artefactos.

Activación de la integración con Kaspersky Endpoint Detection and Response Expert

Se requiere la función de Administrador de MDR para configurar la integración.

Para activar la integración:

1. [Configure el complemento MDR](#) en la Consola de Open Single Management Platform.
2. En la sección MDR de la interfaz de la Consola OSMP, haga clic en la pestaña **Uso de MDR**.
3. Expanda el bloque **Archivo de configuración de KPSN para la integración con KEDR Expert**.
4. Active la opción **Aceptar acuerdo de KPSN** y haga clic en **Aplicar el archivo de configuración de KPSN para la integridad con KEDR Expert**.

La integración está activada.

Respuestas

La solución [Kaspersky Endpoint Detection and Response Expert](#) proporciona una serie de funciones de respuesta (en lo sucesivo, denominadas respuestas de EDR) que usted puede ejecutar y configurar manualmente.

- Aislamiento de red
- Poner un archivo en cuarentena
- Enviar archivos a Cloud Sandbox
- Borrar archivo
- Ejecutar análisis de áreas críticas
- Análisis de IOC

- Prevención de ejecución
- Iniciar proceso
- Terminar proceso
- Obtener el archivo

Puede encontrar más detalles sobre estas respuestas EDR en la [Ayuda en línea de Kaspersky Endpoint Detection and Response Expert](#).

Las respuestas de EDR descritas en esta sección están disponibles para los activos con Kaspersky Endpoint Security para Windows 11.7 o posterior. Si utiliza Kaspersky Endpoint Security for Windows 11.6 o una versión anterior en sus activos, Kaspersky Endpoint Agent debe estar instalado en estos activos para que funcione con las respuestas de EDR.

Para administrar las acciones de respuestas de alerta de EDR, en [Kaspersky Security Center](#)  vaya a la sección **Supervisión e informes** → **Alertas**.

Administración de inquilinos

El multiinquilinato es un mecanismo que le permite convertirse en un proveedor de Kaspersky Managed Detection and Response para otras organizaciones. Una vez que tenga una cuenta de MDR, puede crear [inquilinos](#) en su cuenta de MDR.

Puede crear hasta 100 inquilinos en su organización.

Su cuenta en Kaspersky Security Center Web Console o Kaspersky Next Expert View debe tener una función con los siguientes [derechos de acceso](#): **Acceso a incidentes** y **Administración de inquilinos**, y la posibilidad de ver, añadir, editar y eliminar inquilinos en la sección **MDR** en Kaspersky Security Center.

Si su organización tiene varias licencias, solo podrá realizar la [administración de inquilinos](#) en Kaspersky Security Center.

Para convertirse en un proveedor de MDR, debe tener acceso a la infraestructura de su inquilino para poder realizar escenarios de despliegue.

Todos los inquilinos son independientes y están aislados, lo que significa que otros inquilinos no pueden acceder a los datos de un inquilino.

Los activos con Kaspersky Embedded Systems Security for Windows y Kaspersky Embedded Systems Security for Linux solo se pueden asignar al inquilino raíz.

Solo los usuarios que tengan asignada la [función de administrador de MDR](#) pueden añadir, editar y eliminar inquilinos en MDR Web Console.

Gestionar inquilinos en Kaspersky Security Center

Esta sección ofrece información sobre cómo administrar inquilinos existentes y añadir nuevos inquilinos.

Ver inquilinos en Kaspersky Security Center

Puede ver los inquilinos disponibles utilizando la lista de inquilinos.

Su cuenta en Kaspersky Security Center Web Console o Kaspersky Next Expert View debe tener una función con los siguientes [derechos de acceso](#): **Acceso a incidentes** y **Administración de inquilinos**, y la posibilidad de ver, añadir, editar y eliminar inquilinos en la sección **MDR** en Kaspersky Security Center.

Para ver inquilinos:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Inquilinos**.

Aparece la lista **Inquilinos**. Cada línea representa un inquilino. Puede hacer clic en el nombre del inquilino para ver la información del inquilino.

2. Los siguientes atributos de inquilinos están presentes encima de la lista:

Nombre

Nombre del inquilino, elegido a voluntad y legible por humanos. Se especifica al crear el inquilino. El nombre de un inquilino puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 100 caracteres. No se puede cambiar el nombre de los inquilinos.

Estado

Uno de los siguientes estados de inquilino:

- **Inactiva**

El inquilino puede usar Kaspersky Managed Detection and Response.

- **Inactiva**

El inquilino no puede usar Kaspersky Managed Detection and Response.

Puede establecer el estado inactivo manualmente en la tarjeta de inquilino. Además, el estado inactivo se establece automáticamente al final de la vida del inquilino.

Activos/límite

Número de activos asignados a un inquilino/Límite de activos.

El límite de activos se especifica al crear inquilinos adicionales y es solo para fines informativos. Se permite superar el límite y no afecta al funcionamiento de la solución MDR.

Descripción

Información de formato libre que ingresa al crear o editar el inquilino. Puede especificar el propósito del inquilino o la cantidad proyectada de activos. La descripción puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 2000 caracteres.

Creado el

Fecha de creación del inquilino.

Fecha de caducidad

Fecha en la que caduca la vida útil del inquilino.

Los inquilinos se ordenan según su fecha de vencimiento en orden descendente.

También puede ver los [inquilinos en MDR Web Console](#).

Ver la configuración de inquilinos en Kaspersky Security Center

Puede ver la configuración de cada inquilino en su cuenta.

Su cuenta en Kaspersky Security Center Web Console o Kaspersky Next Expert View debe tener una función con los siguientes [derechos de acceso](#): **Acceso a incidentes** y **Administración de inquilinos**, y la posibilidad de ver, añadir, editar y eliminar inquilinos en la sección **MDR** en Kaspersky Security Center.

Para ver la configuración del inquilino:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Inquilinos**.

Aparece la lista **Inquilinos**. Cada línea representa un inquilino. Puede hacer clic en el nombre del inquilino para ver la información del inquilino.

2. Haga clic en la línea con el inquilino cuyos detalles desea ver.

Aparece el bloque **Configuración de inquilinos**.

La configuración comienza con ver si el botón de alternancia **Inactiva**, muestra si un inquilino está activo o no. Si es necesario, puede cambiar la posición del botón de alternancia **Inactiva**. A continuación, se muestran los siguientes campos:

Nombre

Nombre del inquilino, elegido a voluntad y legible por humanos. Se especifica al crear el inquilino. El nombre de un inquilino puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 100 caracteres. No se puede cambiar el nombre de los inquilinos.

Id

Identificador de inquilino único generado automáticamente.

Descripción

Información de formato libre que ingresa al crear o editar el inquilino. Puede especificar el propósito del inquilino o la cantidad proyectada de activos. La descripción puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 2000 caracteres.

Activos asignados

Número de activos asignados al inquilino.

Límite de activos

La cantidad de activos que se planea conectar al inquilino. Se permite superar este límite y no afecta al funcionamiento de la solución MDR.

Archivos de configuración para el inquilino

Esta sección muestra información sobre el [archivo de configuración MDR](#) para el inquilino:

- **Licencia:** la [licencia](#) que corresponde al inquilino.
- **Fecha de caducidad:** la vida útil del inquilino. Puede especificar la fecha de caducidad manualmente al crear el inquilino. La fecha de caducidad no puede ser igual o posterior al último día del plazo de su licencia de MDR.
- **Acción:** puede hacer clic en el enlace **Descargar el archivo de configuración** para descargar el archivo ZIP que contiene el archivo de configuración de MDR.

Haga clic en el botón **X** para eliminar un archivo de configuración. Solo puede eliminar un archivo de configuración si otro archivo de configuración está añadido al inquilino.

Haga clic en el botón **Añadir** para agregar un nuevo archivo de configuración. Indique la licencia y la fecha de vencimiento.

3. En la parte inferior del bloque **Configuración de inquilinos** haga clic en el botón **Cerrar** para cerrar el bloque.

También puede [ver la configuración de inquilinos en MDR Web Console](#).

Editar la configuración de inquilinos en Kaspersky Security Center

Puede modificar la configuración de cada inquilino en su cuenta.

Su cuenta en Kaspersky Security Center Web Console o Kaspersky Next Expert View debe tener una función con los siguientes [derechos de acceso](#): **Acceso a incidentes** y **Administración de inquilinos**, y la posibilidad de ver, añadir, editar y eliminar inquilinos en la sección **MDR** en Kaspersky Security Center.

Para modificar la configuración del inquilino:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Inquilinos**.

Aparece la lista **Inquilinos**. Cada línea representa un inquilino. Puede hacer clic en el nombre del inquilino para ver la información del inquilino.

2. Haga clic en la línea con el inquilino cuyos detalles desea editar.

Aparece el bloque **Configuración de inquilinos**. Aquí puede realizar las siguientes acciones:

- Activar o desactivar el inquilino mediante el botón de conmutación **Inactiva**.
- Cambiar el valor del campo **Descripción**.
- Para eliminar un archivo de configuración, haga clic en el botón **X**. Solo puede eliminar un archivo de configuración si otro archivo de configuración está añadido al inquilino.
- **Save** un nuevo archivo de configuración mediante clic en el botón **Añadir**. Indique la licencia y la fecha de vencimiento.

3. En la parte inferior del bloque de **Configuración de inquilinos**, haga clic en el botón **Save**.

- El bloque **Configuración de inquilinos** desaparece. Después de hacer clic en el botón **Save**, Kaspersky Managed Detection and Response genera el nuevo archivo de configuración de MDR que cumple con la configuración de inquilino actualizada. Puede hacer clic en el enlace **Descargar el archivo de configuración** para descargar el archivo ZIP que contiene el archivo de configuración MDR.

Se edita la configuración del inquilino. La configuración actualizada se aplica a los activos de los grupos de administración seleccionados.

También puede editar la [configuración de inquilinos en MDR Web Console](#).

Añadir nuevos inquilinos en Kaspersky Security Center

Si desea convertirse en un proveedor de Kaspersky Managed Detection and Response para otra organización, debe agregar un nuevo inquilino a su cuenta.

Su cuenta en Kaspersky Security Center Web Console o Kaspersky Next Expert View debe tener una función con los siguientes [derechos de acceso](#): **Acceso a incidentes y Administración de inquilinos**, y la posibilidad de ver, añadir, editar y eliminar inquilinos en la sección **MDR** en Kaspersky Security Center.

Para añadir un nuevo inquilino:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Inquilinos**.

Aparece la lista **Inquilinos**.

2. En la parte superior de la ventana, haga clic en el botón **+ Añadir inquilino**.

Aparece el bloque **Configuración de inquilinos**.

3. Si es necesario, cambie el botón de alternancia a **Inactiva**.

El botón de alternancia **Inactiva** está activado de forma predeterminada.

4. Rellene los siguientes campos:

Nombre

Nombre del inquilino, elegido a voluntad y legible por humanos. Se especifica al crear el inquilino. El nombre de un inquilino puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 100 caracteres. No se puede cambiar el nombre de los inquilinos.

Descripción

Información de formato libre que ingresa al crear o editar el inquilino. Puede especificar el propósito del inquilino o la cantidad proyectada de activos. La descripción puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 2000 caracteres.

Archivos de configuración para el inquilino

Esta sección muestra información sobre el [archivo de configuración MDR](#) para el inquilino:

- **Licencia:** la [licencia](#) que corresponde al inquilino.
- **Fecha de caducidad:** la vida útil del inquilino. Puede especificar la fecha de caducidad manualmente al crear el inquilino. La fecha de caducidad no puede ser igual o posterior al último día del plazo de su licencia de MDR.
- **Acción:** puede hacer clic en el enlace **Descargar el archivo de configuración** para descargar el archivo ZIP que contiene el archivo de configuración de MDR.

Haga clic en el botón **X** para eliminar un archivo de configuración. Solo puede eliminar un archivo de configuración si otro archivo de configuración está añadido al inquilino.

Haga clic en el botón **Añadir** para agregar un nuevo archivo de configuración. Indique la licencia y la fecha de vencimiento.

Límite de activos

La cantidad de activos que se planea conectar al inquilino. Se permite superar este límite y no afecta al funcionamiento de la solución MDR.

5. En la parte inferior del bloque de **Configuración de inquilinos**, haga clic en el botón **Guardar**.

El bloque **Configuración de inquilinos** desaparece. Después de hacer clic en el botón **Guardar**, Kaspersky Managed Detection and Response genera el [archivo de configuración de MDR](#) para el nuevo inquilino. Puede hacer clic en el enlace **Descargar el archivo de configuración** para descargar el archivo ZIP que contiene el archivo de configuración MDR.

Se añade el nuevo inquilino.

También puede [añadir nuevos inquilinos en MDR Web Console](#).

Eliminar inquilinos en Kaspersky Security Center

Cuando elimina un inquilino que contiene activos, todos los activos que contiene se desconectan de la solución MDR. Para poder seguir gestionando los activos del inquilino, antes de eliminarlo, [trasládelos al inquilino raíz o a un inquilino nuevo](#).

Su cuenta en Kaspersky Security Center Web Console o Kaspersky Next Expert View debe tener una función con los siguientes [derechos de acceso](#): **Acceso a incidentes** y **Administración de inquilinos**, y la posibilidad de ver, añadir, editar y eliminar inquilinos en la sección **MDR** en Kaspersky Security Center.

Para eliminar un inquilino:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **Inquilinos**.

Aparece la lista **Inquilinos**.

2. En la lista **Inquilinos**, sitúe el cursor sobre el inquilino que desea eliminar y, a continuación, haga clic en el icono de la papelera () en la columna **Actions**.

3. Confirme la eliminación.

Se elimina el inquilino seleccionado.

También puede [eliminar inquilinos en MDR Web Console](#).

Traslado de activos entre inquilinos

Cuando se elimina un inquilino que contiene activos, todos estos activos dejan de enviar telemetría a la solución MDR. Antes de eliminar un inquilino, mueva todos sus activos al inquilino predeterminado o a un nuevo inquilino

Su cuenta en Kaspersky Security Center Web Console o Kaspersky Next Expert View debe tener una función con los siguientes [derechos de acceso](#): **Acceso a incidentes** y **Administración de inquilinos**, y la posibilidad de ver, añadir, editar y eliminar inquilinos en la sección **MDR** en Kaspersky Security Center.

Para mover activos a un nuevo inquilino:

1. En la sección **MDR** de Kaspersky Security Center, [cree un nuevo inquilino](#). Más adelante, añadirá activos a este inquilino.

Cuando cree un nuevo inquilino, descargue un archivo de configuración de MDR.

2. En Kaspersky Security Center Web Console, [cree un nuevo grupo de administración](#).
3. [Agregue los activos](#) que desea mover a un nuevo inquilino al nuevo grupo de administración.
4. [Cree una nueva directiva](#) para Kaspersky Endpoint Agent o una aplicación EPP para el grupo de administración creado.

5. Aplique el archivo de configuración de MDR a la política creada.

Para obtener detalles sobre diferentes casos de implementación, consulte [Implementación de Kaspersky Managed Detection and Response](#).

Una vez que la directiva se aplica a los activos del grupo de administración, los activos se mueven del inquilino raíz al inquilino recién creado.

Para mover activos al inquilino predeterminado (root):

1. Descargue un archivo de configuración de MDR para el inquilino predeterminado:
 - En la Web Console MDR, (<https://mdr.kaspersky.com/guide>), vaya a la página **Getting Started** (Guía de inicio) y haga clic en el enlace del **archivo de configuración de MDR**.
 - En Kaspersky Security Center Web Console o Kaspersky Next Expert View, vaya a **MDR > Getting Started** y haga clic en el enlace **Descargar**.
2. En Kaspersky Security Center Web Console, [cree un nuevo grupo de administración](#).
3. [Agregue los activos](#) que desea mover al inquilino raíz al nuevo grupo de administración.
4. [Cree una nueva directiva](#) para Kaspersky Endpoint Agent o una aplicación EPP para el grupo de administración creado.

5. Aplique el archivo de configuración de MDR a la política creada.

Una vez que la directiva se aplica a los activos del grupo de administración, los activos se mueven al inquilino raíz.

Administrar inquilinos en MDR Web Console

Esta sección proporciona información acerca de cómo realizar la administración de inquilinos en MDR Web Console.

Ver inquilinos en MDR Web Console

Para ver inquilinos:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Settings** del menú.

2. Haga clic en la pestaña **Tenants**.

Aparece la lista **Tenants**. Cada línea representa un inquilino. Puede hacer clic en cualquier parte de la línea para ver la información del inquilino.

3. Los siguientes atributos de inquilinos están presentes encima de la lista:

Name

Nombre del inquilino, elegido a voluntad y legible por humanos. Se especifica al crear el inquilino. El nombre de un inquilino puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 100 caracteres. No se puede cambiar el nombre de los inquilinos.

Status

Uno de los siguientes estados de inquilino:

- **Inactiva**

El inquilino puede usar Kaspersky Managed Detection and Response.

- **Inactiva**

El inquilino no puede usar Kaspersky Managed Detection and Response.

Puede establecer el estado inactivo manualmente en la tarjeta de inquilino. Además, el estado inactivo se establece automáticamente al final de la vida del inquilino.

Assets / limit

Número de activos asignados a un inquilino/Límite de activos.

El límite de activos se especifica al crear inquilinos adicionales y es solo para fines informativos. Se permite superar el límite y no afecta al funcionamiento de la solución MDR.

Description

Información de formato libre que ingresa al crear o editar el inquilino. Puede especificar el propósito del inquilino o la cantidad proyectada de activos. La descripción puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 2000 caracteres.

Created on

Fecha de creación del inquilino.

Expiration date

Fecha en la que caduca la vida útil del inquilino.

Los inquilinos se ordenan según su fecha de vencimiento en orden descendente.

Actions

Muestra el icono de la papelera () al pasar el cursor sobre inquilinos que no son raíz. Para eliminar el inquilino, haga clic en el icono de la papelera y confirme la eliminación.

Ver la configuración de inquilinos en MDR Web Console

Para ver la configuración del inquilino:

1. En la ventana Consola, navegue hasta el elemento del menú **Settings**.

2. Haga clic en la pestaña **Tenants**.

Aparece la lista **Tenants**. Cada línea representa un inquilino. Puede hacer clic en cualquier parte de la línea para ver la información del inquilino.

3. Haga clic en la línea con el inquilino cuyos detalles desea ver.

Aparece el bloque **Tenant settings**.

La configuración comienza con ver si el botón de alternancia **Active**, muestra si un inquilino está activo o no. Puede cambiar el botón de alternancia **Active** para deshabilitar el inquilino.

A continuación, se muestran los siguientes campos:

Tenant name

Nombre del inquilino, elegido a voluntad y legible por humanos. Se especifica al crear el inquilino. El nombre de un inquilino puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 100 caracteres. No se puede cambiar el nombre de los inquilinos.

Description

Información de formato libre que ingresa al crear o editar el inquilino. Puede especificar el propósito del inquilino o la cantidad proyectada de activos. La descripción puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 2000 caracteres.

Assets / limit

La cantidad de activos que se planea conectar al inquilino. Se permite superar este límite y no afecta al funcionamiento de la solución MDR.

Configuration file lifetime

Fecha en la que caduca el archivo de configuración del inquilino.

Este campo no se muestra para el inquilino raíz.

En la parte inferior del bloque, hay un botón para descargar el [archivo de configuración de MDR](#) para el despliegue del inquilino.

4. En la parte inferior del bloque **Tenant settings**, haga clic en el botón **Cancel** para cerrar el bloque.

Editar la configuración de inquilinos en MDR Web Console

La capacidad de añadir, editar y eliminar inquilinos está disponible solo para el usuario que tenga asignado el [rol de administrador de MDR](#).

Para modificar la configuración del inquilino:

1. Abra la Web Console MDR.
2. En la sección **Settings** de la Web Console MDR, haga clic en la pestaña **Tenants**.
Aparece la lista **Tenants**. Cada línea representa un inquilino. Puede hacer clic en cualquier parte de la línea para ver la información del inquilino.
3. Haga clic en la línea con el inquilino cuyos detalles desea editar.
Aparece el bloque **Tenant settings**.
4. Si es necesario, cambie el conmutador de alternancia a **Active**.
5. Si es necesario, cambie los valores de los campos.
6. En la parte inferior del bloque **Tenant settings**, haga clic en el botón **Save**.
El bloque **Tenant settings** desaparece. Después de hacer clic en el botón **Save**, Kaspersky Managed Detection and Response genera el nuevo archivo de configuración de MDR que cumple con la configuración de inquilino actualizada.
7. En la lista de **Tenants**, haga clic en la línea con el inquilino editado.
Aparece el bloque **Tenant settings**. En la parte inferior del bloque, hay un botón para descargar el [archivo de configuración de MDR](#) para el despliegue del inquilino.
8. En la parte inferior del bloque **Tenant settings**, haga clic en el botón **Cancel** para cerrar el bloque.
Se edita la configuración del inquilino. Ahora, debe implementar el nuevo archivo de configuración de MDR en los activos del inquilino para aplicar la configuración editada.

Añadir nuevos inquilinos en MDR Web Console

La capacidad de añadir, editar y eliminar inquilinos está disponible solo para el usuario que tenga asignado el [rol de administrador de MDR](#).

Para añadir un nuevo inquilino:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Settings** del menú.
2. Haga clic en la pestaña **Tenants**.
Aparece la lista **Tenants**.

3. En la parte superior de la ventana, haga clic en el botón **Add**.

Aparece el bloque **Tenant settings**.

4. Si es necesario, cambie el botón de alternancia a **Active**.

El botón de alternancia **Active** está activado de forma predeterminada.

5. Rellene los siguientes campos:

Tenant name

Nombre del inquilino, elegido a voluntad y legible por humanos. Se especifica al crear el inquilino. El nombre de un inquilino puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 100 caracteres. No se puede cambiar el nombre de los inquilinos.

Description

Información de formato libre que ingresa al crear o editar el inquilino. Puede especificar el propósito del inquilino o la cantidad proyectada de activos. La descripción puede contener letras latinas, dígitos y caracteres especiales. No puede tener más de 2000 caracteres.

Assets / limit

La cantidad de activos que se planea conectar al inquilino. Se permite superar este límite y no afecta al funcionamiento de la solución MDR.

Configuration file lifetime

Fecha en la que caduca el archivo de configuración del inquilino.

Este campo no se muestra para el inquilino raíz.

6. En la parte inferior del bloque de **Tenant settings**, haga clic en el botón **Save**.

El bloque **Tenant settings** desaparece. Después de hacer clic en el botón **Save**, Kaspersky Managed Detection and Response genera el [archivo de configuración de MDR](#) para el nuevo inquilino.

7. En la lista **Tenants**, haga clic en la línea con el nuevo inquilino.

Aparece el bloque **Tenant settings**. Aquí puede descargar el [archivo de configuración de MDR](#) para el despliegue del inquilino.

8. Haga clic en el botón **Configuration archive** para descargar el nuevo archivo de configuración de MDR.

9. En la parte inferior del bloque **Tenant settings**, haga clic en el botón **Cancel** para cerrar el bloque.

Se añade el nuevo inquilino. Ahora, puede desplegar en los activos del inquilino el archivo de configuración de MDR descargado.

Tenga en cuenta que los inquilinos que se han creado en la Web Console MDR no están disponibles en la sección **MDR** de Kaspersky Security Center. Utilice MDR Web Console para trabajar con estos inquilinos.

Eliminar inquilinos en MDR Web Console

Cuando elimina un inquilino que contiene activos, todos los activos que contiene se desconectan de la solución MDR. Los incidentes asignados a un inquilino eliminado ya no están disponibles. Esta acción es irreversible. Antes de eliminar un inquilino, [mueva todos sus activos al inquilino raíz o a un nuevo inquilino](#).

La capacidad de añadir, editar y eliminar inquilinos está disponible solo para el usuario que tenga asignado el [rol de administrador de MDR](#).

Para eliminar un inquilino:

1. En la ventana Consola, navegue hasta el elemento del menú **Settings**.
2. Haga clic en la pestaña **Tenants**.
Aparece la lista **Tenants**.
3. En la lista de inquilinos, pase el puntero del mouse sobre el inquilino que desea eliminar y haga clic en el botón **Delete tenant** con el icono de la papelera a la derecha.
Aparece la ventana **Confirm tenant deletion**.
4. Haga clic en el botón **Delete** para eliminar el inquilino.

Tenga en cuenta que los inquilinos creados en MDR Console no están disponibles en la sección **MDR** de Kaspersky Security Center. Utilice MDR Web Console para trabajar con estos inquilinos.

Administrar la solución a través de la API de REST

Esta función está disponible en MDR Expert, MDR Advanced (disponible solo en algunas regiones) y MDR Prime (disponible solo en algunas regiones). Consulte la comparación de soluciones de licencia [en esta sección](#).

Para tener acceso a la API de REST en Kaspersky Security Center, su cuenta en Kaspersky Security Center Web Console debe tener los siguientes derechos de acceso: Acceso a incidentes y Acceso a la API de REST.

En algunos [niveles de licencia comerciales](#), en MDR Web Console solo será posible generar un token de actualización para [configurar el complemento MDR](#), sin acceso a la API de REST en Kaspersky Security Center.

Kaspersky Managed Detection and Response le permite obtener, crear y actualizar entidades de MDR mediante programación a través de la API de REST. La API de REST opera a través de HTTP y consta de un conjunto de métodos de solicitud/respuesta. En otras palabras, puede administrar Kaspersky Managed Detection and Response a través de una solución de terceros, no de MDR Web Console.

Para comenzar a trabajar con la API de REST, debe [crear un token de actualización](#) y [un token de acceso](#).

[ABRIR LA REFERENCIA DE LA API DE REST](#) 

Escenario: realizar una autorización basada en token

Este caso explica cómo realizar una autorización basada en token para trabajar con la API de REST.

Prerrequisitos

Asegúrese de tener una cuenta de MDR con uno de los siguientes roles asignado:

- La [función](#) de administrador de MDR
- Un rol personalizado con los siguientes [derechos de acceso](#) (aplicable solo a Kaspersky Security Center):
 - Acceso a incidentes
 - Acceso a la API de REST

Etapas

La autorización basada en tokens procede en etapas:

1 Crear un token de actualización en MDR Web Console

Necesita [un token de actualización](#) para crear un token de acceso. Un token de actualización es válido durante 24 horas. Puede usar un token de actualización solo una vez.

2 Crear un token de acceso a través de la API de REST

Necesita [un token de acceso](#) para trabajar con la API de REST. Un token de acceso es válido por 1 hora. Puede utilizar un token de acceso varias veces durante su vida útil.

Cuando crea un token de acceso, la API de REST genera un nuevo token de actualización y lo incluye en la respuesta. Cuando caduca el token de acceso, puede crear un nuevo token de acceso utilizando el token de actualización generado por la API más reciente.

Un token de actualización generado por la API es válido durante 7 días.

Resultados

Una vez completado este escenario, puede [comenzar a trabajar con la API de REST](#), enviando solicitudes con el token de acceso.

Crear una conexión API en Kaspersky Security Center

Cuando cree una nueva conexión API, se genera un token de actualización. Un *token de actualización* es una secuencia única de letras, dígitos y símbolos. Una vez creado, un token de actualización le permite crear un token de acceso.

Para crear una conexión API:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **API**.

Aparece la lista **API**.

2. En la parte superior de la ventana, haga clic en el botón **Añadir conexión**.

Aparece el bloque **Añadir una nueva conexión de API**.

3. Especifique la siguiente configuración:

- **Nombre de la conexión**

El nombre de una conexión puede contener letras latinas, dígitos y caracteres especiales. El nombre de una conexión se especifica como `author_name` en las respuestas de la API de REST y se muestra como el autor del comentario en la pestaña **Communication** de un incidente.

- **Derechos de acceso**

Seleccione qué derechos de acceso otorgar para realizar acciones a través de la API HTTP:

- **Acceso completo + API e inquilinos**

Derechos de acceso del rol de administrador de MDR. Un administrador de MDR es un superusuario que tiene acceso a todas las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia. El administrador de MDR puede otorgar acceso a los orígenes de datos del cliente a otros usuarios. Cuando activa Kaspersky Managed Detection and Response, usted se convierte automáticamente en el administrador de MDR. Por esto, le recomendamos utilizar una dirección de correo electrónico corporativa para el proceso de activación y no una dirección de correo electrónico personal. Crear el Administrador de MDR con una dirección de correo electrónico personal puede suponer riesgos de seguridad, como el robo de la cuenta de Administrador de MDR.

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	✓	—
Administración de respuestas	✓	—
Administración de inquilinos	✓	—
Información consolidada sobre incidentes	✓	—
Acceso a la API de REST	✓	—

- **Configuración de acceso a incidentes, administración de respuestas y aceptación automática**

Derechos de acceso del rol de oficial de seguridad superior. Un oficial de seguridad superior es un empleado que tiene acceso a las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia, pero que no tiene acceso a la API de REST. El Director de seguridad tiene derecho a aceptar y rechazar [respuestas](#).

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	✓	—
Administración de respuestas	✓	—
Administración de inquilinos	—	✓
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

- **Acceso a incidentes**

Derechos de acceso del rol de oficial de seguridad. Un oficial de seguridad es un empleado que tiene acceso a las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia, pero que no tiene acceso a la API de REST. El Encargado de seguridad no puede aceptar ni rechazar [respuestas](#).

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	—	✓
Administración de respuestas	—	✓
Administración de inquilinos	—	✓

Área funcional	Permitir	Negar
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

- **Inquilino**

Si es necesario, seleccione el valor (o valores) en la lista desplegable **Inquilino**.

El usuario puede ver solo los activos e incidentes relacionados con los inquilinos especificados.

4. Haga clic en el botón **Generar**.

Aparece el campo del **Token JWT**.

5. Haga clic en el botón **Cerrar**.

La nueva conexión de API aparece en la lista **API**. Ahora, puede usar este token de actualización para [crear un token de acceso](#).

También puede [crear conexiones API en MDR Web Console](#).

Crear una conexión API en MDR Web Console

Un *token de actualización* es una secuencia única de letras, dígitos y símbolos. Una vez creado, un token de actualización le permite crear un token de acceso.

Para crear un token de actualización:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Settings** del menú.

2. Haga clic en la pestaña **API**.

Aparece la lista **All tokens**.

3. En la parte superior de la ventana, haga clic en el botón **Add**.

Aparece un bloque **Generate token**.

4. Especifique la siguiente configuración:

- **Connection name**

El nombre de un token.

El nombre de un token puede contener letras latinas, dígitos y caracteres especiales. El nombre de un token se especifica como `author_name` en las respuestas de la API de REST y se muestra como el autor del comentario en la pestaña **Communication** de un incidente.

En algunos [niveles de licencia comerciales](#), este es el único campo disponible al crear un token de actualización.

- **User role**

La función de usuario para especificar los permisos que se otorgarán para realizar acciones a través de la API HTTP.

Están disponibles los siguientes roles de usuario:

- **MDR Administrator**

Superusuario que tiene acceso a todas las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia. El administrador de MDR puede otorgar acceso a los orígenes de datos del cliente a otros usuarios. Cuando activa Kaspersky Managed Detection and Response, usted se convierte automáticamente en el administrador de MDR. Por esto, le recomendamos utilizar una dirección de correo electrónico corporativa para el proceso de activación y no una dirección de correo electrónico personal. Crear el Administrador de MDR con una dirección de correo electrónico personal puede suponer riesgos de seguridad, como el robo de la cuenta de Administrador de MDR.

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	✓	—
Administración de respuestas	✓	—
Administración de inquilinos	✓	—
Información consolidada sobre incidentes	✓	—
Acceso a la API de REST	✓	—

- **Senior Security Officer**

Empleado que tiene acceso a las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia, pero que no tiene acceso a la API de REST. El Director de seguridad tiene derecho a aceptar y rechazar [respuestas](#).

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	✓	—
Administración de respuestas	✓	—
Administración de inquilinos	—	✓
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

- **Security Officer**

Empleado que tiene acceso a las funciones de Kaspersky Managed Detection and Response otorgadas por la licencia, pero que no tiene acceso a la API de REST. El Encargado de seguridad no puede aceptar ni rechazar [respuestas](#).

En Kaspersky Security Center, esta función corresponde a los siguientes derechos de acceso:

Área funcional	Permitir	Negar
Acceso a incidentes	✓	—
Aceptar automáticamente la configuración	—	✓
Administración de respuestas	—	✓
Administración de inquilinos	—	✓
Información consolidada sobre incidentes	—	✓
Acceso a la API de REST	—	✓

- **Tenant**

Si es necesario, seleccione el valor (o valores) en la lista desplegable **Tenant**.

En la Consola se pueden seleccionar inquilinos existentes o el valor **Root tenant**.

El usuario puede ver solo los activos e incidentes relacionados con los inquilinos especificados. Si tiene activos e incidentes que no estén asignados a ningún inquilino, el usuario puede verlos si usted selecciona el valor **Root tenant**.

Puede seleccionar el valor **Root tenant** además de especificar los nombres de los inquilinos.

5. En la parte inferior del bloque, haga clic en el botón **Generate**.

El bloque **Token info** reemplaza al bloque **Generate token**.

6. Haga clic en el botón **Close** en la parte inferior del bloque **Token info**.

El token de actualización que ha creado aparece en la lista **All tokens**. Ahora, puede usar este token de actualización para [crear un token de acceso](#).

Editar una conexión API en Kaspersky Security Center

Puede editar las conexiones de API existentes.

Para editar una conexión de API:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **API**.

Aparece la lista **API**.

2. Haga clic en la conexión de API que desea editar.

Aparece un bloque que contiene la información de conexión.

3. Cambie la configuración de la conexión.

4. Haga clic en el botón **Guardar**.

Se guardan las nuevas configuraciones de la conexión de API seleccionada.

Editar una conexión API en MDR Web Console

Puede editar las conexiones de API existentes.

Para editar una conexión de API:

1. En MDR Web Console, haga clic en la pestaña **API**.

Aparece la lista **All tokens**.

2. Haga clic en el token de la API que desea modificar.

Aparece un bloque que contiene la información de conexión.

3. Cambie la configuración de la conexión.

4. Haga clic en el botón **Save**.

Se guardan las nuevas configuraciones de la conexión de API seleccionada.

Crear un token de acceso en Kaspersky Security Center

Un *token de acceso* es una secuencia única de caracteres (letras, dígitos y caracteres especiales) que le autoriza a utilizar los métodos de la API de REST.

Para crear un token de acceso:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **API**.

Aparece la lista **API**.

2. Haga clic en una conexión con un estado de **Activación pendiente**.

Aparece un bloque que contiene la información de conexión.

3. En el campo **Token JWT**, haga clic en el botón **Actualizar**.

Aparece un token de actualización.

4. Seleccione y guarde el valor del campo **Id. del cliente**.

5. Seleccione y guarde la secuencia de caracteres del token en el portapapeles.

6. Envíe una solicitud POST al punto final `/session/confirm`.

Reemplace `{client_id}` y `{refresh_token}` con los valores seleccionados y guardados en los pasos anteriores.

Ejemplo (Python):

```
#####
# Parte general
#####

import time
import datetime
import requests
import jwt

# El certificado es necesario para la autenticación de un recurso externo
#Puede descargar el certificado desde https://mdr.kaspersky.com,
#guárdelo en su disco y agregue la ruta en la variable:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# El id. de su cliente y sus tokens de usted
# Para obtener más información sobre cómo obtener su ID y los tokens, consulte la ayuda https://support.kaspersky.com/MDR/en-US/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Pegue su valor)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Pegue su valor)
ACCESS_TOKEN = "AcCeSsToKeN" # (Pegue su valor)

#####
#Obtenga un token de acceso y un token de actualización para la próxima actualización del token de acceso
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN fecha y hora de caducidad: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN es válido")
    else:
        print(
            "Debe actualizar REFRESH_TOKEN; tómelo de la Web Console MDR (https://support.kaspersky.com/MDR/es-ES/258285.htm)"
        )
        exit()
else:
    print(
        "Debe rellenar el valor REFRESH_TOKEN; tómelo de la Web Console MDR (https://support.kaspersky.com/MDR/es-ES/258285.htm)"
    )
    exit()

#Verificar la presencia y validez del token de acceso
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN fecha y hora de caducidad: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN es válido")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

#Si es necesario, actualice el token de acceso y actualice el token para la próxima actualización del token de acceso
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body, verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    #Es necesario guardar el token de actualización para obtener el siguiente token de acceso cuando caduque el token de acceso actual
    refresh_token = result_json["refresh_token"]
    print(
        f'Su nuevo REFRESH_TOKEN para la próxima vez que solicite ACCESS_TOKEN (reemplace el valor de REFRESH_TOKEN con este valor): "{refresh_token}"'
    )

    # Se requiere un nuevo token de acceso para recuperar los datos
    access_token = result_json["access_token"]
    print(f'Su nuevo ACCESS_TOKEN (reemplace el valor de ACCESS_TOKEN con este valor): "{access_token}"')

#El token de acceso se añade al encabezado de la solicitud
headers = {"Authorization": f"Bearer {access_token}"}
```

Ejemplo (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

La API de REST envía una respuesta con el token de acceso y un nuevo token de actualización.

```
{
  "access_token": "SamPLET346yoKEsAmPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkEnSaMPleT2590KEsS123aMPle926tOkEnSaMPle"
}
```

Ahora, puede enviar solicitudes a la API de REST utilizando el token de acceso. Cada solicitud a la API de REST requiere un token de acceso; una solicitud sin un token de acceso solo devolverá un error de autorización.

También puede [crear un token de acceso en MDR Web Console](#).

Crear un token de acceso en MDR Web Console

Para crear un token de acceso:

1. En la ventana de MDR Web Console, navegue hasta el elemento **Settings** del menú.

2. Haga clic en la pestaña **API**.

Aparece la lista **All tokens**. Cada línea representa un token. Puede hacer clic en cualquier parte de la línea para ver la información del token.

3. Haga clic en un token con un estado de **Pending activation**.

Aparece un bloque de **Token info**.

4. En el campo **JWT token**, haga clic en el botón **Actualizar**.

Aparece un token de actualización.

5. Seleccione y guarde el valor del campo **Client ID**.

6. Seleccione y guarde la secuencia de caracteres del token en el portapapeles.

7. Envíe una solicitud POST al endpoint `/session/confirm` (consulte los ejemplo de abajo).

Reemplace `{client_id}` y `{refresh_token}` con los valores seleccionados y guardados en los pasos anteriores.

Ejemplo (Python):

```
#####
# Parte general
#####

import time
import datetime
import requests
import jwt

# El certificado es necesario para la autenticación de un recurso externo
#Puede descargar el certificado desde https://mdr.kaspersky.com,
#guárdelo en su disco y agregue la ruta en la variable:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

# MDR REST API URL:
API_URL = "https://mdr.kaspersky.com/api/v1"

# El id. de su cliente y sus tokens de usted
# Para obtener más información sobre cómo obtener su ID y los tokens, consulte la ayuda https://support.kaspersky.com/MDR/en-US/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Pegue su valor)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Pegue su valor)
ACCESS_TOKEN = "AcCeSsToKeN" # (Pegue su valor)

#####
#Obtenga un token de acceso y un token de actualización para la próxima actualización del token de acceso
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN fecha y hora de caducidad: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN es válido")
    else:
        print(
            "Debe actualizar REFRESH_TOKEN; tómelo de la Web Console MDR (https://support.kaspersky.com/MDR/es-ES/258285.htm)"
        )
        exit()
else:
    print(
        "Debe rellenar el valor REFRESH_TOKEN; tómelo de la Web Console MDR (https://support.kaspersky.com/MDR/es-ES/258285.htm)"
    )
    exit()

#Verificar la presencia y validez del token de acceso
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN fecha y hora de caducidad: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN es válido")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

#Si es necesario, actualice el token de acceso y actualice el token para la próxima actualización del token de acceso
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body, verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    #Es necesario guardar el token de actualización para obtener el siguiente token de acceso cuando caduque el token de acceso actual
    refresh_token = result_json["refresh_token"]
    print(
        f'Su nuevo REFRESH_TOKEN para la próxima vez que solicite ACCESS_TOKEN (reemplace el valor de REFRESH_TOKEN con este valor): "{refresh_token}"'
    )

    # Se requiere un nuevo token de acceso para recuperar los datos
    access_token = result_json["access_token"]
    print(f'Su nuevo ACCESS_TOKEN (reemplace el valor de ACCESS_TOKEN con este valor): "{access_token}"')

#El token de acceso se añade al encabezado de la solicitud
headers = {"Authorization": f"Bearer {access_token}"}
```

Ejemplo (Shell):

```
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
```

La API de REST envía una respuesta con el token de acceso y un nuevo token de actualización.

```
{
  "access_token": "SamPLET346yoKEsAmPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkEnSaMPleT2590KEsS123aMPle926tOkEnSaMPle"
}
```

Ahora, puede enviar solicitudes a la API de REST utilizando el token de acceso. Cada solicitud a la API de REST requiere un token de acceso; una solicitud sin un token de acceso solo devolverá un error de autorización.

Trabajar con la API de REST

Trabajar con MDR a través de la API de REST incluye obtener, crear y actualizar activos, incidentes, respuestas y usuarios.

[ABRIR LA REFERENCIA DE LA API DE REST](#)

Los métodos de la API de REST requieren un valor `client_id`. Puede obtener su valor `client_id` abriendo el bloque de **Token info** de cualquier token de actualización en MDR Web Console.

He aquí ejemplos de secuencias de comandos para Python y Shell que muestran las capacidades básicas de la API de REST:

- Definir la ruta del certificado, la URL de la API REST, el id. del cliente y los tokens
- Obtener el token de acceso y actualizar el token para la siguiente actualización del token de acceso
- Obtener el número de activo
- Obtener la lista de activos o los detalles de los activos
- Obtener el número de incidentes, la lista de incidentes o los detalles del incidente
- Obtener la lista de respuestas al incidente
- Confirmar o rechazar la respuesta o actualizar la lista de respuestas
- Obtener la lista de comentarios para el incidente especificado o crear un nuevo comentario para el incidente especificado

Ejemplo (Python):

```
#####
# Parte general
#####

import time
import datetime
import requests
import jwt

# El certificado es necesario para la autenticación de un recurso externo
#Puede descargar el certificado desde https://mdr.kaspersky.com,
#guárdelo en su disco y agregue la ruta en la variable:
VERIFY_CERT_PATH = "C:\\tools\\DigiCert Global Root G2.crt"

#URL de la API de REST de MDR:
API_URL = "https://mdr.kaspersky.com/api/v1"

# El id. de su cliente y sus tokens de usted
#Para obtener más información sobre cómo obtener su ID y los tokens, consulte la ayuda https://support.kaspersky.com/MDR/en-US/258285.htm
CLIENT_ID = "9ed43ed54sAmpleIdf349323951f" # (Pegue su valor)
REFRESH_TOKEN = "ReFrEsHToKeN" # (Pegue su valor)
ACCESS_TOKEN = "AcCeSsToKeN" # (Pegue su valor)

#####
#Obtenga un token de acceso y un token de actualización para la próxima actualización del token de acceso
#####

if REFRESH_TOKEN:
    refresh_token_exp = jwt.decode(REFRESH_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"REFRESH_TOKEN fecha y hora de caducidad: {datetime.datetime.fromtimestamp(refresh_token_exp)}")
    if refresh_token_exp > time.time():
        print("REFRESH_TOKEN es válido")
    else:
        print(
            "Debe actualizar REFRESH_TOKEN; tómelo de la consola MDR (https://support.kaspersky.com/MDR/es-ES/258285.htm)"
        )
        exit()
else:
    print(
        "Debe rellenar el valor REFRESH_TOKEN; tómelo de la Consola MDR (https://support.kaspersky.com/MDR/es-ES/258285.htm)"
    )
    exit()

#Verificar la presencia y validez del token de acceso
need_update_access_token = False
if ACCESS_TOKEN:
    access_token_exp = jwt.decode(ACCESS_TOKEN, options={"verify_signature": False}).get("exp")
    print(f"ACCESS_TOKEN fecha y hora de caducidad: {datetime.datetime.fromtimestamp(access_token_exp)}")
    if access_token_exp > time.time():
        print("ACCESS_TOKEN es válido")
    else:
        need_update_access_token = True
else:
    need_update_access_token = True

#Si es necesario, actualice el token de acceso y actualice el token para la próxima actualización del token de acceso
access_token = ACCESS_TOKEN
if need_update_access_token:
    request_body = {"refresh_token": REFRESH_TOKEN}
    result = requests.post(url=f"{API_URL}/{CLIENT_ID}/session/confirm", json=request_body, verify=VERIFY_CERT_PATH)
    result_json = result.json()

    if "error" in result_json:
        print(result_json)
        exit()

    #Es necesario guardar el token de actualización para obtener el siguiente token de acceso cuando caduque el token de acceso actual
    refresh_token = result_json["refresh_token"]
    print(
        f'Su nuevo REFRESH_TOKEN para la próxima vez que solicite ACCESS_TOKEN (reemplace el valor de REFRESH_TOKEN con este valor):: "{refresh_token}"'
    )

    # Se requiere un nuevo token de acceso para recuperar los datos
    access_token = result_json["access_token"]
    print(f'Su nuevo ACCESS_TOKEN (reemplace el valor de ACCESS_TOKEN con este valor): "{access_token}"')

#El token de acceso se añade al encabezado de la solicitud
headers = {"Authorization": f"Bearer {access_token}"}

#####
#Obtener el número de activos
#####

#La fecha y la hora están en milisegundos a partir de 1970-01-01T00:00:00Z
request_body = {
    "max_last_seen": int(time.time())
    * 1000, # Limitar el tiempo máximo de la última aparición del activo a la hora actual
    "min_last_seen": 163931132000, # Limitar el tiempo mínimo de la última aparición del activo a la constante: Domingo 12 de diciembre, 2021 12:12:12
    PM (GMT)
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
#Obtener la lista de activos
#####

request_body = {
    # Parámetros de búsqueda:
    "version": 2, # Especificar 2 como la versión de la solución
    "max_last_seen": int(time.time())
    * 1000, # Limitar el tiempo máximo de la última aparición del activo a la hora actual
    "min_last_seen": 163931132000, # Limitar el tiempo mínimo de la última aparición del activo a la constante: Domingo 12 de diciembre, 2021 12:12:12
    PM (GMT)
}
```

```

"domain": "",
"host_names": ["MA-MDR-KES-5", "SIN-MDR-KSC"], # (Pegue su valor) Lista de hosts
"is_isolated": False,
"network_interface": "10.70.104.1",
"os_version": "Windows", # El activo debe contener la línea especificada en el nombre del SO
"product": "",
"search_phrase": "mdr", # Frase para buscar en el contenido de los campos: "host_name", "domain", "installed_product_info", "network_interfaces",
"os_version"
"statuses": ["OK", "ABSENT"], # Buscar activos que tengan los estados actuales enumerados aquí
# Opciones para mostrar los resultados de la búsqueda:
"sort": "first_seen:asc", # Ordenar los resultados por la hora de la primera aparición; en el caso de la recuperación de resultados página por
página, es necesario especificar un campo de ordenación que no cambie de una consulta a otra, por ejemplo, "first_seen" (no especifique campos cuyos
valores cambian constantemente, por ejemplo, el campo "last_seen"; esto puede llevar a resultados incorrectos)
"page_size": 100, # Activos por página: 100
"page": 1, # Obtener la primera página de resultados de búsqueda
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtener detalles de los activos
#####

request_body = {
    "version": 2, # Especificar 2 como la versión de la solución
    "asset_id": "0xFA6A68CC9A9415963DE841048A3BE929", # (Pegue su valor) Id. del activo
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/assets/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
).json()
print(result)

#####
# Obtener el número de incidentes
#####

request_body = {
    "max_update_time": int(time.time())
    * 1000, # Limitar el tiempo máximo de la última actualización del incidente a la hora actual
    "min_update_time": 1639311132000, # Limitar el tiempo mínimo de la última actualización del incidente a la constante: Domingo 12 de diciembre, 2021
    "affected_hosts": [
        "MA-MDR-KES-5:0xFA6A68CC9A94145456E841048A3BE929"
    ], # (Pegue su valor) Lista de hosts en formato "host_name:asset_id"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/count", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtener la lista de incidentes
#####

request_body = {
    # Parámetros de búsqueda:
    "max_creation_time": int(time.time())
    * 1000, # Limitar el tiempo máximo de creación del incidente a la hora actual
    "min_creation_time": 1639311132000, # Limitar el tiempo mínimo de la creación del incidente a la constante: Domingo, 12 de diciembre de 2021
    "asset_ids": [
        "0xFA6A68CC9A9415963DE841048A3BE929"
    ], # (Pegue su valor) Lista de activos cuyos incidentes recopilamos
    "priorities": ["HIGH"],
    "resolutions": ["True positive"],
    "response_statuses": ["Confirmed"],
    "response_types": ["hash"],
    "statuses": ["Closed"],
    # Parámetros para entregar los resultados
    "markdown_to_html": True, # Resultados en formato HTML; si el valor es "False", los resultados tendrán el formato Markdown
    "sort": "creation_time:asc", # Ordena los resultados por la fecha y hora en que se creó el incidente. Si recupera los resultados página por página,
asegúrese de especificar un campo de ordenación que se mantenga constante entre consultas, como por ejemplo, "creation_time" (no use campos cuyos valores
cambien constantemente, por ejemplo, el campo "update_time", ya que esto puede dar lugar a resultados incorrectos)
    "page_size": 100, # Incidentes por página: 100
    "page": 1, # Obtener la primera página de resultados de búsqueda
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtener detalles del incidente
#####

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m", # (Pegue su valor) Id. del incidente
    "markdown_to_html": True, # Resultados en formato HTML; si el valor es "Falso", los resultados tendrá el formato Markdown
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/incidents/details", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Obtener una lista de respuestas al incidente
#####

request_body = {
    "incident_id": "60gWG4UBMUGN-LWUuv1m", # (Pegue su valor) Id. del incidente
    "page_size": 10, # respuestas por página: 10
    "page": 1, # Obtener la primera página de resultados de búsqueda
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/list", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)

```

```

)
print(result.json())

#####
# Confirmar la respuesta
#####

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W", # (Pegue su valor) Response ID
    "comment": "comment_text", # Comentario que se añadirá a la respuesta
    "status": "Confirmed", # Nuevo estado de respuesta: "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Rechazar la respuesta
#####

request_body = {
    "response_id": "CEgYG4UBMUGN-LWULP7W", # (Pegue su valor) Response ID
    "comment": "comment_text", # Comentario que se añadirá a la respuesta
    "status": "Declined", # Nuevo estado de respuesta: "Declined"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/response/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

#####
# Actualizar la lista de respuestas
#####

request_body = {
    "responses_ids": [
        "CEgYG4UBMUGN-LWULP7W",
        "2ES16IgB4cAOuyXBb5IB",
    ], # (Pegue sus valores) Id. de respuestas
    "comment": "comment_text", # Comentario que se añadirá a las respuestas
    "status": "Confirmed", # Estado de las nuevas respuestas: "Confirmed"
}
result = requests.post(
    url=f"{API_URL}/{CLIENT_ID}/responses/update", json=request_body, headers=headers, verify=VERIFY_CERT_PATH
)
print(result.json())

```

Ejemplo (Shell):

```
# Obtener token de acceso y nuevo token de actualización
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/session/confirm -H "Content-Type: application/json" -d '{"refresh_token": "{refresh_token}"}'
# Ejemplo de respuesta: A continuación, debe usar access_token para recuperar los datos y el refresh_token para recuperar el nuevo token de acceso y el token de actualización
{
  "access_token": "SamPLET346yoKEsSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkEnSaMPlEt2590KEsS123aMPlE926tOkEnSaMPlE"
}

# Obtener el número de activos
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/count -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"max_last_seen": 1704103200000, "min_last_seen": 1704762000000}'

# Obtener la lista de activos
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/list -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"max_last_seen": 1704103200000, "min_last_seen": 1704762000000, "domain": "", "host_names": ["MA-MDR-KES-S", "SIN-MDR-KSC"], "is_isolated": false, "network_interface": "10.70.104.1", "os_version": "Windows", "product": "", "search_phrase": "mdr", "statuses": ["OK", "ABSENT"], "sort": "first_seen:asc", "page_size": 100, "page": 1, "version": 2}'

# Obtener detalles de los activos
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/assets/details -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"asset_id": "0xFA6A68CC9A9415963DE841048A3BE929", "version": 2}'

# Obtener el número de incidentes
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/count -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"max_update_time": 1704103200000, "min_update_time": 1704762000000, "affected_hosts": ["MA-MDR-KES-S:0xFA6A68CC9A9415963DE841048A3BE929"]}'

# Obtener la lista de incidentes
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/list -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"max_creation_time": 1704103200000, "min_creation_time": 1704762000000, "asset_ids": ["0xFA6A68CC9A9415963DE841048A3BE929"], "priorities": ["HIGH"], "resolutions": ["True positive"], "response_statuses": ["Confirmed"], "response_types": ["hash"], "statuses": ["Closed"], "markdown_to_html": true, "sort": "creation_time:asc", "page_size": 100, "page": 1}'

# Obtener detalles del incidente
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/incidents/details -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"incident_id": "60gWG4UBMUGN-LWUuv1m", "markdown_to_html": true}'

# Obtener una lista de respuestas al incidente
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/responses/list -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"incident_id": "60gWG4UBMUGN-LWUuv1m", "page_size": 10, "page": 1}'

# Actualizar la respuesta
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/response/update -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"response_id": "CEgYG4UBMUGN-LWULP7W", "comment": "comment_text", "status": "Confirmed"}'

# Actualizar la lista de respuestas
curl -X POST https://mdr.kaspersky.com/api/v1/{client_id}/responses/update -H "Content-Type: application/json" -H "Authorization: Bearer {access_token}" -d '{"responses_ids": ["CEgYG4UBMUGN-LWULP7W", "2ES16IgB4cA0UyXB5iB"], "comment": "comment_text", "status": "Confirmed"}'
```

Ejemplo de respuesta de la API de REST con el token de acceso y el nuevo token de actualización:

```
{
  "access_token": "SamPLET346yoKEsSamPLEToK25EnSamPLEToK35EnS",
  "refresh_token": "tOkEnSaMPlEt2590KEsS123aMPlE926tOkEnSaMPlE"
}
```

Ejemplo de respuesta de la API de REST con la estructura y los valores de los comentarios:

```
[{
  "comment_id": "bfu6TiNghqp",
  "author_name": "John Doe",
  "text": "<p>El primer comentario</p>",
  "creation_time": 1601295428640
}, {
  "comment_id": "bfu6TiNghqt",
  "author_name": "Jane Doe",
  "text": "<p>El segundo comentario</p>",
  "creation_time": 1601295433441
}]
```

Ejemplo de respuesta de la API REST cuando la API de REST crea un nuevo comentario y envía una respuesta con los detalles del comentario:

```
{
  "comment_id": "AXTej0Qi4bfu6TiNgmvT",
```

```
"author_name": "Nombre del token",  
"text": "Este es un nuevo comentario creado a través de la API de REST",  
"creation_time": 1601461748122  
}
```

Revocar un token de actualización en Kaspersky Security Center

Puede anular tokens de actualización desde las conexiones de API que actualmente tienen el estado *Activo* o *Inactivo*.

Para anular un token de actualización:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **API**.
Aparece la lista **API**.
2. Haga clic en la conexión de API desde la que desea anular un token de actualización.
Aparece un bloque que contiene la información de conexión.
3. Haga clic en el botón **Revocar**.
Se anula el token de actualización.

Eliminar una conexión API en Kaspersky Security Center

Puede eliminar las conexiones de API existentes.

Para eliminar una conexión de API:

1. En la sección **MDR** de Kaspersky Security Center, haga clic en la pestaña **API**.
Aparece la lista **API**.
2. Seleccione el botón de opción junto a la conexión de API que desea eliminar y haga clic en **Eliminar conexión**.
Se elimina la conexión de API seleccionada.

Eliminar una conexión API en MDR Web Console

Puede editar las conexiones de API existentes.

Para editar una conexión de API:

1. En MDR Web Console, haga clic en la pestaña **API**.

Aparece la lista **All tokens**.

2. Señale la conexión de API que desea eliminar y, luego, haga clic en el icono de la papelera () en el lado derecho de la línea.

Se elimina la conexión de API seleccionada.

Desactivar Kaspersky Managed Detection and Response

Si desea dejar de usar Kaspersky Managed Detection and Response, puede finalizar su uso de forma permanente o suspenderlo temporalmente en activos específicos.

Finalización del uso de Kaspersky Managed Detection and Response

Puede finalizar manualmente el uso de Kaspersky Managed Detection and Response si desea dejar de usarlo.

Al finalizar el uso de Kaspersky Managed Detection and Response, Kaspersky Managed Detection and Response deja de enviar telemetría desde sus activos. Para eliminar los datos sobre su organización desde la infraestructura de Kaspersky Managed Detection and Response, comuníquese con [el soporte técnico](#).

Para finalizar el uso de Kaspersky Managed Detection and Response:

1. En Kaspersky Security Center Web Console o Kaspersky Next Expert View, vaya a la sección **Activos (dispositivos)** → **Directivas y perfiles** si está utilizando [aplicaciones EPP](#) que admiten directivas.

Si está utilizando aplicaciones EPP que no admiten directivas, vaya a la sección **Activos (dispositivos)** → **Tareas**.

Se abre la lista de directivas (o la lista de tareas).

2. Haga clic en una política o tarea que haya creado durante la implementación de Kaspersky Managed Detection and Response para configurar la integración entre una aplicación de EPP y Kaspersky Managed Detection and Response.

Se abre la ventana de configuración de políticas (o la ventana de configuración de tareas).

3. En la pestaña **Configuración de la aplicación**, en el panel izquierdo, seleccione **Detection and Response** y, luego, en el panel derecho, seleccione **Managed Detection and Response**.

Se abre el panel de configuración de **Managed Detection and Response**.

4. Desactive la opción **Managed Detection and Response activada**.

El nombre de la opción cambia a **Managed Detection and Response deshabilitada**.

5. Guarde los cambios en la directiva o tarea.

6. [Revoque su consentimiento con los términos de uso de la solución MDR](#).

7. Si utiliza Kaspersky Security Center Web Console para trabajar con Kaspersky MDR, también se recomienda [eliminar el archivo de configuración de KPSN del Servidor de administración de Kaspersky Security Center](#) .

Finaliza el uso de Kaspersky Managed Detection and Response.

Suspender temporalmente el uso de Kaspersky Managed Detection and Response

Para cumplir con los [términos de uso de la solución MDR](#), se debe suspender el uso de la solución en los activos si se encuentran temporalmente en el territorio de los Estados Unidos (p. ej., durante un viaje de negocios).

Para suspender el uso de la solución MDR temporalmente en activos particulares:

1. En Kaspersky Security Center, cree un nuevo [grupo de administración](#) para los activos en los que desea suspender el uso de la solución MDR. Podrá modificar la lista de activos de este grupo más adelante.
2. Para este grupo de administración, [cree nuevas directivas](#) de las aplicaciones de EPP utilizadas para proporcionar la telemetría MDR de los activos y, luego, desactive el uso de la solución MDR y Kaspersky Security Network en la configuración de la directiva.

Para obtener detalles sobre la configuración de las directivas, consulte los artículos de ayuda de una aplicación de EPP en particular. Por ejemplo, la ayuda de Kaspersky Endpoint Security para Windows contiene instrucciones sobre la [gestión de directivas](#) y los ajustes de la [integración con la solución MDR](#).

3. [Mueva los activos](#) en los que desea suspender el uso de la solución MDR al grupo de administración creado.

La nueva directiva en la que el uso de la solución MDR y Kaspersky Security Network están desactivados se aplicará a los activos después de la sincronización. También puede [forzar la sincronización](#) manualmente.

Para reanudar el uso de Kaspersky Managed Detection and Response después de la suspensión:

1. Excluya el activo del grupo de administración utilizado para la suspensión.
2. Aplique una directiva regular en la que el uso de la solución MDR esté activado y configurado para este activo.

La solución MDR no supervisará los activos hasta que se les aplique una directiva en la que se active y configure el uso de la solución MDR.

Revocación de su consentimiento con los términos de uso de la solución MDR

Si decide dejar de usar Kaspersky Managed Detection and Response, revoque su consentimiento con los términos de uso de MDR y, luego, [desactive el uso de Kaspersky Managed Detection and Response](#) en los activos.

Esta función solo está disponible si tiene configurado el derecho de acceso a la **Integración de la aplicación** en [Kaspersky Security Center Web Console](#) o [Kaspersky Next Expert View](#).

Para revocar su consentimiento con los términos de uso de la solución MDR:

1. Para hacerlo, en la sección MDR de Kaspersky Security Center, haga clic en la pestaña **Uso de MDR**.
2. Expanda el bloque **Condiciones de uso para la solución MDR** haciendo clic en su nombre.
3. Haga clic en el enlace **Revocar la confirmación de aceptación de las Condiciones de uso para la solución MDR**.
4. Confirme que desea revocar su consentimiento con los términos de uso de la solución MDR.
Su consentimiento con los términos de uso de la solución MDR queda revocado.

Si desea eliminar la información sobre su organización de la infraestructura de MDR, comuníquese con el [Servicio de soporte técnico](#).

Problemas conocidos

Kaspersky Managed Detection and Response tiene una serie de limitaciones que no son críticas para el funcionamiento de la aplicación:

- Si clona un activo virtual o físico con Kaspersky Endpoint Security para Linux que ya está conectado a la solución MDR, los datos de telemetría de los activos clonados no se transmiten correctamente. En estos activos clonados, desinstale Kaspersky Endpoint Security for Linux, elimine el archivo `install_id` en la carpeta `/var/opt/kaspersky/epagent/` y luego vuelva a instalar Kaspersky Endpoint Security for Linux.
- Para los activos con Kaspersky Endpoint Security para Windows en la configuración de Endpoint Detection and Response Agent (EDR Agent), los estados *Advertencia* y *Crítico* para los componentes de protección y control no se muestran.
- No puede usar las [funciones de Kaspersky Endpoint Detection and Response Optimum](#) para los activos con Kaspersky Endpoint Security para Windows en la configuración de EDR Agent.
- Las **aplicaciones de Kaspersky que funcionan con la sección MDR** de la tarjeta de recursos en MDR Web Console pueden contener aplicaciones de Endpoint Protection Platform (EPP) desactualizadas, que ya no se utilizan para trabajar con Kaspersky Managed Detection and Response. Se produce cuando en el activo una aplicación EPP nueva sustituye a una desactualizada. Para estas aplicaciones desactualizadas, el campo **Visto por última vez** contiene la fecha anterior, mientras que para la nueva aplicación de EPP, el campo **Visto por última vez** contiene la fecha más reciente.
- La solución MDR que usa los ajustes de KPSN no es compatible con jerarquías de Servidores de administración de Kaspersky Security Center si solo el servidor principal de la jerarquía tiene Accesibilidad a Internet.
- La solución de MDR no es compatible con la carga automática de archivos mayores a 64 MB cuando se utiliza la respuesta [Get artefacts](#), que está disponible en Kaspersky Endpoint Detection and Response Expert, integrado en la Open Single Management Platform.
- El complemento de MDR para Kaspersky Security Center y el complemento de MDR para Open Single Management Platform no admiten la visualización de información sobre Kaspersky Embedded Systems Security para Linux versión 4.0 o posterior en la lista de activos que no funcionan.

Ponerse en contacto con el Soporte técnico

Esta sección describe cómo obtener soporte técnico y los términos en los que está disponible.

Cómo obtener soporte técnico

Si no puede encontrar una solución a su problema en la [documentación de Kaspersky Managed Detection and Response](#) o en [cualquiera de las fuentes de información sobre Kaspersky Managed Detection and Response](#), póngase en contacto con Asistencia al cliente. Los especialistas de soporte técnico responderán todas sus preguntas sobre la instalación y el uso de Kaspersky Managed Detection and Response.

Kaspersky brinda soporte a Kaspersky Managed Detection and Response durante su ciclo de vida (consulte la [página del ciclo de vida del soporte del producto](#)). Antes de ponerse en contacto con el Servicio de soporte técnico, lea las [reglas de soporte](#).

Puede ponerse en contacto con el Servicio de soporte técnico de una de las siguientes maneras:

- [Visitando el sitio web del Servicio de soporte técnico](#)
- Enviando una solicitud al Servicio de soporte técnico desde el [portal de Kaspersky CompanyAccount](#)

Soporte técnico a través de Kaspersky CompanyAccount

[Kaspersky CompanyAccount](#) es un portal para las empresas que utilizan las aplicaciones Kaspersky. El portal Kaspersky CompanyAccount está diseñado para facilitar la interacción entre los usuarios y los especialistas de Kaspersky mediante solicitudes en línea. Puede usar Kaspersky CompanyAccount para hacer un seguimiento del estado de sus solicitudes en línea y almacenar un historial de dichas solicitudes.

Puede registrar a todos los empleados de su organización en una única cuenta de Kaspersky CompanyAccount. Esta cuenta única le permite administrar de forma centralizada las solicitudes electrónicas que envían los empleados registrados a Kaspersky, además de administrar los privilegios de estos empleados mediante Kaspersky CompanyAccount.

El portal Kaspersky CompanyAccount está disponible en los idiomas siguientes:

- Inglés
- Español
- Italiano
- Alemán
- Polaco

- Portugués
- Ruso
- Francés
- Japonés

Para obtener más información sobre Kaspersky CompanyAccount, visite el [sitio web del Servicio de soporte técnico](#) .

Fuentes de información sobre la solución

En la página de [Kaspersky Managed Detection and Response](#), puede ver información general sobre la solución, sus funciones y sus características.

Glosario

Activo

Dispositivo con una aplicación Kaspersky EPP instalada (por ejemplo, Kaspersky Endpoint Security para Windows).

Aplicación de EPP

Una aplicación incluida en un sistema de protección para dispositivos de extremos (plataforma de protección de extremos o EPP). Las aplicaciones de EPP se instalan en dispositivos endpoints dentro de la infraestructura de TI de una organización (por ejemplo, dispositivos móviles, ordenadores o portátiles). Un ejemplo de una aplicación de EPP es Kaspersky Endpoint Security para Windows como parte de la solución EPP Kaspersky Endpoint Security for Business.

Incidente

Actividad considerada crítica por la tecnología de detección y que requiere una reacción inmediata de Kaspersky Managed Detection and Response.

Inquilino

Un inquilino es una organización a la que usted proporciona Kaspersky Managed Detection and Response.

IOC

Un indicador de compromiso (o IOC) muestra las pruebas en un dispositivo que apuntan a una violación de la seguridad.

Plataforma de protección de extremos (EPP)

Sistema integrado de protección compleja para dispositivos de extremos (por ejemplo, dispositivos móviles, ordenadores o portátiles) que incluye varias tecnologías de seguridad. Un ejemplo de plataforma de protección de endpoints es Kaspersky Endpoint Security for Business.

Respuesta

La respuesta a incidentes es una metodología estructurada para manejar incidentes de seguridad, brechas y amenazas cibernéticas.

Táctica MITRE

El objetivo que quería lograr un atacante durante un ciberataque en la infraestructura del cliente.

Técnica MITRE

Método utilizado por el atacante para realizar acciones maliciosas en la infraestructura del cliente durante un ciberataque. Cada táctica MITRE contiene una serie de técnicas MITRE.

Telemetría

Datos que se envían desde los activos a Kaspersky Managed Detection and Response.

Información sobre el código de terceros

Se ha utilizado código de terceros en el desarrollo de la solución.

Para obtener información sobre código de terceros en la Web Console MDR, póngase en contacto con el equipo de soporte de Kaspersky Managed Detection and Response.

La información sobre el código de terceros utilizado en el complemento de MDR se encuentra en el archivo [legal_notices.txt](#) .

Avisos de marcas registradas

Las marcas registradas y las marcas de servicio son propiedad de sus respectivos propietarios.

Apple, Mac, macOS y Safari son marcas comerciales de Apple Inc.

Amazon AWS, Amazon Web Services son marcas comerciales de Amazon.com, Inc. o sus filiales.

Active Directory, Internet Explorer, Microsoft, Microsoft Edge, Outlook, PowerShell, Windows PowerShell, Windows y Windows Server son marcas comerciales del grupo de empresas de Microsoft.

Firefox y Mozilla son marcas comerciales de Mozilla Foundation en EE. UU. y otros países.

Google y Google Chrome son marcas comerciales de Google, LLC.

Linux es la marca comercial registrada de Linus Torvalds en EE. UU. y otros países.

Python es una marca comercial o una marca comercial registrada de Python Software Foundation.

Configurar los ajustes de auditoría para trabajar con Kaspersky Managed Detection and Response

Recomendamos configurar los siguientes ajustes de auditoría para garantizar un funcionamiento estable y maximizar la eficiencia de Kaspersky Managed Detection and Response:

- **Configurar la Directiva de auditoría de eventos de Windows**

Para maximizar la eficiencia de Kaspersky Managed Detection and Response, debe configurar la Directiva de auditoría de eventos de Windows en sus activos.

Para configurar la Directiva de auditoría de eventos de Windows:

1. En su controlador de dominio de Windows, pulse **Win + R** para abrir la ventana **Ejecutar**.
2. En el campo **Abrir**, escriba `gpedit.msc` y luego presione **Intro** o haga clic en **Aceptar**. Aparece la ventana **Editor de directivas de grupo local**.
3. En el árbol de la consola, haga clic en **Configuración del equipo** → **Configuración de Windows** → **Configuración de seguridad** → **Configuración avanzada de directiva de auditoría** → **Directivas de auditoría del sistema** - **Objeto de directiva de grupo local**.
4. Haga clic en el nodo **Inicio de sesión en la cuenta**. Establezca los siguientes valores en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Auditar validación de credenciales	Éxito y fracaso
Auditar servicio de autenticación Kerberos	Éxito y fracaso
Auditar operaciones de tickets del servicio Kerberos	Éxito y fracaso

5. Haga clic en el nodo **Administración de cuentas**. Establezca los siguientes valores en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Auditar la administración de cuentas de equipo	Éxito y fracaso
Auditar la administración de grupos de seguridad	Éxito
Auditar la administración de cuentas de usuario	Éxito y fracaso

6. Haga clic en el nodo **Acceso a DS**. Establezca los siguientes valores en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Auditar el acceso al servicio de directorio	Éxito y fracaso
Auditar los cambios en el servicio de directorio	Éxito y fracaso

7. Haga clic en el nodo **Iniciar sesión / Cerrar sesión**. Establezca los siguientes valores en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Auditar bloqueo de cuentas	Fallo
Auditar inicios de sesión	Éxito y fracaso
Auditar el inicio de sesión especial	Éxito y fracaso

8. Haga clic en el nodo **Acceso a objetos**. Establezca los siguientes valores en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Auditar servicios de certificación	Éxito y fracaso
Auditar archivos compartidos	Éxito
Auditar plataforma de filtrado	Éxito
Auditar otros eventos de acceso a objetos	Éxito

9. Haga clic en el nodo **Cambio de directiva**. Establezca los siguientes valores en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Auditar cambios de directiva	Éxito
Auditar cambios de directivas a nivel de reglas de MPSSVC	Éxito

10. Haga clic en el nodo **Uso de privilegios**. Establezca el siguiente valor en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Auditar el uso de privilegios confidenciales	Éxito

11. Haga clic en el nodo **Sistema**. Establezca los siguientes valores en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Auditoría del cambio de estado de seguridad	Éxito
Auditar extensión del sistema de seguridad	Éxito

12. En el árbol de la consola, haga clic en **Configuración del equipo** → **Plantillas administrativas** → **Componentes de Windows** → **Windows PowerShell**. Establezca el siguiente valor en el lado derecho de la ventana:

Subcategoría	Auditar eventos
Activar el registro de bloques de scripts de PowerShell	Habilitado

13. Cierre la ventana del **Editor de directivas de grupo local**.

Todos los cambios se guardan automáticamente.

La Directiva de auditoría de eventos de Windows está configurada para usarse con Kaspersky Managed Detection and Response.

• Configurar la Auditoría de objetos de Active Directory

Para maximizar la eficacia de Kaspersky Managed Detection and Response, debe configurar la auditoría en sus controladores de dominio de Windows.

Para configurar la Auditoría de objetos de Active Directory:

1. En su controlador de dominio de Windows, pulse **Win + R** para abrir la ventana **Ejecutar**.
2. En el campo **Abrir**, escriba `dsa.msc` y, a continuación, pulse **Intro** o haga clic en **Aceptar**. Aparece la ventana **Usuarios y equipos de Active Directory**.

3. En el árbol de la consola, haga clic con el botón derecho en <su nombre de dominio> y seleccione **Buscar**. Aparece la ventana **Buscar usuarios, contactos y grupos**.
4. Introduzca **Administrador** en el campo **Nombre** y haga clic en **Buscar ahora**.
5. En el área de **Resultados de la búsqueda**, haga clic con el botón derecho en el objeto **Administrador** y seleccione la pestaña **Propiedades** → **Seguridad** → **Avanzado** → **Auditoría**.
6. Haga clic en **Agregar** para abrir la ventana **de Entrada de auditoría para el administrador**. Haga clic en **Seleccionar una entidad de seguridad**, escriba Todos, haga clic en **Comprobar nombres** y luego haga clic en **Aceptar**.
7. En la ventana **Entrada de auditoría para el administrador**, marque las casillas **Mostrar contenido**, **Permisos de lectura**, **Modificar permisos**, **Modificar propietario**, **Leer todas las propiedades** y **Escribir todas las propiedades**.
8. Haga clic en **Aceptar** → **Aplicar** → **Aceptar**.

La auditoría del objeto de Active Directory **Administrador** ahora está configurada para usarse con Kaspersky Managed Detection and Response.

9. Realice los mismos pasos para los siguientes objetos predeterminados de Active Directory y para los usuarios y grupos importantes de su dominio que existan y estén activados en su sistema:

- **Administradores**
- **Grupo con autorización de replicación de contraseñas RODC**
- **Editores de certificados**
- **Controladores de dominio clonables**
- **Grupo de replicación de contraseñas RODC denegado**
- **DnsAdmins**
- **DnsUpdateProxy**
- **Administradores de dominio**
- **Equipos de dominio**
- **Controladores de dominio**
- **Administradores de organización**
- **Administradores clave de organización**
- **Controladores de dominio de organización de solo lectura**
- **Propietarios del creador de directivas de grupo**
- **Administradores clave**
- **krbtgt**

- Usuarios protegidos
- Servidores RAS e IAS
- Controladores de dominio de solo lectura
- Administradores de esquemas
- Configurar la auditoría para los servicios de certificados de Active Directory, las plantillas de certificados y los objetos de certificado

Para maximizar la eficiencia de Kaspersky Managed Detection and Response, debe configurar la auditoría para el servicio **Servicios de certificados de Active Directory**, las plantillas de certificados y los objetos en los hosts que tengan activados los **Servicios de certificados de Active Directory** (AD CS).

*Para configurar la auditoría para el servicio **Servicios de certificados de Active Directory**:*

1. En Windows, presione **Win + R** para abrir la ventana **Ejecutar**.
2. En el campo **Abrir**, escriba `cmd` y, a continuación, pulse **Intro** o haga clic en **Aceptar**. Aparece la ventana del **símbolo del sistema**.
3. Para configurar la auditoría de la entidad de certificación, introduzca los siguientes comandos y después presione Intro:


```
certutil -setreg CA\AuditFilter 127
certutil -setreg policy\EditFlags +EDITF_AUDITCERTTEMPLATELOAD
```
4. Para reiniciar el servicio **Servicios de certificados**, ingrese el siguiente comando y presione Intro:


```
net stop certsvc && net start certsvc
```

Para configurar la auditoría de seguridad de plantillas de certificados:

1. En Windows, presione **Win + R** para abrir la ventana **Ejecutar**.
2. En el campo **Abrir**, escriba `adsiedit.msc`, y, a continuación, pulse **Intro** o haga clic en **Aceptar**.
3. Haga clic con el botón derecho en **Editar ADSI** y seleccione **Conectar a**.
4. En la sección **Punto de conexión**, seleccione el valor **Configuración** en el campo **Seleccionar un contexto de nomenclatura conocido**.
5. Haga doble clic en **Configuración/Esquema** en el panel izquierdo.
6. Seleccione la carpeta **CN=Configuration,DC=...** → **CN=Services** → **CN=Public Key Services** → **CN=Certificate Templates**.
7. Haga clic con el botón derecho en la carpeta **CN=Certificate Templates**, seleccione **Propiedades** y abra la pestaña **Seguridad**.
8. Haga clic en el botón **Avanzado** y seleccione la pestaña **Auditoría**.
9. Haga clic en **Todos**, marque las casillas **Escribir todas las propiedades**, **Eliminar**, **Modificar permisos**, **Modificar propietario**, **Todas las escrituras validadas** y haga clic en **Aceptar**.

Para configurar la auditoría de seguridad para el objeto NTAAuthCertificates:

1. En el campo **Abrir**, escriba `adsiedit.msc` y luego presione **Intro** o haga clic en **Aceptar**.
2. Haga clic con el botón derecho en **ADSI Edit** y seleccione **Conectar a**.
3. En la sección **Punto de conexión**, seleccione el valor **Configuración** en el campo **Seleccionar un contexto de nomenclatura conocido**.
4. Haga doble clic en **Configuración/Esquema** en el panel izquierdo.
5. Seleccione la carpeta **CN=Configuration,DC=...** → **CN=Services** → **CN=Public Key Services** → **CN=NTAuthCertificates**.
6. Haga clic con el botón derecho en la carpeta **CN=NTAuthCertificates**, seleccione **Propiedades** y abra la pestaña **Seguridad**.
7. Haga clic en el botón **Avanzado** y seleccione la pestaña **Auditoría**.
8. Haga clic en **Todos**, marque las casillas **Escribir todas las propiedades**, **Eliminar**, **Modificar permisos**, **Modificar propietario**, **Todas las escrituras validadas** y haga clic en **Aceptar**.

Vídeo de incorporación

Vea el vídeo para obtener más información sobre las principales funciones de la solución MDR.



Solución MDR. Vídeo de incorporación